Vulnerability Assessment and Presentation Attack Detection Using a Set of Distinct Finger Vein Recognition Algorithms

Johannes Schuiki, Georg Wimmer, and Andreas Uhl

University of Salzburg
Department of Computer Sciences

IJCB'21
Paper #0152

The Presentation Attack Problem

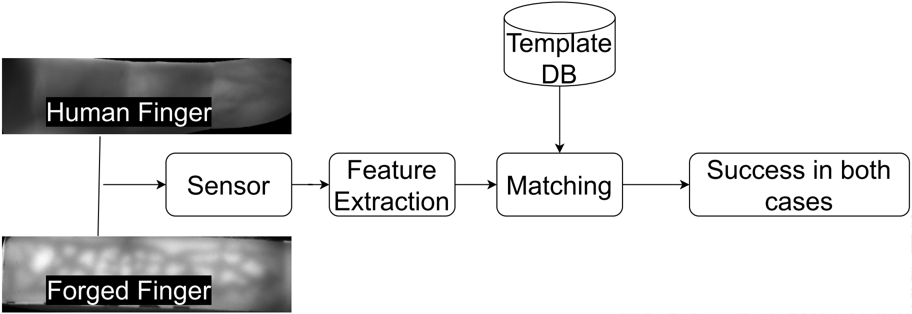


Figure: Block diagram visualisation of presentation attack problem

This Talk

- 3 Finger vein attack data sets
  - Paris Lodron University of Salzburg Finger Vein Spoofing Data Set (**PLUS-LED** and **PLUS-Laser**) [1]
  - The Idiap Research Institute VERA Fingervein Database (**IDIAP VERA**) [2]
  - South China University of Technology Spoofing Finger Vein Database (**SCUT-SFVD**) [3]
- Extensive threat analysis using 12 finger vein recognition schemes
- Presentation attack detection by fusion of similarity scores

Metrics

- False Match Rate (FMR)

$$FMR = \frac{\textit{accepted impostor attempts}}{\textit{all impostor attempts}}$$

- False Non Match Rate (FNMR)

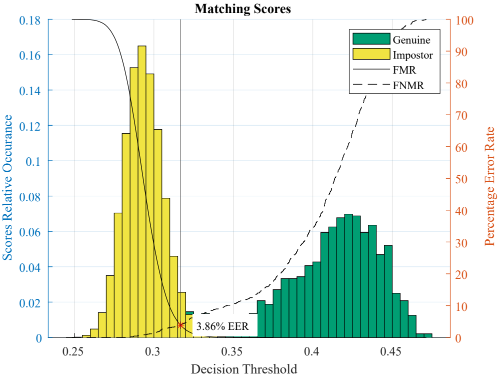
$$FNMR = \frac{\textit{denied genuine attempts}}{\textit{all genuine attempts}}$$

- Equal Error Rate (EER)

$$EER = \textit{Operating point where } FMR = FNMR$$

- Impostor Attack Presentation Match Rate (IAPMR)

$$IAPMR = \frac{\textit{accepted attack attempts}}{\textit{all attack attempts}}$$



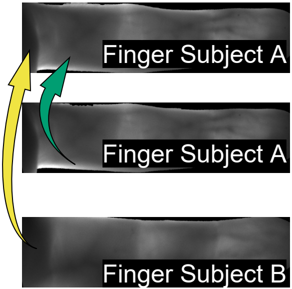
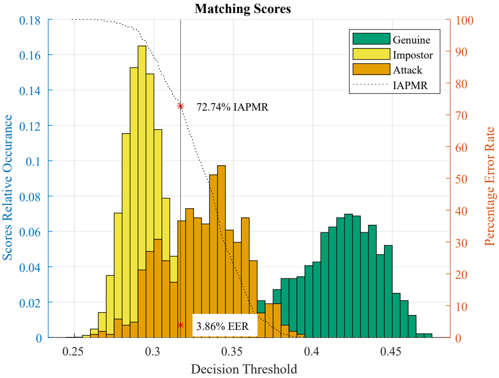


