I. INTRODUCTION

Vein biometrics, as it is commonly referred to, describes the task of either identifying a person or verify a person’s claim of identity using a scan of their vascular pattern. The two most popular regions used in the context of vascular biometrics are the eye and hand regions [1]. According to [2], vein patterns from the following four locations are eligible options for hand-based vascular biometrics: Finger vein, palm vein, hand vein and wrist vein.

Since blood vessels are mostly hidden below the skin, and therefore hard to detect with the human visual system or consumer cameras, additional hardware is needed to make them visible. A relatively low-cost solution to do so is the usage of light in the near infrared region together with an infrared-sensitive imaging sensor. Since the hemoglobin in the blood absorbs light in this wavelength spectrum while surrounding tissues do not, the blood vessels appear as dark structures on the acquired images.

Despite the demand for additional hardware, vascular biometrics offers some advantages over more traditional ways of authentication in terms of security: Access tokens (such as keys, cards or badges) can be stolen, sweat on the fingertip leaves behind a latent fingerprint that can be reconstructed and the face is always exposed which makes it easy to capture. Therefore one would assume that vein biometrics is secure against attempted attacks, however German hackers [3] demonstrated at a hacking conference, that under the right circumstances hand vein structures can be captured even from a few meters distance. In addition to that they suggested that hand dryers in restrooms could potentially be manipulated to capture vein structures in the hand region. It has been shown in past research [4], [5] that without countermeasures, a simple print (e.g., using a laser printer) of such maliciously captured vein structures would suffice to fool a vein recognition system. Attacks of such kind are known as presentation attacks (PA). The ISO/IEC [6] defines presentation attacks as a presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system. This definition includes the intent to impersonate someone as well as the intent to conceal one's identity.

To counter such attacks, numerous research has been carried out over the last decade. A comprehensive overview of such is given in [7, Table 14.1], including handcrafted methods that employ image quality, generic texture and spatial frequency components as well as convolutional neural network based methods.

To further motivate research in this field and also to enable comparable and transparent results, publicly available attack databases, containing attack artefacts, are needed.

Currently, three finger vein attack databases and one palm vein attack database exist: The Idiap Research Institute VERA FingeVein Database (VeraFV) [8], the South China University of Technology Finger Vein Database (SCUT) [9], the Paris Lodron University of Salzburg Finger Vein Spoofing Data Set (PLUS) [10] and the The Idiap Research Institute VERA Spoofing PalmVein Database (VeraPV) [11]. All four are included in this work and therefore described in detail in Section II.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/
However, to actually demonstrate the effectiveness of created attack samples, only limited results are available in the literature. For doing this, one can utilize a so-called two-scenario-protocol or two-step-protocol, as described in Section III-A1. The outcome of this threat evaluation protocol is the percentage of attack samples that would be accepted by a given vein recognition system. For the VeraFV database, one recent publication [12] tests three vein recognition schemes (Wide Line Detector [13], Repeated Line Tracking [14] and Maximum Curvature [15]) using the two-step-protocol. In case of the SCUT, a publication [16] reports a pass rate, defined as successful attacks divided by the total attacks using a recognition method that is not further described. The publication that introduced the PLUS database contains a vulnerability analysis that employs twelve different finger vein recognition schemes in order to evaluate how hazardous the presentation attacks are from a broader perspective. The VeraPV database was evaluated on its introduction using the two-step-protocol on a local binary pattern [17] based feature extraction together with histogram intersection as biometric comparison technique.

Since every database was introduced with its own study to prove the actual success of created attacks, often with limited variability of confronted recognition schemes, this study aims to measure the threat potential in a comparable manor. To do so, an extensive collection of varying vein recognition schemes are employed to test all publicly available attack databases to perform a comprehensive threat evaluation.

A common strategy to increase vein recognition performance is to combine various recognition schemes that add complementary information (e.g., in [18]). Analogously, merging multiple attack detection schemes is used to improve the success rate of a single attack detection scheme, like in [19]. However, to combine the output of several recognition schemes in order to perform attack detection, is unexplored for the domain of unimodal hand-based vascular biometrics. Therefore, in this work, as a second step to the threat evaluation, biometric comparison scores from the threat assessment are utilized in order to perform presentation attack detection.

The content of this study constitutes an extension to the authors’ previous work [10], [20], [21] and can summarized as follows:

1) First, an extensive threat evaluation is carried out for all aforementioned attack databases. The goal is to measure the potential to deceive a real system by confronting 15 different vein recognition schemes that can be categorized into four classes of algorithms based on what type of feature they consider for classification.

2) Second, it is tested whether multiple similarity scores from vein recognition schemes generated in the first part could be fused in order to achieve presentation attack detection. To do so, exhaustive cross combination is carried out employing seven different fusion strategies together with six feature scaling approaches (including the possibility to omit feature scaling).

This article introduces the transfer of the threat evaluation from the finger vein databases assessed in our earlier conference publication [20] to the publicly available palm vein attack database mentioned earlier. In addition to that, a second convolutional neural network is added for the experiments in this article that employs a DenseNet architecture together with a softmax loss. Further differences to the reference work [20] include: two minutiae-based vein recognition schemes that constitute a fourth feature extraction category, two additional score-level-fusion strategies and three extra feature scaling approaches.

The remainder of this work is structured as follows: Section II describes all databases used throughout the experiments in this article. Section III explains the experimental setup for both, the threat evaluation as well as the presentation attack detection experiments. Section IV includes the experimental results and finally, Section V provides a summary of this work.

