Analysis of Master Vein Attacks on Finger Vein Recognition Systems

Inter-University Research Institute Corporation / Research Organization of Information and Systems
National Institute of Informatics

Email: nhhuy@nii.ac.jp

Huy H. Nguyen[1], Trung-Nghia Le[1], Junichi Yamagishi[1], and Isao Echizen[1,2]

[1]National Institute of Informatics, Japan [2]The University of Tokyo Japan

WACV WAIKOLOA HAWAII JAN 3-7 • 2023

Introduction

Source: CNN

- Finger vein recognition systems (FVRS) have been deployed in ATMs.
- Some systems use hand-crafted features and do not have proper presentation attack detectors.

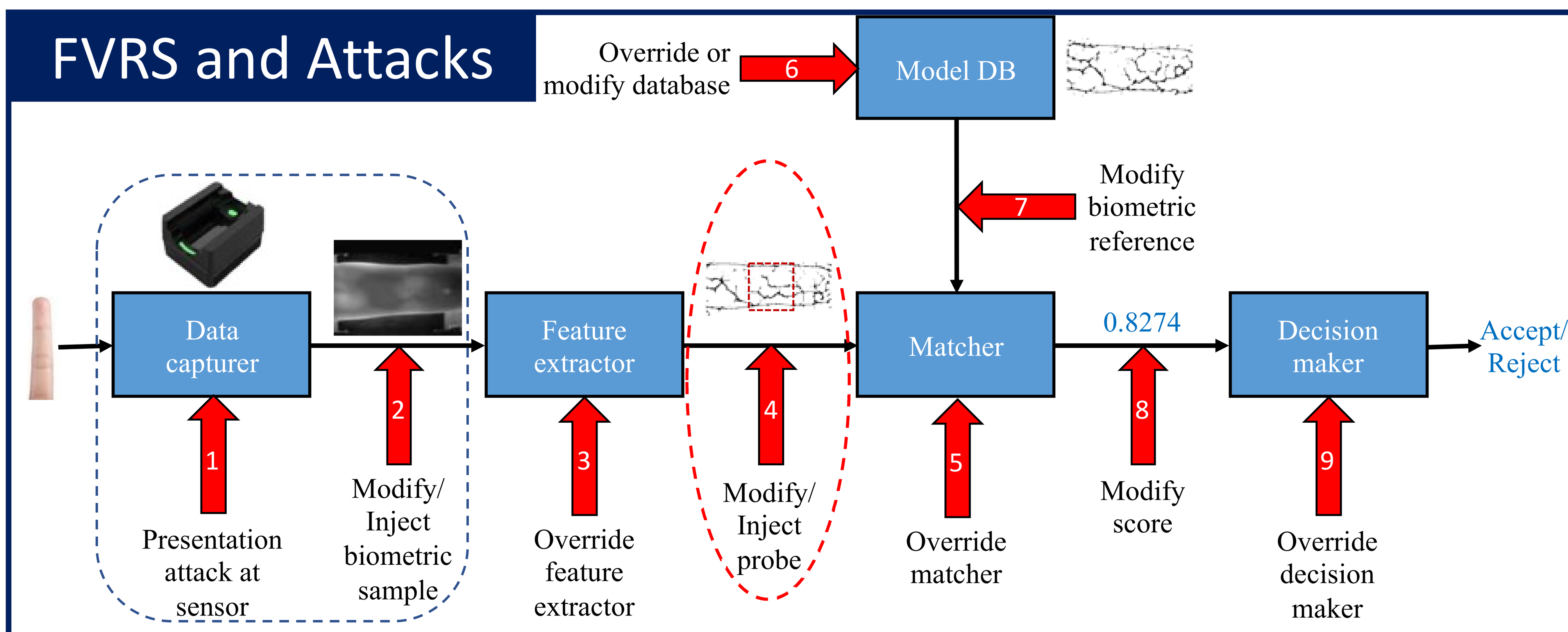
→ They may be vulnerable to **master vein attacks**.

Contributions

Four-fold:

- Point out that Miura's FVRS can be easily compromised by non-vein-looking and vein-looking images (FAR up to 94.21%).
- Combine β-VAE and WGAN-GP models to generate large, good-quality vein images used in latent variable evolution (LVE)-based attack.
- Present a k-label targeted adversarial machine learning (AdvML) attack.
- Combine LVE-based attack and AdvML-based attack (FAR up to 88.79%).

