Morphing-Attacks against Binary Fingervein Templates

Tobias Mitterreiter, Jutta Hämmerle-Uhl, Andreas Uhl

Visual Computing and Security Lab (VISEL)
Department of Artificial Intelligence & Human Interfaces, University of Salzburg, Austria
uhl@cs.sbg.ac.at

Abstract. For the first time, the feasibility of creating morphed templates for attacking vascular biometrics is investigated, in particular finger vein recognition schemes generating binary vascular patterns 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 construct the morphed template for a given target template depends on the employed sensor. It turns out that targeted template doppelgaenger selection is important for an attack success. The identified threat level in terms of IAPMR is often found to be > 0.8 for several sensor / template generation scheme / morphing technique combinations. Thus, the risk as imposed by such attacks can be said to be considerable.

1 Introduction

Since the introduction of the "magic passport" [1] 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 [2, 3]. Apart from the face modality, the threat originating from morphed samples or templates of other modalities is less obvious, as there is no connection with ID documents and no corresponding inclusion of morphed sample image data. As a consequence, we have seen only a single proposal for fingerprint morphing using traditional model-based techniques [4] and its potential detection [5, 6], and a second proposal for fingerprint morphing using learning-based schemes (i.e. GANs [7]). For iris recognition, a first work deals with the construction of morphed iris codes [8], later also image-level iris morphing has been demonstrated [9]. Also, a suggestion for systematic analysis of biometric system vulnerability with respect to morphing attacks [10] addressed face and iris morphing attacks. Recently, sample-oriented generation of morphed fingervein sample data has been explored together with a demonstration of the feasibility of using these data as presentation attack artefacts [11].

In this work, we investigate the feasibility of creating morphed vascular binary templates, in particular we deal with finger vein recognition systems. Based on the morphed finger vein templates we conduct a vulnerability analysis of five different recognition systems. The actual threat of such data is illustrated in Fig. 1 - the most efficient attacks inject such morphed templates into the database, replacing the templates of a legitimate user, thus allowing the legitimate user as well as the attacker to authenticate to the biometric system based on the morphed templates.

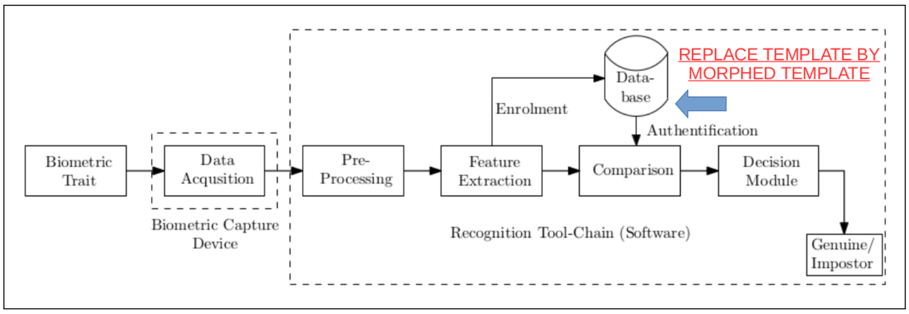

Fig. 1: Main point of morphed template attack against a biometric system.

The principle of the attack is visualised in Fig. 2: The attacker's template is f_1 and there is no corresponding template stored in the database. Therefore the attacker can not authenticate him/herself with the system via f_1 ("failed"). Template f_2 is computed from a sample of a legitimate user. The authentication is successful because the user's template t_1 is stored in the database and the similarity score derived in the comparison is higher than the threshold. As the attacker has full access to all database templates, he/she aims to morph his/her template f_1 with a template derived from a legitimate users' sample, in this case, t_1.

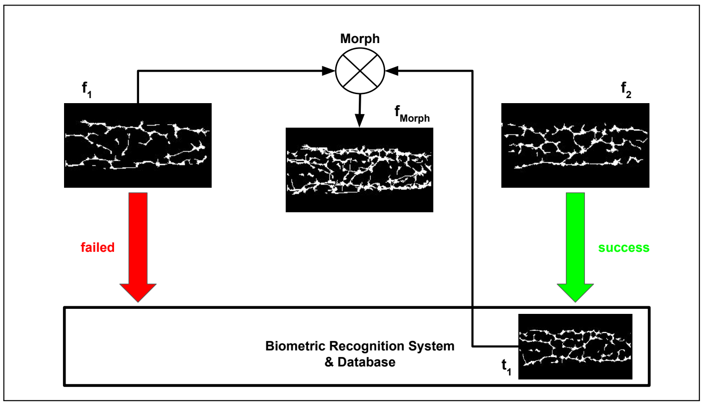

Fig. 2: Working principle of attacking the template database.