II. DATABASES

Four databases are included in this work which are presented in the following:

A) Paris Lodron University of Salzburg Palmar Finger Vein Spoofing Data Set (PLUS)\(^1\): The PLUS-FV3 Spoof data set uses a subset of the PLUS Vein-FV3 [22] database as bona fide samples. For the collection of presentation attack artefacts, binarized vein images from 6 fingers (i.e., index, middle and ring finger of both hands) of 22 subjects were printed on paper and sandwiched into a top and bottom made of beeswax. The binarization was accomplished by applying Principal Curvature [23] feature extraction in two different levels of vessel thickness, named thick and thin. The original database was captured with two types of light sources, namely LED and Laser. Therefore, presentation attacks were created for both illumination variants. While the original database was captured in 5 sessions per finger, only three of those were reused for presentation attack generation. Summarized, a total of 396 (22*6*3) presentation attacks per light source (LED & Laser) and vein thickness (thick & thin) with corresponding to 660 (22*6*5) bona fide samples are available. Every sample is of size 192 × 736.

B) The Idiap Research Institute VERA Fingervein Database (IDIAP VeraFV)\(^2\): The IDIAP VERA finger vein database consists of 440 bona fide images that correspond to 2 acquisition sessions of left and right hand index fingers of 110 subjects. Therefore these are considered as 220 unique fingers captured 2 times each. Every sample has one presentation attack counterpart. Presentation attacks are generated by printing preprocessed samples on high quality paper using a laser printer and enhancing vein contours with a black whiteboard marker afterwards. Every sample is provided in two modes named full and cropped. While the full set is comprised of the raw images captured with size 250 × 665, the cropped images were generated by removing a

\(^1\)https://wavelab.at/sources/PLUS-FV3-PALMAR-Image-Spoof/
\(^2\)https://www.idiap.ch/en/dataset/vera-fingervein
50 pixel margin from the border, resulting in images of size $150 \times 565$.

C) **South China University of Technology Spoofing Finger Vein Database (SCUT-SFVD)**$^3$: The SCUT-SFVD database was collected from 6 fingers (i.e., index, middle and ring finger of both hands) of 100 persons captured in 6 acquisition sessions, making a total of 3600 bona fide samples. For presentation attack generation, each finger vein image is printed on two overhead projector films which are aligned and stacked. In order to reduce over-exposure, additionally a strong white paper ($200\, \text{g/m}^2$) is put in-between the two overhead projector films. Similar to the IDIAP VERA database, the SCUT-SFVD is provided in two modes named *full* and *roi*. While in the full set every image sample has a resolution of $640 \times 288$ pixel, the samples from the roi set are of variable size. Since the LBP and the ASA VE matching algorithm can not be evaluated on variable sized image samples, a third set was generated for this study named *roi-resized* where all roi samples have been resized to $474 \times 156$ which corresponds to the median of all heights and widths from the roi set.

D) **The Idiap Research Institute VERA Spoofing Palmvein Database (IDIAP VeraPV)**$^4$: The bona fide samples used in the IDIAP Vera Spoofing Palmvein database descend from a palmvein database that was introduced at the same time. The palmvein database consists of 2200 images from 110 subjects where both hands were captured five times in two sessions. Attacks were created for all samples from the first 50 subjects. For the creation of the attack samples, one of the ten available samples per hand was chosen and after preprocessing is printed on 100g paper using a commercial ink printer. Every sample is available in a *raw* or *full* version and a region of interest (*roi*) version. The resolution of the *full* samples is $480 \times 640$ pixel. Similar to the SCUT-SFVD database, the *roi* samples are of variable size and are therefore resized to the median of all heights and widths from the roi image set for the experiments in this study: $273 \times 322$.

Fig. 1 shows an exemplary pair of images from each database. While the samples from the *full* versions of the databases often also include the contour of the finger or hand as well as some background, the *cropped* or *roi* versions tend to only show the parts that include vein structures. Since the process for creation of the SCUT, VeraFV and VeraPV databases includes a scan of a printed sample, the resulting presentation attacks show certain similarities to their bona fide counterparts. The *PLUS* attack samples, however, can potentially be distinguished from the bona fide samples even with the naked eye, which is owed to the process of creating these attack samples.

III. EXPERIMENTAL SETUP

In the following section the different experimental setups are described. First, the setup regarding the vulnerability assessment is elaborated, followed by a detailed description of the presentation attack detection experiments.

A. Threat Evaluation Setup

In order to get a broader view on what attack creation recipes are a threat to what systems, various feature extraction and comparison schemes are confronted with the attack
databases. In total, 15 different biometric vein recognition schemes are employed for the experiments. They can be categorized into four classes of algorithms based on the feature type extracted from the vein samples:

- **Binarized vessel networks:** Algorithms from this category work by transforming a raw vein image into a binary image where the background (and also other parts of the human body such as flesh) is removed and only the extracted vessel structures remain. The binarized image is then used as a feature image for the comparison step. Seven of such approaches are included in this work. *Maximum Curvature* (MC) [15] and *Repeated Line Tracking* (RLT) [14] try to achieve this by looking at the cross sectional profile of the finger vein image. Other methods such as *Wide Line Detector* (WLD) [13], *Gabor Filter* (GF) [24] and *Isotropic Undecimated Wavelet Transform* (IUWT) [25] also consider local neighbourhood regions by using filter convolution. A slightly different approach is given by *Principal Curvature* (PC) [23] which first computes the normalized gradient field and then looks at the eigenvalues of the Hessian matrix at each pixel. All so far described binary image extraction methods use a correlation measure to compare probe and template samples which is often referred to as *Miura-matching* due to its introduction in Miura et al. [14]. One more sophisticated vein pattern based feature extraction and matching strategy is *Anatomy Structure Analysis-Based Vein Extraction* (ASAVE) [26], which includes two different techniques for binary vessel structure extraction as well as a custom matching strategy.

- **Keypoints:** The term keypoint is generally understood as a specific pixel or pixel region in an digital image that provides some interesting information to a given application. Every keypoint is stored by describing its local neighbourhood and its location. This research uses three keypoint based feature extraction and matching schemes. One such keypoint detection method, known as *Deformation Tolerant Feature Point Matching* (DTFPM) [27], was especially tailored for the task of finger vein recognition. This is achieved by considering shapes that are common in finger vein structures. Additionally, modified versions of general purpose keypoint detection and matching schemes, *SIFT* and *SURF*, as described in [18] are tested in this research. The modification includes filtering such that only keypoints inside the finger are used while keypoints at the finger contours or even in the background are discarded.