FVRS and Attacks



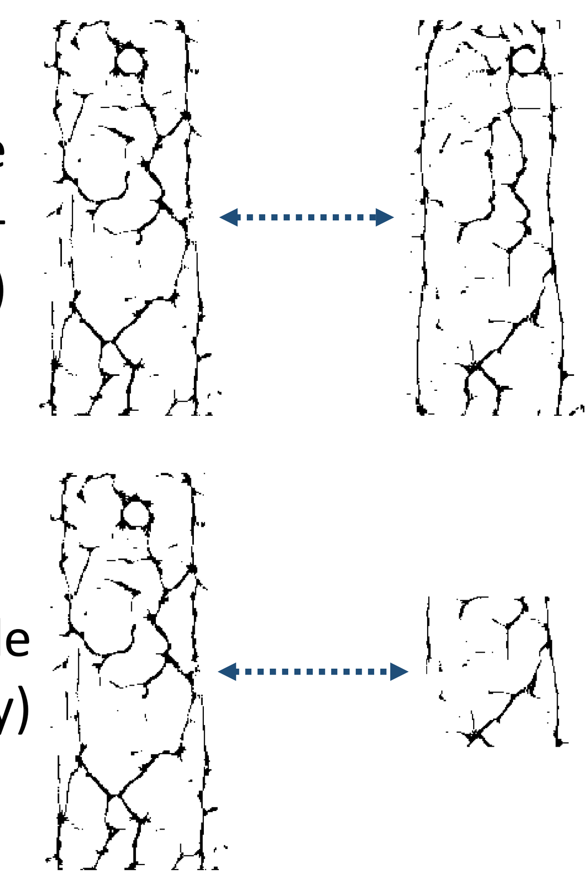
We focus on attack no. 4:

- Have clear vein images → Easy for generation & analysis.
- Master veins can be "translated" to other forms to perform attack no. 1 and 2.