The attacker then replaces template t_1 with the resulting morphed template f_{Morph} in the database. This approach allows both, the attacker and the legitimate user, to authenticate successfully via their finger veins in the future, as both extracted templates f_1 and f_2 should be close enough to the morphed template f_{Morph} in the database.

Another attack option is to replace a template retrieved from the database for the comparison process by a morphed template achieving the same effect, but this attack is much less static and requires dynamic injection into the data transfer from the database or into an ongoing template comparison process, respectively. Also, for this attack we do not really require a morphed template, injecting the attackers template directly is sufficient to make the attack work.

The remainder of the paper is organised as follows. In Section 2, we will demonstrate how a digitally morphed template can be created from two binary finger vein templates. Section 3 explains the experimental setup to conduct the vulnerability analysis, including the definition of the used recognition software and finger vein datasets, respectively, and defining the way how to actually assess the vulnerability. This section also contains an explanation how we aim to reveal the existence of morphed templates in a database. Experimental results are presented and discussed in Section 4, while we conclude the paper in Section 5.

2 Morphing of Binary Finger Vein Templates

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 two 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 (this has been applied to finger vein samples in [11]).

However, we aim at binary templates but not at grayscale samples, and the original concept of morphing needs to be adapted correspondingly as we cannot rely on particular landmarks and interpolation of binary values is hardly possible in meaningful manner. In particular, it makes sense to consider the way how the similarity of two binary templates is determined during template comparison. Contrasting to e.g. iris code comparisons, where binary codes are compared under left-right shifting them against each other and taking the minimum resulting Hamming distance as their similarity value, in comparing vascular binary features typically the "Miura Matcher" [12] is being employed. In this comparison algorithm, two binary templates are correlated against each other computing the maximum among two-dimensional shifts of rotated template versions. The correlation is computed on the center region of the templates, the so-called "kernel" (see Fig. 4).

We define the following template morphing approaches (in fact, these are more template fusion schemes):

- **Template OR (XOR)**: This approach applies a logical OR to the two vascular samples f_1 and f_2: $f_{morph} = f_1 \vee f_2$ without any alignment between the two templates. Note the $\vee$ is the fundamental operation for all template morphing variants, the sole difference is the type of alignment that is applied between the two. Fig. 3 illustrates the simple XOR process and outcome.
- **(Template) Rotation**: The Miura Matcher uses a rotation compensation in the template comparison process, which we use to determine under which rotation parameter the similarity between the two templates to be morphed is maximal. Thus we rotate one of the two templates by that parameter, and use nearest neighbour interpolation and cropping to result in an identical template size. Finally, the rotated template and the second one are fused by logical OR.

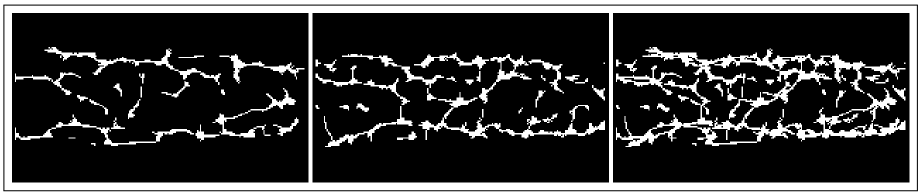

Fig. 3: Two MC binary templates from the MMCBNU dataset and their XOR morphed template.

- **(Kernel) Alignment**: The approach is to determine how to align the kernel (i.e. central area according to the Miura Matcher) of a template to a second template, so that the similarity is highest. To do this, we employ the Miura Matcher to compute the convolution matrix and filter the result for the highest value, corresponding to the alignment with the highest similarity, and to return the optimal shift parameters (in two directions). This process is repeated for different rotations to obtain the optimal kernel alignment and shift parameters for the subsequent morphing process. Fig. 4 illustrates the kernel of a template and its aligned OR fusion with another template.