- **Texture information:** Image texture is a feature that describes the structure of an image. Shapiro and Stockman [28] define image texture as something that gives information about the spatial arrangement of color or intensities in an image or selected region of an image. While two images can be identical in terms of their histograms, they can be very different when looking at their spatial arrangement of bright and dark pixels. Three methods are included in this work that can be counted to texture-based approaches. One of which is a *Local Binary Pattern* (LBP) [29] descriptor that uses the output of Gabor filters in various scales and orientations as an input. The resulting LBP are block-wise transformed into concatenated histograms. For comparison, histogram intersection is used as a similarity metric. The other two methods are convolutional neural network (CNN) based approaches. The first CNN approach (CNN-S) uses a Squeeze-Net architecture together with triplet loss function [30]. The second recognition approach employs a DenseNet-161 network architecture with soft-max loss function [31] (CNN-D). Similarity scores for the CNN approaches are obtained by computing the inverse Euclidean distance given two feature vectors corresponding to two finger vein samples.

- **Minutiae-based:** The term minutiae descends from the domain of fingerprint biometrics. Every fingerprint is a unique pattern that consists of ridges and valleys. The locations where such a pattern has discontinuities such as ridge endings or bifurcations are named “minutiae points”. This concept of finding such minutiae points was successfully transferred [32] to the vein biometrics domain by skeletonization of an extracted binarized vein image, such as described in the first category. This study now employs two schemes in order to perform
vein recognition, that both use these extracted minutiae points. First, the proprietary software VeriFinger SDK (VF)\(^5\) is used for comparison of these minutiae points. A second method, Location-based Spectral Minutiae Representation (SML) [33] uses the minutiae points as an input in order to generate a representation that can finally be compared using a correlation measure.

Fig. 2 shows the extracted features from one exemplary vein sample, stemming from the PLUS database. The ASAVE method extracts two feature representations, coined vein network and vein backbone, which are overlaid using white and gray, respectively, in order to fit the illustration. The LBP illustration shows four Gabor filter responses after applying the LBP algorithm. Since the output of the CNN based approaches is a vector embedding, such a visualization is not applicable. Acting as a representative for both minutiae schemes, a skeletonized finger vein structure is shown, where the minutiae point locations are marked with circles. Since the minutiae schemes are based on a binarized vessel network, their solidity depends on the robustness of the underlying procedure for extracting the vessel network.

Every vein recognition scheme has its own set of hyper-parameters. For the experiments in this work, the same settings were applied to every vein database.

The minutiae-based recognition schemes are evaluated using the VeinPLUS+ Framework [34]. The binary vessel network based methods, the keypoint based methods and the LBP scheme are evaluated using the PLUS OpenVein Toolkit [35]. The CNN approaches were implemented in Python. The network training for the PLUS databases was done using finger vein images from the PROTECT [36] open source data set, since these descend from a similar imaging sensor. The training for the VeraPV was achieved using the remaining bona fide subjects 51-110 that have no presentation attack counterpart. Network training for the remaining databases was done using 2-fold-cross validation. Due to the fact that such network training is non-deterministic, the EERs and IAPMRs for the CNN methods are calculated by taking the arithmetic mean over both folds.

For comparison the ‘FVC’ protocol, named after the Fingerprint Verification Contest 2004 [37] is used. With this protocol all samples are compared against all remaining samples descending from the same subject as genuine comparisons as given by equation (1). The number of genuine comparisons is denoted as \(n_{\text{genuine}}\), the number of impostor comparisons as \(n_{\text{impostor}}\) and the number of subjects as \(n_{\text{subjects}}\). For the case of finger vein data every individual finger is treated as unique subject, while for the palm vein data the term subject refers to a whole hand. For the formulas in this section, is assumed that every subject has the same number of samples \(n_{\text{samples}}\).

\[
n_{\text{genuine}} = \frac{n_{\text{samples}} \times (n_{\text{samples}} - 1)}{2} \times n_{\text{subjects}} \tag{1}
\]

For the Impostor comparisons, the FVC protocol defines that only the first sample of every subject is compared against the first of the remaining subjects. The number of impostor comparisons is given by equation (2) and only depends on the number of unique subjects regardless of the number of samples per subject.

\[
n_{\text{impostor}} = \frac{n_{\text{subjects}} \times (n_{\text{subjects}} - 1)}{2} \tag{2}
\]

Hence, it is ensured that every genuine comparison is made, but largely reduces the amount of impostor scores. Symmetric comparisons are omitted. It is important to note however that the correlation based comparison algorithm used for the binarized vessel network based approaches (Miura matching) is not symmetric.

1) Threat Evaluation Protocol: Biometric template comparison systems, which are basically binary classifiers, produce four types of outcome: (i) correct match (True Positive, TP), (ii) wrong rejection (False Negative, FN; often called type II error), (iii) correct rejection (True Negative, TN) and (iv) wrong match (False Positive, FP; often called type I error). The decision whether a comparison is considered to be a match or a reject is based on a decision threshold \(\tau\). Through varying the decision threshold, the False Match Rate (FMR, i.e., the ratio of wrongly accepted impostor attempts to the number of total impostor attempts) and the False-Non Match Rate (FNMR, i.e., the ratio of wrongly denied genuine attempts to the total number of genuine verification attempts) can be determined as seen in equations (3) and (4).

\[
FMR(\tau) = \frac{FP}{FP + TN} \tag{3}
\]

\[
FNMR(\tau) = \frac{FN}{FN + TP} \tag{4}
\]

The operating point where FMR = FNMR is called Equal Error Rate (EER) and its corresponding decision threshold value denoted as \(\tau_{\text{EER}}\).