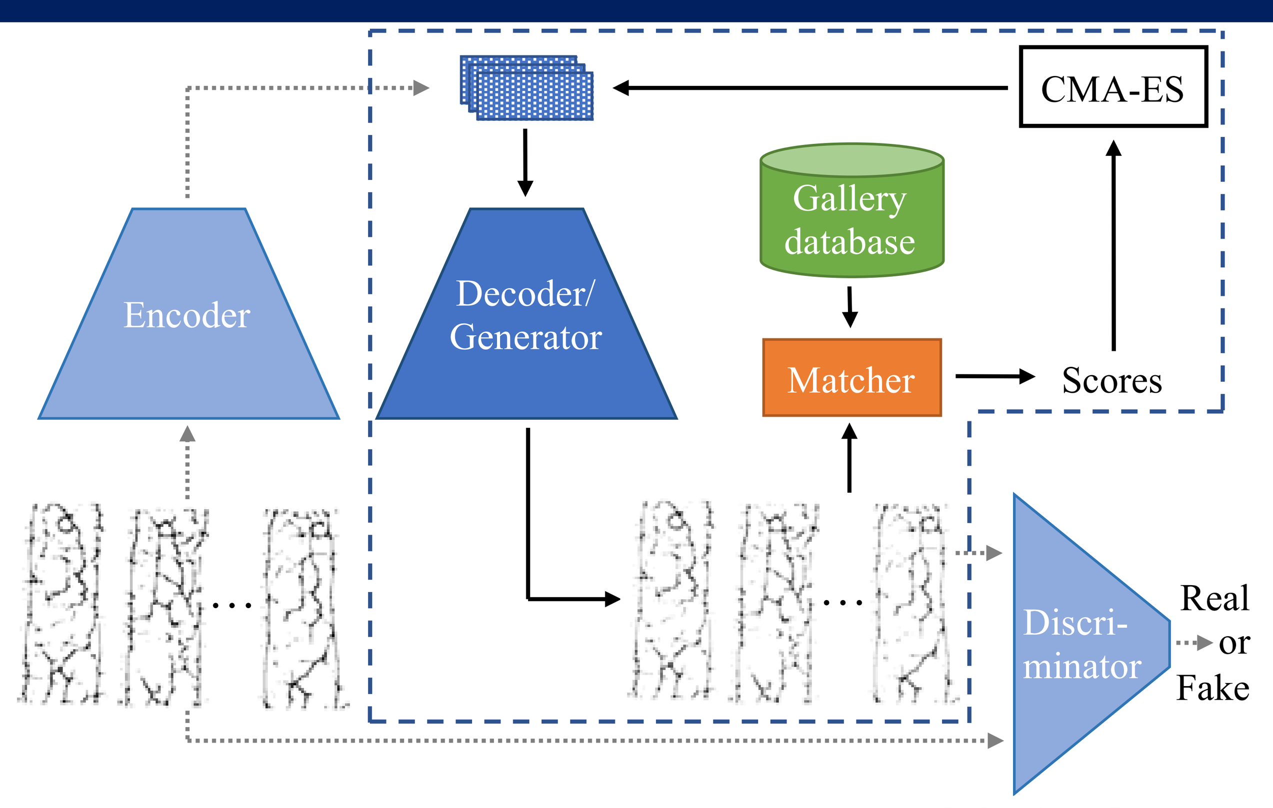
Gallery **Probe**

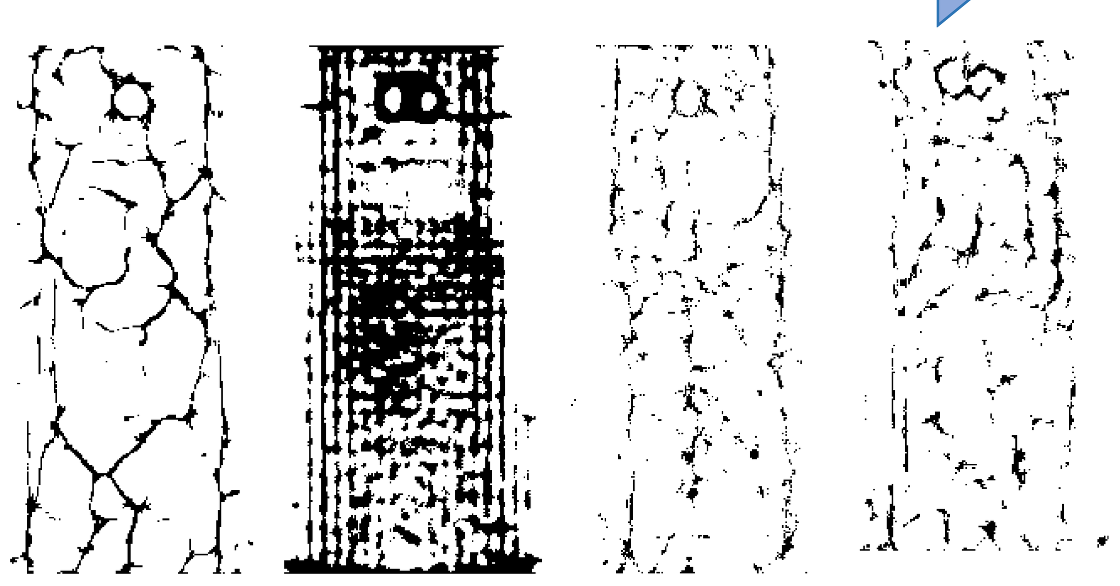
Full-maching mode (Miura's system & CNN-based systems)

Partial-maching mode (Miura's system only)



Method 1: LVE-Based Attack





a. Original image b. WGAN-GP (LVE^1) c. β-VAE (LVE^2) d. Our method (LVE^3)

Flow:

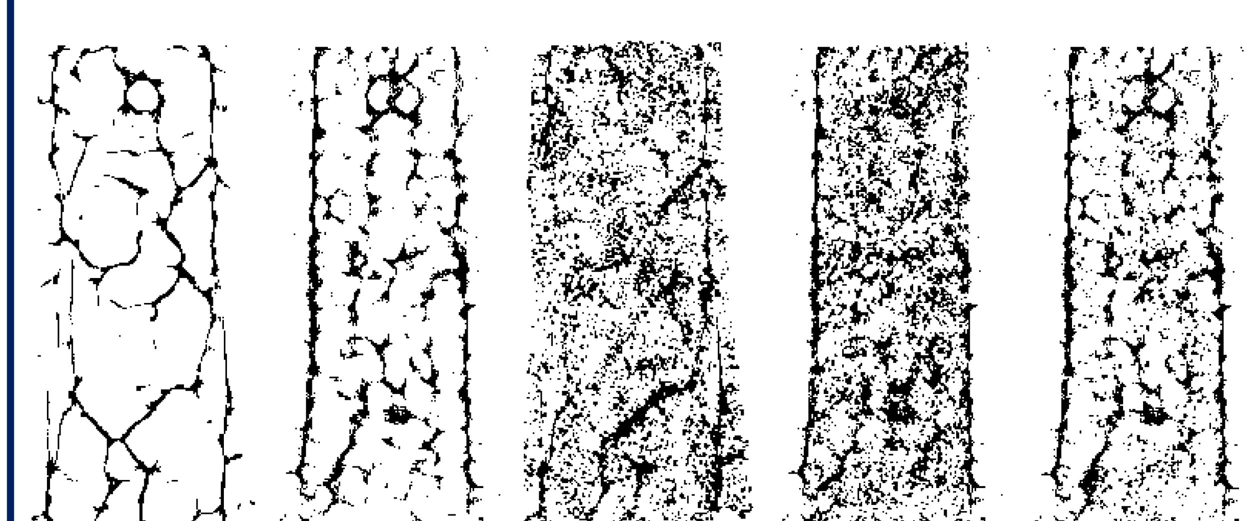
Train β-VAE
↓
Decoder → generator
↓
Add discriminator
↓
Train WGAN-GP
↓
Generator
↓
Run LVE algorithm
↓
Master vein