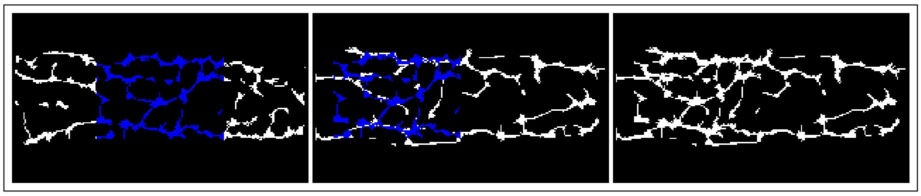

Fig. 4: The kernel of a MC template from the MMCBNU dataset (in blue), and its morphing with a second template (in blue overlay and binary).

- **F(ull) Alignment**: This approach is an extended version of the previous (Kernel) Alignment approach. The difference is that we no longer consider the kernel alone but rotate and shift the entire template to optimise similarity, before template OR is being applied. Fig. 5 illustrates the process and highlights the difference to (Kernel) Alignment.

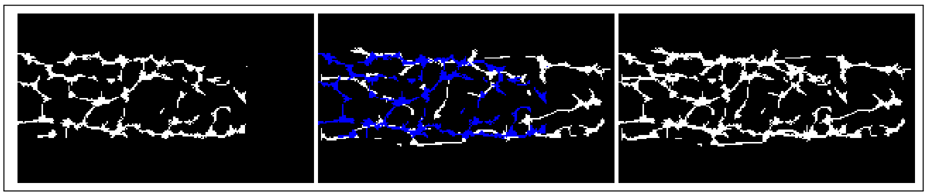

Fig. 5: A rotated and shifted MC template from the MMCBNU dataset, and its morphing with a second template (in blue overlay and binary).

For the envisioned attack, typically an attacker does not just morph his/her template with an arbitrary template in the database. We have an attacker template, say f_1, and need to select a suited template t_1 in the database from a legitimate 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" [13], but in the finger vein setting, we only need to consider a smaller set of requirements for a suited "doppelgaenger" finger vein template. In order to investigate the role this selection plays, we have chosen two approaches: First, in "similar" mode, we select t_1 as the closest template of a different subject contained in the dataset determined in terms of Miura Matcher template comparison score using a particular recognition system. Second, in "unsimilar" mode, we select t_1 as the most distinct sample to f_1 in the same sense.

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 [14]. 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 [15] 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 have found both involved subjects to be symmetrically represented (which is to be expected due to the symmetric XOR construction of the morphs), we resort to the simpler IAPMR for result reporting.

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

- IAPMR$_1$ determines IAPMR by considering template comparison scores for which the morphed template is compared to template t_1 only, i.e. the template of the legitimate user that has actually been used to create the morph.
- IAPMR$_n$ determines IAPMR by considering template comparison scores for which the morphed template is compared to all templates of the subject from which t_1 has been derived.
- IAPMR$_{n-1}$ determines IAPMR by considering template comparison scores for which the morphed template is compared to all templates of the subject from which t_1 has been acquired *except* for template t_1.

For defining a "successful" template comparison in the context of IAPMR, we first compute the EER of the corresponding dataset / recognition scheme combination and use the corresponding threshold in the decision. Subsequently, we start with the first template of the first subject, determine its most similar and dissimilar template in the database (from different subjects) and generate the corresponding morphs. Then we compute the template comparisons between all templates of the first subject and the generated morphs and check if the result adheres to the threshold (i.e. a successful attack has been conducted). The results increase the correspondings counters and we proceed to the next template of the first subject. This procedure is conducted for all subjects.

3.2 Data and Recognition Software

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

- *The Finger Vein Universiti Sains Malaysia Database* (**FV-USM** [16]): Contains 5904 palmar finger vein images, exhibiting a resolution of 640x480 pixels, acquired from 123 subjects. All of them participated in 2 acquisition sessions where each time 4 fingers per subject and 6 images per finger were captured by a custom built capturing device.
- *The Multimedia Chonbuk National University Database* (**MMCBNU_6000** [17]): The 6000 palmar light transmission finger vein images, exhibiting a resolution of 640x480 pixels, contained in this dataset were acquired from 100 subjects. From all of them 6 fingers per subject and 10 images per finger were captured in a single session utilizing a capturing system based on a modified webcam.
- The *University of Twente Finger Vascular Pattern Database* (**UTFVP** [18]) contains six fingers (ring, middle and index finger from both hands) from 60 volunteers in two sessions. At each session, two palmar samples per finger were captured (resulting in 4 samples per finger). The samples have an original resolution of 672x380 pixels, while their region of interest (RoI) is 672x285 pixels.
- The *PLUSVein-FV3 Palmar LED Finger Vein Data Set* (**PLUS** [19]) contains palmar 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 [20]. Here, only LED illuminated images are used, the resolution of the single finger RoI cropped from the 3-finger capture is 736x192 pixels.