A common way to evaluate the level of threat exhibited by a certain database is to use a so called two-scenario or two-step protocol [4], [5], [38]. The two steps are briefly summarized hereafter:

- **Scenario 1, Normal Mode:** The first scenario employs two types of users: Genuine (positives) and zero effort impostors (negatives). Therefore, both enrollment and verification is accomplished using bona fide finger vein samples. Through calculation of the FMR and FNMR, the EER can be computed and the decision threshold set at \(\tau_{\text{EER}}\). The normal mode can be understood as a biometric comparison evaluation experiment which has the goal to determine an operating point \(\tau_{\text{EER}}\) for the second scenario.

- **Scenario 2, Attack Mode:** The second scenario uses genuine (positives) and presentation attack (negatives) users. Similar to the first scenario, enrollment is accomplished using bona fide samples. This time, however, verification attempts are performed by comparing presentation attack samples against their corresponding genuine enrollment templates. Given the threshold determined in step 1, the proportion of wrongly matched presentation attacks is then reported as the Impostor Attack Presentation Match Rate (IAPMR), as defined in the ISO/IEC 30107-3:2017 [6].

---

\(^5\)https://www.neurotechnology.com/verifinger.html
B. Presentation Attack Detection Setup

Throughout the following section, genuine scores (i.e., scores that descend from intra-subject comparisons) are viewed as bona fide scores and scores that descend from comparisons where an attack sample is compared to its bona fide counterpart are considered to be presentation attack scores.

Solving the presentation attack problem via combination of multiple similarity scores from different recognition schemes can be formally written as follows. Let $s_{ij}$ be the $i$th comparison score out of $m$ total eligible comparisons that was assigned by the $j$th recognition scheme out of $n$ considered recognition schemes at a time, i.e., $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$. Note that for an $i$th comparison, every recognition scheme needs to compare the same biometric samples. Further, let $x_i$ be the vector $x_i = (s_{i1}, \ldots, s_{im})$ that describes the $i$th comparison by concatenation of all $n$ recognition schemes considered at a time. Let $X$ be the set of all $m$ eligible comparisons from a certain database $X = \{x_1, \ldots, x_m\}$. Since some of the following fusion strategies demand for training data, the set of all comparisons $X$ is always divided into a train $X_{train}$ and a test split $X_{test}$ using 2-fold cross validation. The combined score that remains after score level fusion for the $i$th comparison shall be denoted as $S_i$. The comparison can then be classified as bona fide or attack comparison by simple thresholding of $S_i$.

In total, seven score fusion strategies and six score normalization techniques are included in this study. Let $EER_j$ denote the Equal Error Rate estimate for recognition scheme $j$. This decision can be justified since $X_{train}$ consists of bona fide scores and presentation attack scores, therefore giving a rough estimate on how much a particular recognition scheme contributes to the PAD-task. The formula in equation (9) depicts the calculation of $w_j$.

$$w_j = \frac{1}{\sum_{v=1}^{n} EER_v}$$

In addition to the four fusion strategies above, three learning based classifiers are included in this study. The classifiers that are trained using $X_{train}$ in order to predict the test data $X_{test}$ per fold: (i) Linear Discriminant Analysis, (ii) Support Vector Machine with Linear Kernel and (iii) Support Vector Machine with Radial Basis Function Kernel.

A more sophisticated method, Weighted Sum-Rule Fusion, is defined in equation (8). Here every similarity score is multiplied by a weighting constant. The weights remain constant for all subjects, thus also known as “Matcher Weighting” [40]. All weights together form a convex combination, i.e., are non negative and add up to one.

- **Weighted Sum-Rule Fusion**

$$S_i = \sum_{j=1}^{n} s_{ij} \ast w_j$$  \hspace{1cm} \text{(8)}$$

To use the weighted sum rule fusion, a strategy has to be chosen on how to assign the weights $w_j$. Snelick et al. [40] propose to choose weights indirect proportional to the error rates. Hence, the training split $X_{train}$ is used to calculate an Equal Error Rate estimate $EER_j$ per recognition scheme $j$. This can be justified since $X_{train}$ consists of bona fide scores and presentation attack scores, therefore giving a rough estimate on how much a particular recognition scheme contributes to the PAD-task. The formula in equation (9) depicts the calculation of $w_j$. 

$$w_j = \frac{1}{\sum_{v=1}^{n} EER_v}$$

In addition to the four fusion strategies above, three learning based classifiers are included in this study. The classifiers that are trained using $X_{train}$ in order to predict the test data $X_{test}$. The weights remain constant for all subjects, thus also known as “Matcher Weighting” [40]. All weights together form a convex combination, i.e., are non negative and add up to one.

- **Weighted Sum-Rule Fusion**

$$S_i = \sum_{j=1}^{n} s_{ij} \ast w_j$$  \hspace{1cm} \text{(8)}$$
Bona Fide Presentation Classification Error Rate (BPCER): Proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario

\[ \text{BPCER}(\tau) = \frac{\text{FP}}{\text{FP} + \text{TN}} \]  

IV. EXPERIMENTAL RESULTS

Within this section, the experimental results for the threat evaluation and the presentation attack detection are described.

A. Threat Evaluation

The experiments carried out in this section aim to evaluate how harmful the attack recipes used for creation of the attack samples in the databases from Section II are. To do so, every database undergoes the threat evaluation protocol described in Section III-A1. The results from the threat evaluation experiments are listed in Table I. The dashed horizontal line is meant to separate finger vein and palm vein results. Note that for the PLUS LED and PLUS Laser databases, where different attacks descend from the same bona fide samples, the reported EER values for thin and thick are equal since the error rate calculation is solely based on bona fide data.

Using the same hyper-parameters per recognition scheme for every database makes the results more comparable, while performing an exhaustive grid search for every experiment could potentially lead to improved EER values. Lower EER values imply a better vein recognition performance. High IAPMR values indicate that a high proportion of the presented attack artifacts are wrongfully accepted.