Method 2: AdvML-Based Attack

Input: Real images or master vein images.

$$\mathbf{x}^{t+1} = \text{Clip}_{\mathbf{x},\epsilon}(\mathbf{x}^t + \alpha(\zeta * K) \odot M)$$
$$\text{with} \quad \zeta = \nabla_{\mathbf{x}} \mathcal{L}(\theta, \mathbf{x}^t, \mathbf{y})$$

iteration (t), filter kernel (K), mask (M), image ($\mathbf{x}$), loss function ($\mathcal{L}$), target soft label vector ($\mathbf{y}$)



a. Original image b. LVE^3 c. AdvML d. Combi-nation e. Combi-nation with top labels

Results & Discussions

Dataset: SDUMLA-HMT: 106 subjects; VERA FingerVein: 110 subjects

Metric: False acceptance rate

Attacks on Known Database (SDUMLA-HMT) and Systems

Matcher	Miura's system (Partial matching)		Miura's system (Full matching)		ResNeXt-50		ResNet-18		MobileNetV3-L	
Attack \ Dataset	Train set	Test set	Train set	Test set	Train set	Test set	Train set	Test set	Train set	Test set
Bona fide	07.57	08.02	08.46	08.98	0.00	2.25	0.00	3.37	0.00	1.31
LVE^1 (WGAN-GP)	**68.24**	**70.41**	**92.46**	**94.21**	**1.85**	1.92	**1.51**	2.25	0.67	1.50
LVE^2 (β-VAE)	**59.63**	**59.27**	**54.75**	**43.89**	0.10	1.44	0.90	2.42	0.33	0.33
LVE^3 (Combination)	**70.47**	**69.85**	**73.29**	**71.84**	**1.46**	**6.07**	0.96	**5.86**	0.53	2.03
AdvML	**11.34**	**13.11**	**32.02**	**49.52**	**1.88**	**3.69**	**1.44**	2.24	0.61	1.46
LVE^3 + AdvML	**48.20**	**50.00**	**82.36**	**88.79**	**1.82**	**3.35**	**1.15**	1.93	0.48	0.64
LVE^3 + AdvML (Top)	**62.73**	**62.52**	**77.82**	**80.41**	**2.37**	**5.32**	**1.60**	4.00	**1.03**	**3.47**
LVE^1 + AdvML (Top)	**76.60**	**76.95**	**91.86**	**93.81**	**1.68**	1.85	**1.52**	2.09	0.55	0.40

Cross-Database (VERA FingerVein) and Cross-System Attacks

Matcher / Attack	Miura's system (Partial matching)	Miura's system (Full matching)	ResNeXt 50	ResNet 18	Mobile NetV3-L
Bona fide	04.07	03.13	8.22	7.28	8.10
LVE^1 (WGAN)	**38.84**	**43.86**	0.18	0.10	0.18
LVE^2 (β-VAE)	**15.08**	02.92	0.00	0.00	0.00
LVE^3 (Comb.)	**20.84**	**19.54**	0.54	0.00	0.01
AdvML (A)	03.12	03.57	0.20	0.04	0.18
LVE^3+A	**16.37**	**47.73**	0.42	0.01	0.18
LVE^3+A (Top)	**22.25**	**26.34**	0.82	0.52	0.21
LVE^1+A (Top)	**39.28**	**44.49**	0.18	0.01	0.17

- Miura's system was vulnerable in most attack scenarios.
- LVE-based + AdvML-based methods achieved better results than single methods.
- CNN-based systems were more robust.

→ Raises the alarm on the robustness of the FVRS, especially hand-crafted systems → Must use counter-measure methods (e.g., quality assessment, presentation attack detection).