GRU-AUNET: A DOMAIN ADAPTATION FRAMEWORK FOR CONTACTLESS FINGERPRINT PRESENTATION ATTACK DETECTION

Banafsheh Adami, Nima Karimian

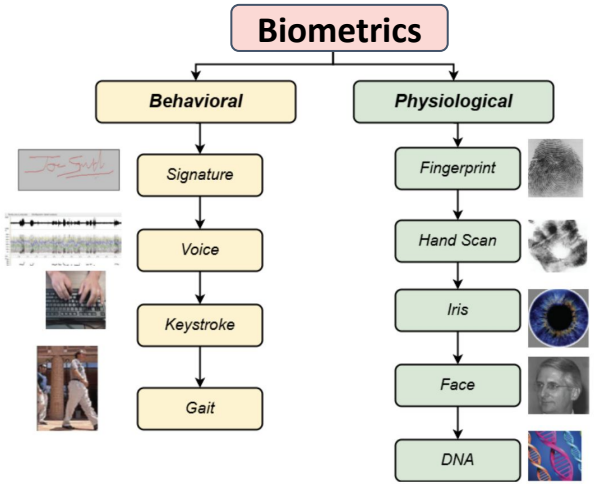
SVCC 2025

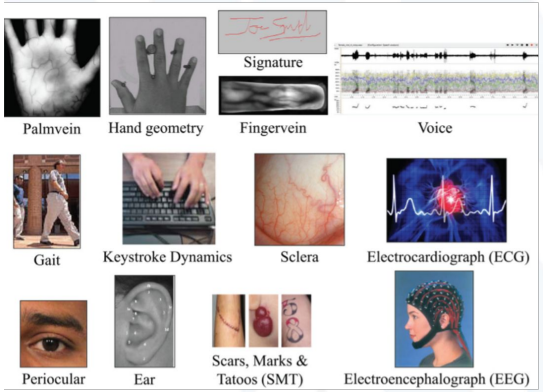


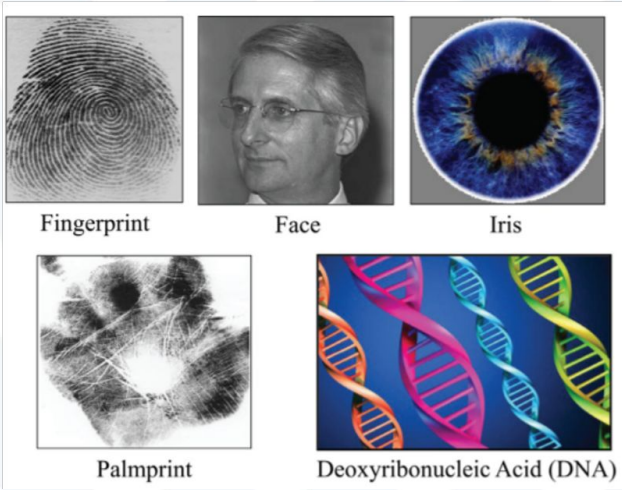
Agenda

- ❑ Biometrics Modalities
- ❑ Biometric Applications
- ❑ Biometric Security & Privacy
- ❑ Biometric Spoofing
- ❑ Contactless Fingerprint Recognition (Unsupervised)

Biometrics Modalities







Jain, Anil K., Karthik Nandakumar, and Arun Ross. "50 years of biometric research: Accomplishments, challenges, and opportunities." *Pattern recognition letters* 79 (2016): 80-105.