1) Finger Veins: In general, binary vessel pattern based schemes tend to accept finger vein attack samples regardless of the used attack recipe. The highest IAPMR per database being 93.48% for the VeraFV, 86.33% for the SCUT and 89.54% for the PLUS databases. Effectively this means that in a real world scenario, without further attack detection measures, up to 9 out of 10 attack samples would be accepted. A change in comparison hyper parameter settings, namely allowing for vertical and horizontal translation during the “Miura matching” comparison step, reduced the EER values for the roi/cropped attack samples by up to 15%, compared to the reference work. As a consequence also the IAPMRs increased, now giving a clearer image on the threat that the roi samples pose to the binary vessel pattern based schemes. For the VeraFV database, authors from the same research institute that initially published the database, also reported in [12] EER and IAPMR values for three binarized vessel pattern based recognition algorithms. These can be used to verify that the hyper parameters used in the experiments in this work lead to comparable results within an acceptable range: MC (1-2% EER, 77-89% IAPMR), RLT (11-19% EER, 32-38% IAPMR) and WLD (3-7% EER, 70-80% IAPMR).

The general purpose keypoint scheme SIFT tends to be resistant against the PLUS attacks, while the other two finger vein databases seem to pose a threat, having IAPMRs ranging from 14% - 44%. The other general purpose keypoint recognition scheme, SURF, seems to be quite unimpressed
TABLE I
RESULTS THREAT EVALUATION USING 2-SCENARIO-PROTOCOL IN TERMS OF EER AND IAPMR. THE HORIZONTAL LINE SEPARATES FINGER VEIN (ABOVE DASHED LINE) AND PALM VEIN (BELOW DASHED LINE) EXPERIMENTS. VALUES IN %

|                  | MC  | PC  | GF  | IUWT | RLT  | WLD | ASAVE | DTFPM | SIFT | SURF | LBP  | CNN-S | CNN-D | SML | VF  |
|------------------|-----|-----|-----|------|------|-----|-------|-------|------|------|------|-------|-------|-----|-----|
| **PLUS LED Thick** |     |     |     |      |      |     |       |       |      |      |      |       |       |     |     |
| EER              | 0.60| 0.75| 1.06| 0.68 | 4.62 | 1.14| 2.35  | 2.35  | 1.06 | 3.33 | 3.86 | 2.90  | 1.97  | 2.79 | 0.80 |
| IAPMR            | 72.81| 69.93| 36.99| 79.08 | 40.65 | 69.15| 24.31 | 16.34 | 0.00 | 0.00 | 0.00 | 0.67  | 0.00  | 4.02 | 5.16 |
| **PLUS LED Thin** |     |     |     |      |      |     |       |       |      |      |      |       |       |     |     |
| EER              | 0.60| 0.75| 1.06| 0.68 | 4.62 | 1.14| 2.35  | 2.35  | 1.06 | 3.33 | 3.86 | 2.90  | 1.97  | 2.79 | 0.80 |
| IAPMR            | 89.65| 79.80| 59.72| 89.77 | 32.83 | 83.96| 19.07 | 15.78 | 0.00 | 0.00 | 0.25 | 0.35  | 0.00  | 5.87 | 5.24 |
| **PLUS Laser Thick** |     |     |     |      |      |     |       |       |      |      |      |       |       |     |     |
| EER              | 1.29| 1.65| 2.72| 1.97 | 6.21 | 2.80| 2.50  | 2.90  | 1.04 | 3.71 | 4.27 | 6.82  | 2.15  | 2.95 | 1.01 |
| IAPMR            | 59.90| 57.47| 31.55| 79.44 | 22.48 | 57.22| 9.07  | 4.98  | 0.00 | 0.00 | 0.00 | 0.00  | 0.00  | 2.67 | 6.54 |
| **PLUS Laser Thin** |     |     |     |      |      |     |       |       |      |      |      |       |       |     |     |
| EER              | 1.29| 1.65| 2.72| 1.97 | 6.21 | 2.80| 2.50  | 2.90  | 1.04 | 3.71 | 4.27 | 6.82  | 2.15  | 2.95 | 1.01 |
| IAPMR            | 76.52| 66.92| 52.65| 84.34 | 16.79 | 77.78| 2.02  | 5.18  | 0.13 | 0.00 | 0.00 | 0.05  | 0.00  | 3.60 | 5.62 |
| **Vera FV Full** |     |     |     |      |      |     |       |       |      |      |      |       |       |     |     |
| EER              | 2.66| 2.73| 6.83| 4.95 | 29.55| 6.03| 9.11  | 10.45 | 4.54 | 11.39| 8.17 | 6.35  | 7.73  | 6.69 | 4.04 |
| IAPMR            | 93.38| 90.45| 85.76| 93.18 | 35.00 | 93.48| 72.58 | 26.21 | 14.24| 0.91 | 16.97| 17.27 | 8.98  | 39.09| 21.67 |
| **Vera FV Cropped** |     |     |     |      |      |     |       |       |      |      |      |       |       |     |     |
| EER              | 5.52| 6.91| 11.56| 6.36 | 27.19| 9.09| 19.10 | 6.69  | 5.43 | 11.62| 5.80 | 9.93  | 10.91 | 17.27| 11.11 |
| IAPMR            | 92.27| 89.24| 81.97| 91.82 | 38.64 | 90.45| 68.79 | 81.97 | 44.55| 14.24| 69.09| 7.84  | 15.68 | 64.55| 21.97 |
| **SCUT Full**    |     |     |     |      |      |     |       |       |      |      |      |       |       |     |     |
| EER              | 4.01| 4.79| 9.40| 6.29 | 14.01| 7.60| 11.56 | 8.90  | 2.37 | 5.49 | 8.78 | 0.74  | 1.04  | 7.63  | 1.41 |
| IAPMR            | 86.33| 84.67| 54.90| 74.06 | 40.36 | 74.21| 74.98 | 73.75 | 30.43| 4.18 | 45.43| 68.65 | 28.53 | 59.76 | 32.90 |
| **SCUT ROI-Resized** |     |     |     |      |      |     |       |       |      |      |      |       |       |     |     |
| EER              | 2.28| 2.12| 3.52| 2.10 | 2.94 | 2.36| 6.03  | 5.63  | 1.92 | 9.41 | 3.51 | 0.84  | 1.33  | 7.25  | 3.78 |
| IAPMR            | 60.86| 47.95| 36.88| 49.85 | 9.46 | 52.49| 59.88 | 55.08 | 34.93| 7.42 | 55.36| 55.00 | 27.59 | 61.22 | 40.40 |
| **Vera PV Full** |     |     |     |      |      |     |       |       |      |      |      |       |       |     |     |
| EER              | 11.02| 16.70| 14.85| 18.23 | 27.20| 18.45| 17.20 | 7.26  | 1.39 | 4.18 | 17.32 | 6.24  | 3.29  | 15.64 | 2.56 |
| IAPMR            | 91.33| 65.71| 79.93| 70.73 | 85.24| 78.96| 77.33 | 84.93 | 54.80| 41.36| 75.76| 0.42  | 46.39 | 63.87 | 70.24 |
| **Vera PV ROI-Resized** |     |     |     |      |      |     |       |       |      |      |      |       |       |     |     |
| EER              | 1.44| 3.12| 4.03| 1.61 | 15.16| 4.57| 1.64  | 0.72  | 0.42 | 2.88 | 0.33 | 8.76  | 7.04  | 3.42  | 2.02 |
| IAPMR            | 56.05| 50.60| 42.31| 62.53 | 24.11| 47.87| 63.73 | 62.04 | 57.11| 35.22| 60.84 | 47.72 | 47.90 | 34.22 | 51.29 |
TABLE II