Figure: Step 1



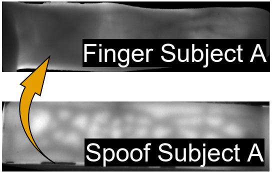
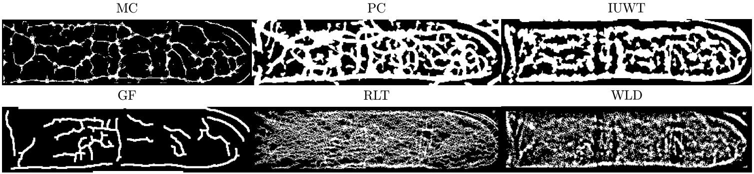


Figure: Step 2

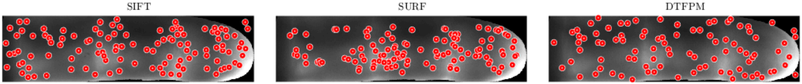
- Binarized Vessel Network
  - Maximum Curvature (MC) [4]
  - Principal Curvature (PC) [5]
  - Wide Line Detector (WLD) [6]
  - Repeated Line Tracking (RLT) [7]
  - Gabor Filters (GF) [8]
  - Isotropic Undecimated Wavelet Transform (IUWT) [9]
  - Anatomy Structure Analysis-Based Vein Extraction (ASAVE) [10]

Figure: Binarized Vessel Networks



- Binarized Vessel Network
  - Maximum Curvature (MC) [4]
  - Principal Curvature (PC) [5]
  - Wide Line Detector (WLD) [6]
  - Repeated Line Tracking (RLT) [7]
  - Gabor Filters (GF) [8]
  - Isotropic Undecimated Wavelet Transform (IUWT) [9]
  - Anatomy Structure Analysis-Based Vein Extraction (ASAVE) [10]
- Keypoints
  - Scale Invariant Feature Transform (SIFT) based [11]
  - Speeded Up Robust Features (SURF) based [11]
  - Deformation Tolerant Feature Point Matching (DTFPM) [12]

Figure: Keypoints



Feature Extraction Algorithms

- Binarized Vessel Network
  - Maximum Curvature (MC) [4]
  - Principal Curvature (PC) [5]
  - Wide Line Detector (WLD) [6]
  - Repeated Line Tracking (RLT) [7]
  - Gabor Filters (GF) [8]
  - Isotropic Undecimated Wavelet Transform (IUWT) [9]
  - Anatomy Structure Analysis-Based Vein Extraction (ASAVE) [10]
- Keypoints
  - Scale Invariant Feature Transform (SIFT) based [11]
  - Speeded Up Robust Features (SURF) based [11]
  - Deformation Tolerant Feature Point Matching (DTFPM) [12]
- Texture
  - Local Binary Pattern & Histogram Intersection (LBP) [13]
  - Convolutional Neural Network trained using triplet loss (CNN) [14] [1]

[1] Everything except CNN used matching implementation from OpenVein-Toolkit [15]

PLUS-LED and PLUS-Laser Generation [1]