The finger detection, finger alignment and RoI extraction for UTFVP and PLUS is done as described in [21]. After pre-processing and feature extraction, the resulting binary templates are used to perform the experiments. We conducted these experiments by applying the PLUS OpenVein Finger- and Hand-Vein Toolkit (`http://www.wavelab.at/sources/OpenVein-Toolkit/` [22]). We selected five techniques based on the binary vessel structure. The extraction schemes used are *Wide Line Detector (WLD)* [23], *Isotropic Undecimated Wavelet Transform (IUWT)* [24], *Gabor Filter (Gabor)* [25], *Maximum Curvature (MC)* [12], and *Principal Curvature (PC)* [26]. These binary feature templates are subsequently compared using a correlation-based approach proposed in [12], the so called Miura Matcher.

4 Experimental Results

The experimental section is split into two parts - first, we conduct a threat analysis, i.e., we experiment if the generated morphed templates are a real threat to the biometric system in question, and here we discriminate different data sets and template generation schemes. Second, we investigate if a database maintainer can check the database for eventual morphs, i.e. if we can reliably discriminate morphs from real legitimate templates.

4.1 Threat Evaluation

We explain the results for each IAPMR variant looking at Table 1 (left). The results are based on the FV-USM dataset (123 subjects and 12 samples per finger). For feature extraction we use Maximum Curvature, and for the morphing procedure, we use the XOR Approach. For IAPMR$_1$, we note that the attack is successful in all cases, no matter if the most similar or dissimilar template has been used (the accordance of the template in the morph and the attacking one is sufficient to guarantee the attack is working).

FV-USM (MC Rec.)			MMCBMU (PC Rec.)			UTFVP (PC Rec.)		
	Similar	Unsimilar		Similar	Unsimilar		Similar	Unsimilar
IAPMR$_1$	1	1	IAPMR$_1$	1	1	IAPMR$_1$	1	1
IAPMR$_{n-1}$	0.449	0.263	IAPMR$_{n-1}$	0.180	0.139	IAPMR$_{n-1}$	0.965	0.918
IAPMR$_n$	0.461	0.279	IAPMR$_n$	0.193	0.154	IAPMR$_n$	0.967	0.922

Table 1: IAPMR results of three datasets using XOR Morphing.

The situation is different for IAPMR$_{n-1}$ and IAPMR$_n$. While both values are rather similar (slightly higher for IAPMR$_n$ as the identical template as used in the morph is also considered in the comparison process, among the other ones), there is a clear difference between similar and unsimilar template selection in the morph construction, and IAPMR differs by a factor a bit lower than 2. Therefore, in the following, we will present results for IAPMR$_n$ only but discriminate between the similar and unsimilar template selection process, respectively.

In Fig. 6, we present the overall results for the FV-USM dataset. For the similar doppelgaenger template selection, results follow a clear trend: MC, IUWT, and WLD template generation techniques exhibit a lower IAPMR value (still around 0.40 - 0.45) while PC and GF are most subsceptible to the morphing attack (top IAPMR values are between 0.6 and 0.7). There is also a clear ranking with respect to successful morphing techniques: XOR and Rotation work best, while the Kernel Alignment approach is worst.

For the unsimilar doppelgaenger selection scheme, results are different. While the most vulnerable template generation schemes are still PC and GF, their highest IAPMR values are around 0.4. Contrasting to before, in unsimilar mode the best morphing techniques are Alignment and Falignment. Thus, results clearly confirm that the doppelgaenger selection strategy is of high importance for a successful attack, and that different template generation schemes are fairly different in how far they are vulnerable to template morphing attacks. The former fact also implies, that the attack can be made much more effective if an entire dataset is compromised (as we can select the most similar doppelgaenger), as opposed to the case if only a single template is compromised.