SELECTION OF BEST WORKING METHOD CONSTELLATIONS IN TERMS OF DETECTION ERROR RATE. NOTE THAT THERE ARE OFTEN MULTIPLE ELIGIBLE OPTIONS. ONLY THE CONSTELLATION THAT USES THE LEAST AMOUNT OF RECOGNITION SCHEMES AS POSSIBLE. VALUES IN %

| Database       | D-EER | BPCER20 | BPCER100 | Fusion    | Norm       | MC | PC | WLD | RCT | GF | IUWT | ASAVE | DTFM | SURF | SIFT | LBP | CNN-S | CNN-D | SML | VF |
|----------------|-------|---------|----------|-----------|------------|----|----|-----|-----|----|------|-------|------|------|------|-----|------|-------|-----|----|
| PLUS-LED thick| 0.00  | 0.00    | 0.00     | sum-rule-fusion | tanh-norm | ✓  | ✓  |     |     |    |      |       |      |      |     |     |      |       |     |
| PLUS-LED thin | 0.00  | 0.00    | 0.00     | max-rule-fusion | no-norm   | ✓  | ✓  |     |     |    |      |       |      |      |     |     |      |       |     |
| PLUS-Laser thick| 0.00 | 0.00    | 0.00     | sum-rule-fusion | no-norm   | ✓  | ✓  |     |     |    |      |       |      |      |     |     |      |       |     |
| PLUS-Laser thin| 0.00 | 0.00    | 0.00     | sum-rule-fusion | min-max-norm | ✓  | ✓  |     |     |    |      |       |      |      |     |     |      |       |     |
| VERA-FV full  | 0.91  | 0.45    | 0.91     | svm-fusion-lin | rhe-norm  | ✓  | ✓  | ✓   | ✓   | ✓  |      | ✓     |     |     |     |     |      |     |
| VERA-FV cropped| 3.18 | 2.73    | 12.73    | svm-fusion-lin | rhe-norm  | ✓  | ✓  | ✓   | ✓   | ✓  | ✓     | ✓     |     |     |     |     |      |     |
| SCUT full     | 0.42  | 0.09    | 0.27     | svm-fusion-lin | min-max-norm | ✓  | ✓  | ✓   | ✓   | ✓  | ✓     | ✓     |     |     |     |     |      |     |
| SCUT roi-resized| 0.92 | 0.40    | 0.89     | svm-fusion-rbf | tanh-norm | ✓  | ✓  | ✓   | ✓   | ✓  | ✓     | ✓     |     |     |     |     |      |     |
| VERA-PV full  | 1.09  | 0.82    | 1.09     | svm-fusion-lin | z-norm    | ✓  | ✓  | ✓   | ✓   | ✓  |      | ✓     |     |     |     |     |      |     |
| VERA-PV roi-resized| 1.46 | 0.76    | 1.93     | svm-fusion-lin | z-norm    | ✓  | ✓  | ✓   | ✓   | ✓  | ✓     | ✓     |     |     |     |     |      |     |

Indication of used recognition schemes:

- ✓: Present
- ✓: Present

The PAD performance is reported in Table II in terms of detection equal error rate D-EER (operating point where BPCER = APCER), BPCER20 (BPCER at APCER <= 0.05) and BPCER100 (BPCER at APCER <= 0.01).

For every database, an exhaustive cross combination including all the described fusion strategies, normalization techniques and recognition algorithms is applied. This results in 7 (fusion) * 6 (normalization) * 32 767 (2^15 – 1, all possible combinations of the 15 recognition algorithms) = 1 376 214 D-EER values per database. The results reported in Table II are the best working constellation for a given database in terms of D-EER, that is, if a single best constellation exists. For the case where multiple method constellations result in the same D-EER (especially the PLUS databases tend to have many solutions that would yield 0.00% D-EER, i.e., perfect separation), the method constellation is reported that uses as the least amount of feature extraction schemes as possible. The employed recognition schemes for the best working constellation are indicated using a check symbol. The fact that the PLUS databases are well separable also coincides with the observation from Section IV-A, where the PLUS samples were only a major threat to one category of recognition algorithms (the ones that extract binary images of vessel structures as feature images). This can be explained by the visual difference as seen in Fig. 1, which is due to the process used to create these kind of attack samples.