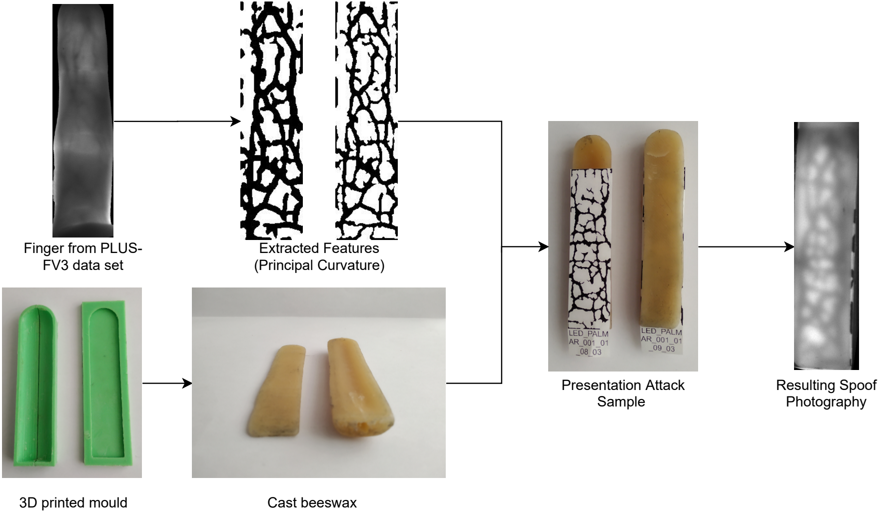


Figure: Presentation Attack generation from [1].

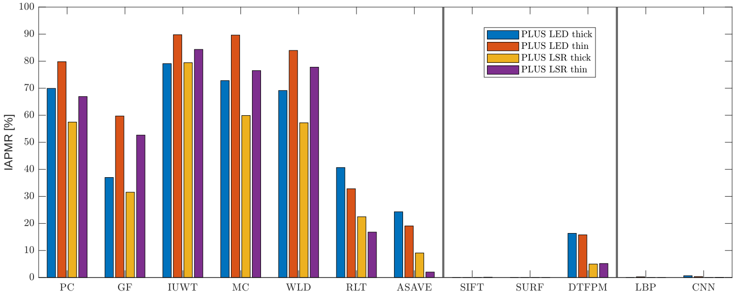


Figure: Results IAPMR PLUS LED and Laser

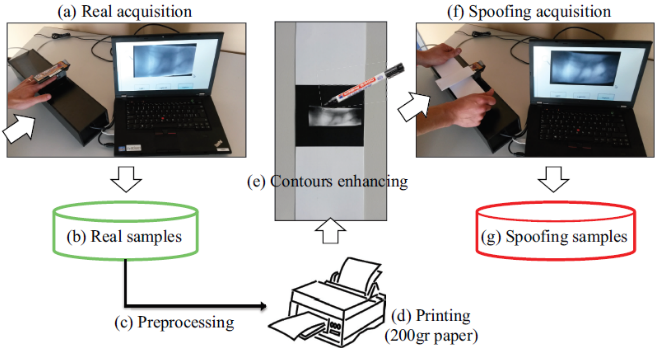


Figure: Presentation Attack generation flow diagram (screenshot from Tome et al. [2]) IDIAP database.

Threat Analysis: IDIAP VERA

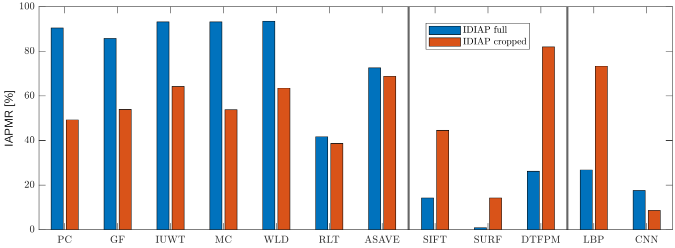


Figure: Results IAPMR IDIAP full and cropped

SCUT-SFVD Generation and Examples

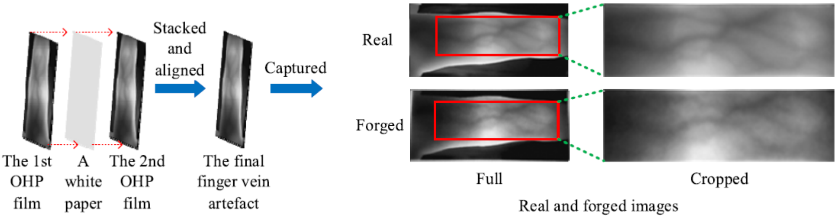


Figure: Presentation Attack generation (screenshot from Qiu et al. [3]) SCUT-SFVD database.