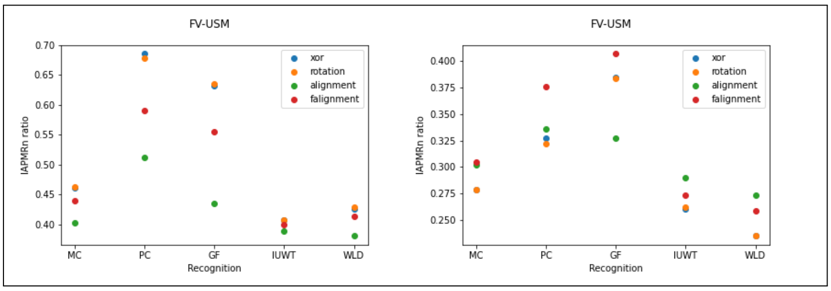

Fig. 6: FV-USM dataset: IAPMR$_n$ results of all template types and morphing approaches in similar (up) and unsimilar (low) mode, respectively.

Now let us look into the question if the results are stable across different datasets (i.e. finger vein sensors). Table 1 (middle, for MMCBMU data) reveals a different behaviour as compared to Table 1 (left). We notice rather low IAPMR$_{n-1}$ and IAPMR$_n$ values and the difference between similar and unsimilar template selection for the morphing process is rather negligible.

Fig. 7 shows the overview results of the MMCBMU dataset. We clearly observe, that the situation is different as compared to the FV-USM dataset. Here, it is only GF template generation which is highly vulnerable by the morphing attack (with IAPMR$_n$ being almost 1.0), and PC is much less vulnerable (actually, here PC is the least vulnerable template generation scheme). For the similar doppelgaenger template selection scheme, there is no significant winner in terms of best morphing approach.

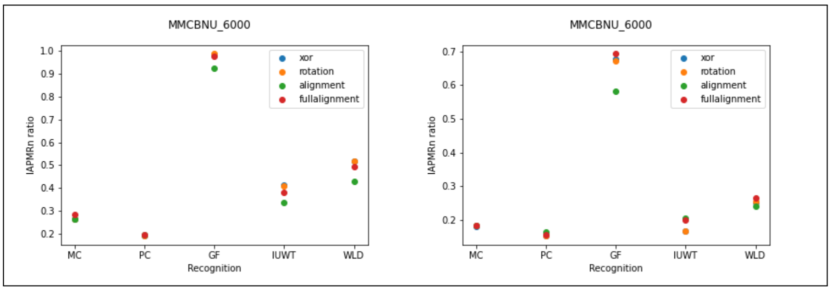

Fig. 7: MMCBMU dataset: IAPMR$_n$ results of all template types and morphing approaches in similar (up) and unsimilar (low) mode, respectively.

When comparing the similar to the unsimilar template selection results, the general trend is almost identical. GF is most vulnerable (with IAPMR$_n$ at 0.7), while the other template generation schemes are between 0.1 and 0.3 in terms of IAPMR$_n$. It is also interesting to note that for the MMCBMU dataset, the doppelgaenger template selection variant chosen is by far less important for the resulting threat (except for GF), as compared to the FV-USM dataset.

Table 1 (right) shows exemplary results for the UTFVP dataset, shown in similar way as Table 1 for the FV-USM and MMCBMU datasets. respectively. Constrasting to the results for FV-USM (but in accordance to those for MMCBMU), here we do not observe a large difference between IAPMR for the similar and unsimilar template selection approach, respectively, while all displayed IAPMR variants are on a very high level (which on the other hand does not correspond to results for MMCBMU data).

Again, a summary of the results for the UTFVP dataset is displayed in Fig. 8, we again observe different behaviour as compared to the previous dataset. PC is most subsceptible (with IAPMR$_n$ close to 1.0), while IUWT and GF still reach IAPMR$_n$ of 0.45 - 0.6. For the similar template selection mode there is no clear winner in terms of morphing generation (Rotation is often pretty well performing).