For further analyzing the contribution of every recognition scheme, fusion strategy and score normalization method, the following figures depict their relative occurrence in the best working constellations. For better visibility which methods provide the most valuable information, only those method constellations which yield D-EERs < 5% are considered. To keep the plots easy to interpret, the databases are split into PLUS databases (Figs. 6 and 7) and the rest (Figs. 4 & 5).

It is important to note that for the PLUS databases, roughly 95% of all 1 376 214 method constellations would be included within the 5% D-EER threshold, resulting in mostly uniform distributions. Therefore, the threshold for the PLUS databases was reduced to D-EERs < 0.5%, where a subset of roughly 13% out of all method constellations remain.

It can be concluded that through combination of fundamentally different approaches, complementary information is available that finally leads to the ability to reasonably well detect presentation attacks. While perfect separation of bona fide and attack samples is not always achieved, using a combination of multiple recognition schemes for this task constitutes a method that has not been explored so far in the domain of hand-vascular biometrics. Of course, however, by doing so, the ability to detect presentation attacks is limited by the performance of the considered recognition schemes, which could potentially be improved by exhaustive hyper parameter optimization.
V. Summary

The present article first analyzed public finger and palm vein attack databases on their potential to deceive state of the art vein recognition algorithms. As a second step, it was tested whether a fusion of recognition algorithms could be employed in order to achieve presentation attack detection.
The first part of this research employed a common threat evaluation protocol, known as 2-step-protocol, in order to make results more comparable. To get a broader perspective on the attack potential, 15 distinct vein recognition algorithms are confronted with the attacks that can be categorized into four meta categories of algorithms based on what type of feature they extract from the vein samples. Evaluation results show that recognition algorithms that extract binary images from the blood vessel patterns as a feature image are susceptible to all of the attack types. The other feature types, i.e., texture based approaches, minutiae based approaches and key-point based approaches are only somewhat susceptible to the VeraFV, SCUT and VeraPV attack samples.

In the second part of this research, it is tested whether similarity scores that were generated in the course of the threat evaluation could be combined using score-level-fusion in order to thwart the attacks. To do so, exhaustive cross combination of all recognition schemes together with seven fusion strategies and six score normalization techniques was carried out. Experimental results show that indeed a sound attack detection can be achieved with this strategy.

REFERENCES
[1] A. Uhl, “State of the art in vascular biometrics,” in Handbook of Vascular Biometrics, A. Uhl, C. Busch, S. Marcel, and R. Veldhuis, Eds. Cham, Switzerland: Springer Int., 2020, pp. 3–61. [Online]. Available: https://doi.org/10.1007/978-3-030-27731-4_1
[2] A. Uhl, “Hand-based vascular patterns,” in Encyclopedia of Cryptography, Security and Privacy, S. Jajodia, P. Samarati, and M. Yung, Germany: Springer, 2021, pp. 1–5.
[3] J. Krissler and Julian. “Venenerkennung hacken—Vom fall der letzten bastion biometrischer Systeme.” Chaos Computer Club e.V. 2018. [Online]. Available: https://doi.org/10.5446/39201
[4] P. Tome, M. Vanoni, and S. Marcel, “On the vulnerability of fingerprint vein recognition to spoofing,” in Proc. Int. Conf. Biometrics Spec. Interest Group (BISIG), 2014, pp. 1–10.
[5] I. Patil, S. Bhilare, and V. Kanhangad, “Assessing vulnerability of dorsal hand-vein verification system to spoofing attacks using smartphone camera,” in Proc. IEEE Int. Conf. Identity Security Behav. Anal. (ISBA), 2016, pp. 1–6.
[6] ISO/IEC JTC 1/SC 37 37 Biometrics, Information Technology—Biometric Presentation Attack Detection—Part 3: Testing and Reporting, Standard ISO/IEC 30107-3:2017, 2017. [Online]. Available: https://www.iso.org/standard/67381.html
[7] J. Kolberg, M. Gomes-Barrero, S. Venkatesh, R. Ramachandra, and C. Busch, Presentation Attack Detection for Fingerprint Recognition, Cham, Switzerland: Springer Int., 2020, pp. 435–463. [Online]. Available: https://doi.org/10.1007/978-3-030-27731-4_14
[8] P. Tome et al., “The 1st competition on counter measures to fingerprint vein spoofing attacks,” in Proc. Int. Conf. Biometrics (ICB), 2015, pp. 513–518.
[9] X. Qiu, W. Kang, S. Tian, W. Jia, and Z. Huang, “Finger vein presentation attack detection using total variation decomposition,” IEEE Trans. Inf. Forensics Security, vol. 13, pp. 465–477, 2018.
[10] J. Schuiki, B. Prommegger, and A. Uhl, “Confronting a variety of fingerprint vein recognition algorithms with wax presentation attack artefacts,” in Proc. 9th IEEE Int. Workshop Biometrics Forensics (IWBF), Rome, Italy, 2021, pp. 1–6.
[11] D. Court and S. Marcel, “On the vulnerability of palm vein recognition to spoofing attacks,” in Proc. Int. Conf. Biometrics (ICB), 2015, pp. 319–325.
[12] A. Anjos, P. Tome, and S. Marcel, “An introduction to vein presentation attacks and detection,” in Handbook of Biometric Anti-Spoofing: Presentation Attack Detection, S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, Eds. Cham, Switzerland: Springer Int., 2019, pp. 419–438.
[13] B. Huang, Y. Dai, R. Li, D. Tang, and W. Li, “Finger-vein authentication based on wide line detector and pattern normalization,” in Proc. 20th Int. Conf. Pattern Recognit., 2010, pp. 1269–1272.
[14] N. Miura, A. Nagasaka, and T. Miyatake, “Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification,” Mach. Vis. Appl., vol. 15, pp. 194–203, Oct. 2004.
[15] N. Miura, A. Nagasaka, and T. Miyatake, “Extraction of finger-vein patterns using maximum curvature points in image profiles,” IEICE Trans. Inf. Syst., vol. E90-D, pp. 1185–1189, Aug. 2007.
[16] W. Yang, W. Luo, W. Kang, Z. Huang, and Q. Wu, “FVRAS-net: An embedded finger-vein recognition and AntiSpoofing system using a unified CNN,” IEEE Trans. Instrum. Meas., vol. 69, no. 11, pp. 8690–8701, Nov. 2020.
[17] L. Mirrhomahadsadeghi and A. Drygajlo, “Palm vein recognition with local texture patterns,” IET Biometrics, vol. 3, no. 4, pp. 198–206, Dec. 2014. [Online]. Available: https://www Instit. 2013.0041
[18] C. Kauba, J. Reissig, and A. Uhl, “Pre-processing cascades and fusion in finger vein recognition,” in Proc. Int. Conf. Biometrics Spec. Interest Group (BISIG), Darmstadt, Germany, Sep. 2014, pp. 1–6.
[19] J. M. Singh, S. Venkatesh, K. B. Raja, R. Ramachandra, and C. Busch, “Detecting finger-vein presentation attacks using 3D shape & diffuse reflectance decomposition,” in Proc. 15th Int. Conf. Signal-Image Technol. Internet-Based. Syst. (SITIS), 2009, art. no. 725111. [Online]. Available: https://doi.org/10.1109/SITIS.2009.22
[20] A. Kumar and Y. Zhou, “Human identification using finger images,” IEEE Trans. Image Process., vol. 21, pp. 2228–2244, 2012.
[21] J.-L. Starck, J. Fadili, and F. Murtagh, “The undecimated wavelet decomposition and its reconstruction,” IEEE Trans. Image Process., vol. 16, pp. 297–309, 2007.
[22] C. Kauba, B. Prommegger, and A. Uhl, “Focussing the beam—A new laser illumination based data set providing insights to finger-vein recognition,” in Proc. IEEE 9th Int. Conf. Biometrics Theory Appl. Syst. (BTAS), Los Angeles, CA, USA, 2018, pp. 1–9.
[23] J. H. Choi, W. Song, T. Kim, S.-R. Lee, and H. C. Kim, “Finger vein extraction using gradient normalization and principal curvature,” in Proc. Image Process. Mach. Vis. Appl. II, 2009, art. no. 725111. [Online]. Available: https://doi.org/10.1109/112.810458
[24] A. Kumar and Y. Zhou, “Human identification using finger images,” IEEE Trans. Image Process., vol. 21, pp. 2228–2244, 2012.
[25] C. Kauba, B. Prommegger, and A. Uhl, “Extensive threat analysis of vein attack databases and attack detection by fusion of comparison scores,” 2020. [Online]. Available: https://doi.org/10.1049/iet-bmt.2013.0041
[26] M. Linortner and A. Uhl, “VeinPLUS++, A. Uhl, C. Busch, S. Marcel, and R. Veldhuis, Eds. Cham, Switzerland: Springer Int., 2019, ch. 3, pp. 77–111.
[36] A. F. Sequeira et al., “PROTECT multimodal DB: A multimodal biometrics dataset envisaging border control,” in Proc. Int. Conf. Biometrics Spec. Interest Group (BIOSIG), Darmstadt, Germany, 2018, pp. 1–8. [Online]. Available: https://doi.org/10.23919/BIOSIG.2018.8552926