Threat Analysis: SCUT-SFVD

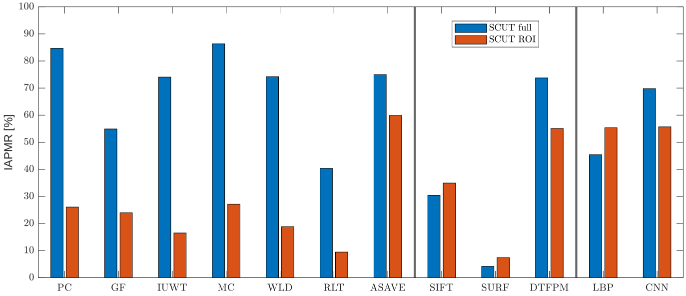


Figure: Results IAPMR SCUT full and cropped

Threat Analysis: Overview

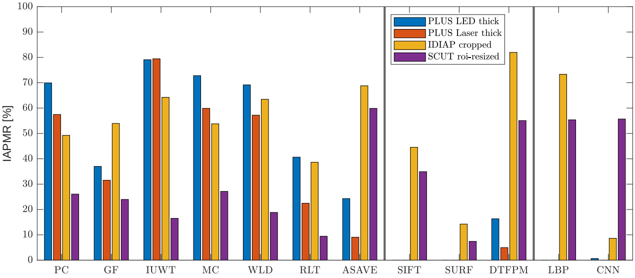


Figure: Overview IAPMRs; one case of every DB

Similarity Score Fusion Strategies

- *Sum-Rule Fusion*

$$f = \sum_{i=1}^{N} S_i \quad (1)$$

- *Min-Rule Fusion*

$$f = min(S_1, ..., S_N) \quad (2)$$

- *Max-Rule Fusion*

$$f = max(S_1, ..., S_N) \quad (3)$$

- *Support Vector Machine with linear and rbf kernel*

$$\vec{x} = (S_1, ..., S_N) \quad (4)$$

f ... fusioned score, S_i *... similarity score of recognition scheme i*

Score Normalisation

- *no-norm*

$$\textit{No normalisation applied} \tag{5}$$

- *z-norm*

$$S' = \frac{S - \mu}{\sigma} \tag{6}$$

- *tanh-norm*

$$S' = 0.5 * \left(tanh \left(0.01 * \frac{S - \mu}{\sigma} \right) + 1 \right) \tag{7}$$

Spoof Detection Metrics

- Attack Presentation Classification Error Rate (APCER)

$$APCER = \frac{spoof\ attempts\ classified\ as\ real\ finger\ attempts}{all\ spoof\ attempts}$$

- Bona Fide Presnetation Classification Error Rate (BPCER)

$$BPCER = \frac{real\ finger\ attmepts\ classified\ as\ spoof}{all\ real\ finger\ attempts}$$

- Detection - Equal Error Rate (D-EER)

$$D - EER = Point\ where\ APCER = BPCER$$

Best Reuslts

Database	D-EER	Fusion	Norm	MC	PC	WLD	RLT	GF	IUWT	ASAVE	DTFPM	SURF	SIFT	LBP	CNN
IDIAP VERA full	1.67	svm-lin	z-norm			✓				✓	✓	✓	✓	✓	✓
IDIAP VERA cropped	4.02	svm-lin	z-norm		✓			✓		✓	✓	✓	✓		✓
SCUT-SFVD full	0.75	svm-rbf	z-norm	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓
SCUT-SFVD roi-resized	1.09	svm-rbf	tanh-norm		✓		✓			✓		✓	✓	✓	✓
PLUS-LED thick	0.00	svm-rbf	z-norm										✓		✓
PLUS-LED thin	0.00	svm-lin	tanh-norm									✓	✓	✓	
PLUS-Laser thick	0.00	svm-lin	z-norm										✓		✓
PLUS-Laser thin	0.00	svm-lin	z-norm		✓						✓		✓		✓

Table: Selection of best working method constellations in terms of D-EER

Summary:

- 3 FV attack datasets were tested on threat they pose to 12 recognition algorithms; Similarity scores of matching experiments were used for score level fusion to achieve spoof detection.