Biometric Applications

- Border control
- Automotive
- Smartphone
- Transportation & Smart Access



Clear



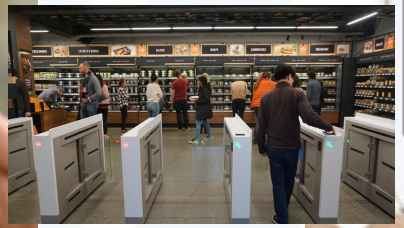
Biometric Border Control



Biometric Future Car



Personal Access Control



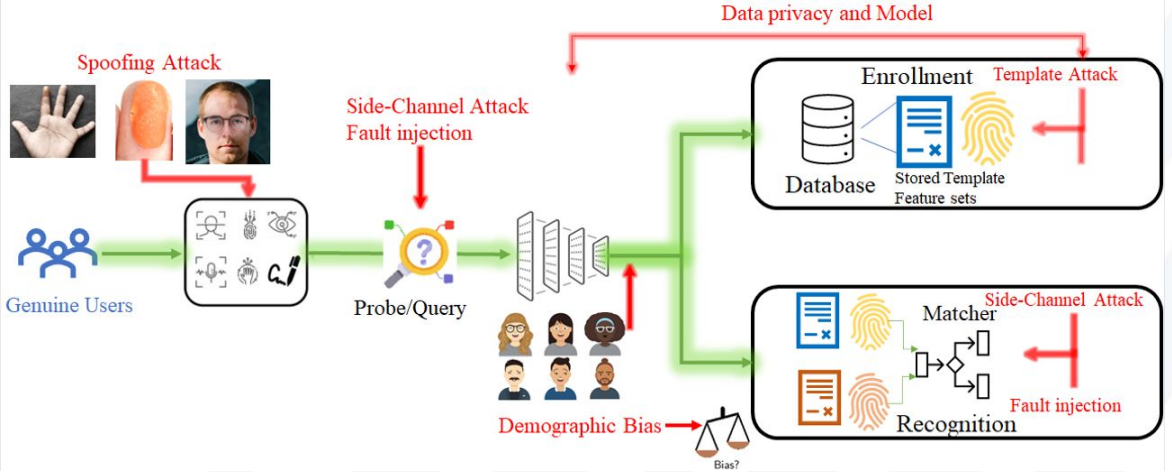
Amazon Go



Apple Fingerprint

Biometrics Security and Privacy

- Template Attack
- Biometric Spoofing
- Privacy
- Fairness and Bias
- Adversarial Attack & Side channel attacks



What is Biometric Spoofing?



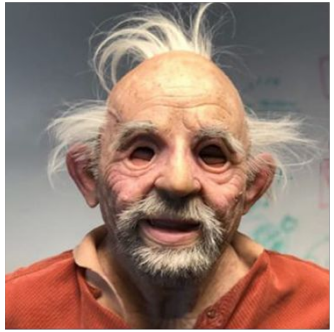
https://www.idrnd.ai/what-is-passive-facial-liveness-and-why-you-shouldnt-use-face-biometrics-without-it/



Aron Ross from MSU demonstrates fake Iris

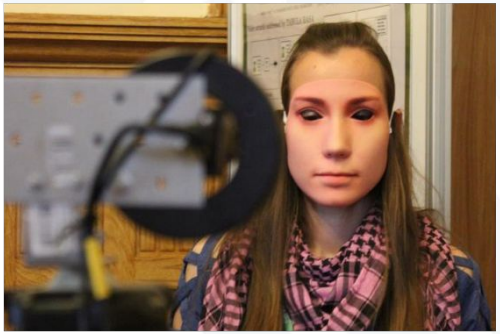


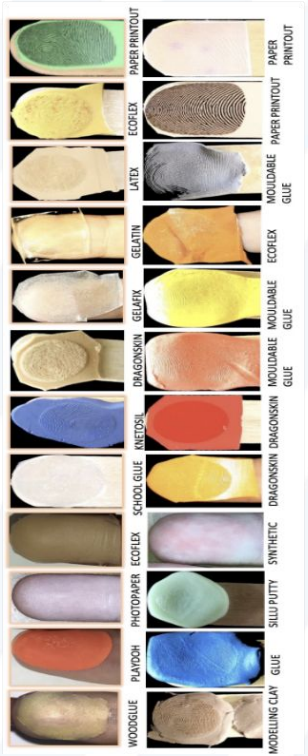
https://www.theverge.com/2017/9/21/16345500/biometrics-fingerprint-identification-technology





https://ec.europa.eu/research-and-innovation/en/horizon-magazine/make-and-fake-fingers-staying-ahead-online-spoofers





Biometric Spoofing



IDIAP Research Institute

Contactless Fingerprint

Why Contactless Biometrics?

- ❑ Hygiene and Safety
- ❑ User Convenience
- ❑ Security Demand
- ❑ Exceptional Speed



Challenges:

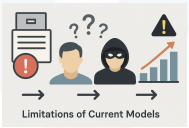
- ❑ Susceptibility to Spoofing (Printed photos, Silicone, playdoh, or other materials)
- ❑ Lack of Physical Contact reduces certain liveness cues.