[37] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, “FVC2004: Third fingerprint verification competition,” in Biometric Authentication, D. Zhang and A. K. Jain, Eds. Berlin, Germany: Springer, 2004, pp. 1–7.

[38] I. Chingovska, A. Mohammadi, A. Anjos, and S. Marcel, “Evaluation methodologies for biometric presentation attack detection,” in Handbook of Biometric Anti-Spoofing: Presentation Attack Detection, S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, Eds. Cham, Switzerland: Springer Int., 2019, pp. 457–480. [Online]. Available: https://doi.org/10.1007/978-3-319-92627-8_20

[39] R. Snelick, M. Indovina, J. Yen, and A. Mink, “Multimodal biometrics: Issues in design and testing,” in Proc. 5th Int. Conf. Multimodal Interfaces, New York, NY, USA, 2003, pp. 68–72. [Online]. Available: https://doi.org/10.1145/958432.958447

[40] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. Jain, “Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 3, pp. 450–455, Mar. 2005.

[41] A. Jain, K. Nandakumar, and A. Ross, “Score normalization in multimodal biometric systems,” Pattern Recognit., vol. 38, no. 12, pp. 2270–2285, 2005.

[42] M. He et al., “Performance evaluation of score level fusion in multimodal biometric systems,” Pattern Recognit., vol. 43, no. 5, pp. 1789–1800, 2010.

Johannes Schuiki received the M.Sc. degree in applied image and signal processing from the University of Salzburg and Salzburg University of Applied Sciences in 2022. He is currently pursuing the Ph.D. degree with the Department of Artificial Intelligence and Human Interfaces, University of Salzburg, where he is working as a Research Assistant. His main research interest lies in vascular biometrics, especially in the hand region, including vein recognition and vein presentation attack detection.

Michael Linortner received the DI (Austrian equivalent to M.Sc.) degree in information technology and systems management from the Salzburg University of Applied Sciences in 2017, and the M.Sc. degree in applied image and signal processing from the University of Salzburg and Salzburg University of Applied Sciences in 2021. He is currently working as a Research Assistant with the Department of Artificial Intelligence and Human Interfaces, University of Salzburg. His main research interest is in vascular biometrics, especially finger vein biometrics.

Georg Wimmer is a Postdoctoral Researcher with the Paris Lodron University of Salzburg and is part of the “Multimedia Signal Processing and Security” Group led by Prof. A. Uhl. Research has been done in the areas of biometrics and medical image analysis. His current works is focused on finger vein recognition and other biometric related applications.

Andreas Uhl is a Professor with the Department of Artificial Intelligence and Human Interfaces, University of Salzburg, where he heads the Multimedia Processing and Security Lab. His research interests include image and video processing and compression, wavelets, media security, medical imaging, biometrics, and number-theoretical numerics.