Lessons learned:

- Every evaluated data sets poses a threat to at least some recognition schemes. However SURF seems to be overall very resistant to spoofing.
- We can combine similarity scores of different recognition schemes to achieve spoof detection (at least to some degree).

Thank You!
Q & A

[1] 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)*, (Rome, Italy (moved to virtual)), pp. 1–6, 2021.

[2] P. Tome, M. Vanoni, and S. Marcel, “On the vulnerability of finger vein recognition to spoofing,” in *2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pp. 1–10, 2014.

[3] X. Qiu, S. Tian, W. Kang, W. Jia, and Q. Wu, “Finger vein presentation attack detection using convolutional neural networks,” in *Biometric Recognition* (J. Zhou, Y. Wang, Z. Sun, Y. Xu, L. Shen, J. Feng, S. Shan, Y. Qiao, Z. Guo, and S. Yu, eds.), (Cham), pp. 296–305, Springer International Publishing, 2017.

[4] 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, p. 1185–1194, Aug. 2007.

[5] 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*, vol. 7251, pp. 7251 – 7251 – 9, 2009.

[6] B. Huang, Y. Dai, R. Li, D. Tang, and W. Li, “Finger-vein authentication based on wide line detector and pattern normalization,” in *2010 20th International Conference on Pattern Recognition*, pp. 1269–1272, 2010.

[7] N. Miura, A. Nagasaka, and T. Miyatake, “Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification,” *Machine Vision and Applications*, vol. 15, pp. 194–203, 10 2004.

[8] A. Kumar and Y. Zhou, “Human identification using finger images,” *IEEE Transactions on Image Processing*, vol. 21, no. 4, pp. 2228–2244, 2012.

[9] J. Starck, J. Fadili, and F. Murtagh, “The undecimated wavelet decomposition and its reconstruction,” *IEEE Transactions on Image Processing*, vol. 16, no. 2, pp. 297–309, 2007.

[10] L. Yang, G. Yang, Y. Yin, and X. Xi, “Finger vein recognition with anatomy structure analysis,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 8, pp. 1892–1905, 2018.

[11] C. Kauba, J. Reissig, and A. Uhl, “Pre-processing cascades and fusion in finger vein recognition,” in *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG’14)*, (Darmstadt, Germany), Sep. 2014.

[12] Y. Matsuda, N. Miura, A. Nagasaka, H. Kiyomizu, and T. Miyatake, “Finger-vein authentication based on deformation-tolerant feature-point matching,” *Machine Vision and Applications*, vol. 27, 02 2016.

[13] E. C. Lee, H. C. Lee, and K. R. Park, “Finger vein recognition using minutia-based alignment and local binary pattern-based feature extraction,” *Int. J. Imaging Syst. Technol.*, vol. 19, p. 179–186, Sept. 2009.

[14] G. Wimmer, B. Prommegger, and A. Uhl, “Finger vein recognition and intra-subject similarity evaluation of finger veins using the cnn triplet loss,” in *Proceedings of the 25th International Conference on Pattern Recognition (ICPR)*, pp. 400–406, 2020.

[15] C. Kauba, B. Prommegger, and A. Uhl, “Openvein - an open-source modular multipurpose finger vein scanner design,” in *Handbook of Vascular Biometrics* (A. Uhl, C. Busch, S. Marcel, and R. Veldhuis, eds.), ch. 3, pp. 77–111, Cham, Switzerland: Springer Nature Switzerland AG, 2019.