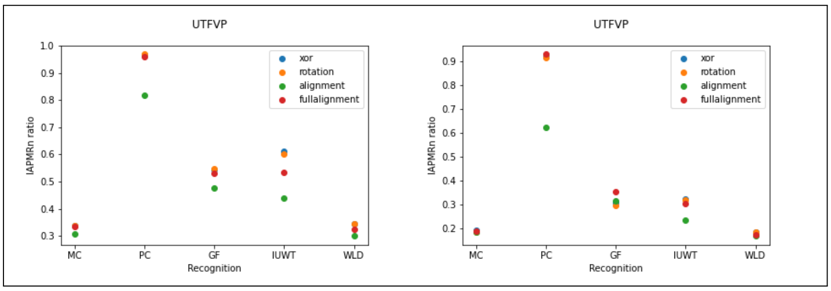

Fig. 8: UTFVP dataset: IAPMR$_n$ results of all template types and morphing approaches in similar (up) and unsimilar (low) mode, respectively.

The unsimilar template selection mode results in lower IAPMR$_n$ values, but not as clear as e.g. for FV-USM data. In this setting, Falignment is the best performing morphing approach. PC can still reach IAPMR$_n$ of > 0.9, so for this setting an arbitrary template can be selected for the morph.

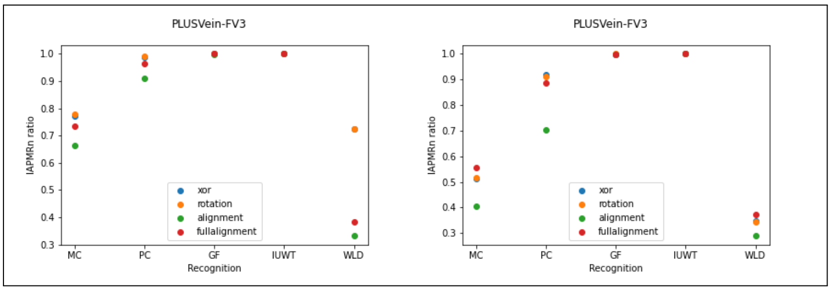

Fig. 9: PLUS dataset: IAPMR$_n$ results of all template types and morphing approaches in similar (up) and unsimilar (low) mode, respectively.

The last dataset we consider is the PLUS dataset as shown in Fig. 9. We notice that these data is most vulnerable to the attacks considered. In similar as well as in unsimilar template selection mode, IAPMR$_n$ of 0.9 - 1.0 is achieved for PC, GF, and IUWT template generation schemes. MC is still between 0.4 and 0.8 IAPMR$_n$ for all variants and only WLD exhibits some resistance against morphing attacks, still with an IAPMR$_n$ between 0.3 and 0.4 for all settings investigated.

Overall, it is difficult to identify overall trends. MC and WLD template generation techniques seem to be least subsceptible to the morphing attacks under investigation, but there is a clear interference between dataset properties and most vulnerable template generation scheme. While a best morphing approach is difficult to figure out, the Alignment approach is often seen as the worst performing one. In general, targeted template selection to identify the most similar doppelgänger template pays off in most cases.

4.2 Detecting Morphed Templates

This subsection deals with the vulnerability assessment of the database itself. As the logical OR operation used in all morphing approaches increases the number of white pixels, this number could serve as a simple criterion to identify morphed templates. We consider to following criterion for the number of white pixels (wPixels) with x serving as variable threshold.

$$\#wPixels \leq x \cdot StdDev(\#wPixels) + Mean(\#wPixels)$$

When applying this criterion with $x = 2$, the number of false positive morph detections is low for all template generation schemes (averaged across all datasets, compare Table 2: 4% - 5%).

	MC	PC	GF	IUWT	WLD
False positives	0.04	0.04	0.05	0.05	0.05

Table 2: The average probabilities across all datasets that a feature is falsely detected as morph at a threshold of $x = 2$.

On the other hand, the correct morph identification rate is very high for all template generation schemes as displayed in Table 3. For the XOR, Rotation and Falignment approaches we detect more than 0.96 of all morphs. This shows that we can easily identify morphs by looking at the number of white pixels. In contrast, morphs that we generate using the Alignment approach can “only” be identified with a probability of 0.66. This is due to the fact that in this technique, we only fuse the kernel with the input template which reduces the number of white pixels in the generated morph.

Approach	**MC**	**PC**	**GF**	**IUWT**	**WLD**
XOR	1.00	0.97	0.98	0.97	0.99
Rotation	1.00	0.97	0.98	0.98	0.99
Alignment	0.84	0.55	0.62	0.63	0.68
Full Alignment	1.00	0.93	0.93	0.94	0.98

Table 3: The probabilities across all datasets that a morph is correctly detected at a threshold of $x = 2$.

Based on these results, the database maintainer is able to run regular checks across the database to identify morphed templates of the type discussed. Therefore, the construction of morphed templates needs to be refined in order to mitigate the problems caused by the highly increased number of white pixels.

5 Conclusion & Future Work

We have investigated the feasibility of creating morphed templates for attacking finger vein recognition schemes by replacing templates in the database by morphed ones. A conducted vulnerability analysis reveals that (i) the extent of vulnerability and (ii) the type of most vulnerable template generation scheme depends on the employed sensor. We have also found that the similarity of the two templates involved in the morph is crucial, so a random selection should be avoided. The optimal method how to generate the morph for a given target template is also found to be sensor dependent. Thus, there is no general rule for an attacker how to conduct an attack of the described type, but for most sensor / template generation scheme we were able to identify a morphing scheme with a significant threat level.

Future work includes the refinement of the morphing techniques to avoid the considerable increase of white pixels (which can be exploited to identify morphed templates of the type discussed). Also the consideration of other template generation schemes, including deep-learning based ones, is of importance as the current investigation is restricted to binary template types.

Acknowledgements

This work has been partially funded by the Austrian Science Fund projects P32201 and I4232, respectively.

References

[1] Ferrara, M., Franco, A., Maltoni, D.: The magic passport. In: IEEE International Joint Conference on Biometrics. (Sept 2014) 1–7

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

[3] Venkatesh, S., Ramachandra, R., Raja, K., Busch, C.: Face morphing attack generation & detection: A comprehensive survey. IEEE Transactions on Technology and Society **2**(3) (2021) 128–145

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

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

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

[7] Makrushin, A., Trebeljahr, M., Seidlitz, S., Dittmann, J.: On feasibility of gan-based fingerprint morphing. In: 2021 IEEE 23rd International Workshop on Multimedia Signal Processing (MMSP). (2021) 1–6

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

[9] Sharma, R., Ross, A.: Image-level iris morph attack. In: 2021 IEEE International Conference on Image Processing (ICIP). (2021) 3013–3017

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

[11] Aydemir, A.K., Hämmerle-Uhl, J., Uhl, A.: Feasibility of morphing-attacks in vascular biometrics. In: 2021 IEEE/IAPR International Joint Conference on Biometrics (IJCB'21). (2021) 1–7

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

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

[14] 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)

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

[16] Asaari, M.S.M., S. A. Suandi, B.A.R.: Fusion of band limited phase only correlation and width centroid contour distance for finger based biometrics. Expert Systems with Applications **41**(7) (2014) 3367–3382

[17] Lu, Y., Xie, S.J., Yoon, S., Wang, Z., Park, D.S.: An available database for the research of finger vein recognition. In: Image and Signal Processing (CISP), 2013 6th International Congress on. Volume 1., IEEE (2013) 410–415

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

[19] Kauba, C., Prommegger, B., Uhl, A.: 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), Los Angeles, California, USA (2018) 1–9

[20] Kauba, C., Prommegger, B., Uhl, A.: Openvein - an open-source modular multipurpose finger vein scanner design. In Uhl, A., Busch, C., Marcel, S., Veldhuis, R., eds.: Handbook of Vascular Biometrics. Springer Nature Switzerland AG, Cham, Switzerland (2019) 77–111

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

[22] Kauba, C., Uhl, A.: An available open-source vein recognition framework. In Uhl, A., Busch, C., Marcel, S., Veldhuis, R., eds.: Handbook of Vascular Biometrics. Springer Nature Switzerland AG, Cham, Switzerland (2019) 113–142

[23] Huang, B., Dai, Y., Li, R., Tang, D., Li, W.: Finger-vein authentication based on wide line detector and pattern normalization. In: Pattern Recognition (ICPR), 2010 20th International Conference on, IEEE (2010) 1269–1272

[24] Starck, J., Fadili, J., Murtagh, F.: The undecimated wavelet decomposition and its reconstruction. IEEE Transactions on Image Processing **16**(2) (2007) 297–309

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

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