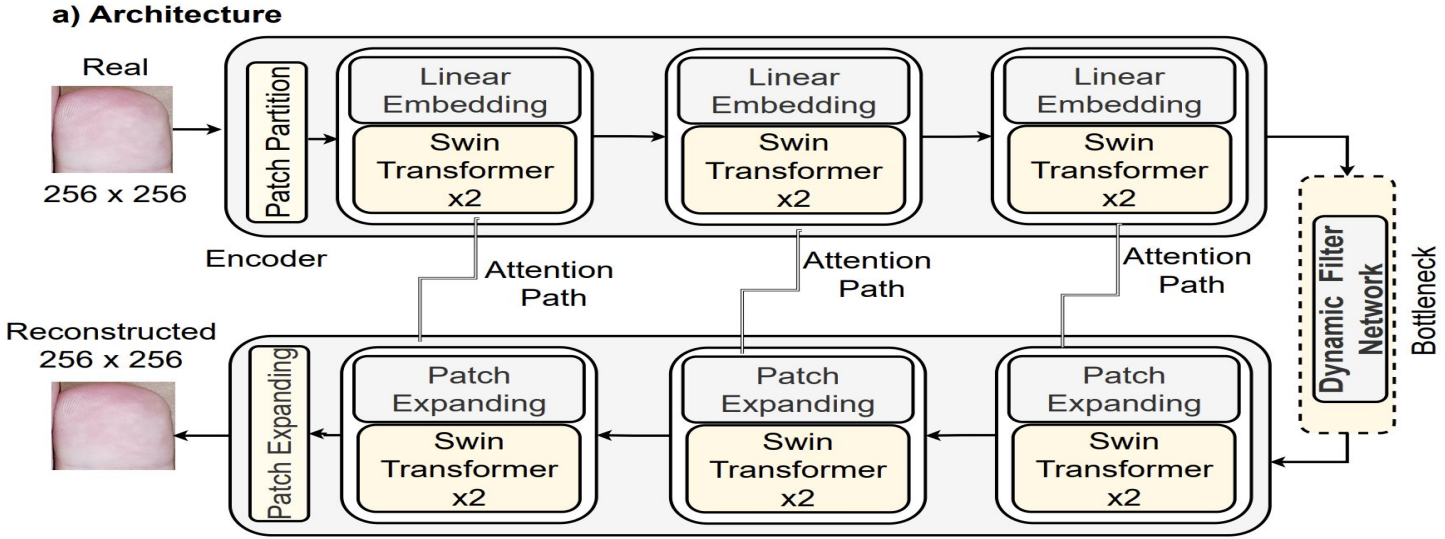
Limitations of Current Models:

- ❑ Heavy reliance on labeled spoof data.
- ❑ Limited generalization to unseen attack types.
- ❑ Difficulty scaling due to evolving spoofing techniques.



Method	Type	Dataset(s)	Results (APCER / BPCER %)
Taneja et al., 2016	Handcrafted	IIITD	10.0 / 1.8, 0, 0.66
Purnapatra et al., 2023	Supervised	CLARKSON	0.14 / 0.18
Hailin Li et al., 2023	Supervised	CLARKSON	8.26 (EER) / –
Adami et al., 2023	Unsupervised	CLARKSON, COLFISPOOF, IIITD	0.63–1.6 / 0.12–0.96
Adami et al., 2024	Unsupervised	CLARKSON, COLFISPOOF, IIITD	1.6 / 0.96
GRU-AUNET (Adami et al.)	Unsupervised	CLARKSON, COLFISPOOF, IIITD	0.47 / 0.09

GRU-AUNet: Architecture Overview



- Encoder-decoder with Swin Transformer
- Dynamic Filter Network in bottleneck
- GRU-based attention path replaces skip connections.

Swin Transformer + (DFN)

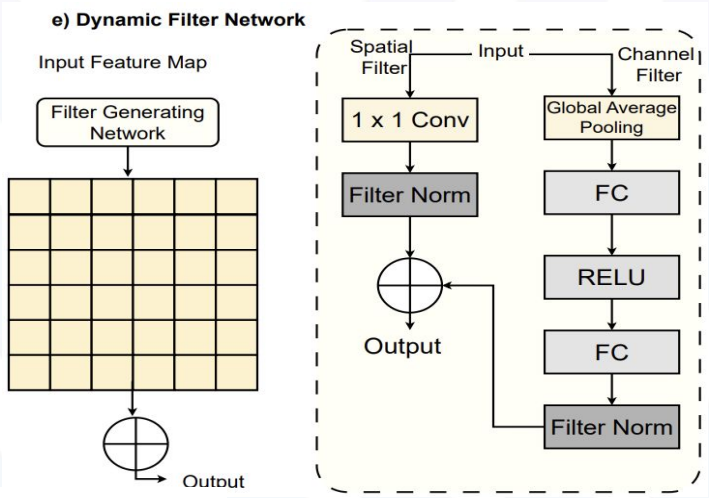
DFN (Dynamic Filter Network): Create specific filters for real/spoof separation

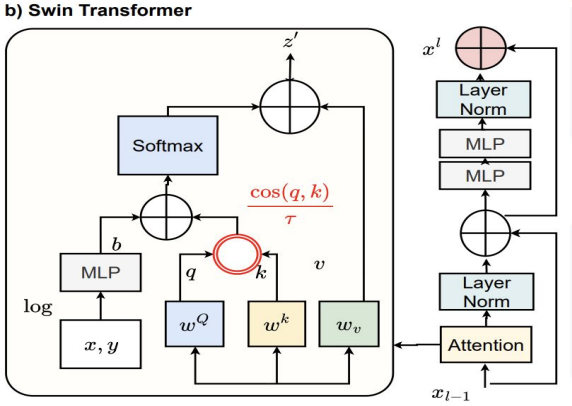
Branches:

- Spatial – local textures
- Channel – key feature

Swin Transformer:

Local & global features via window attention





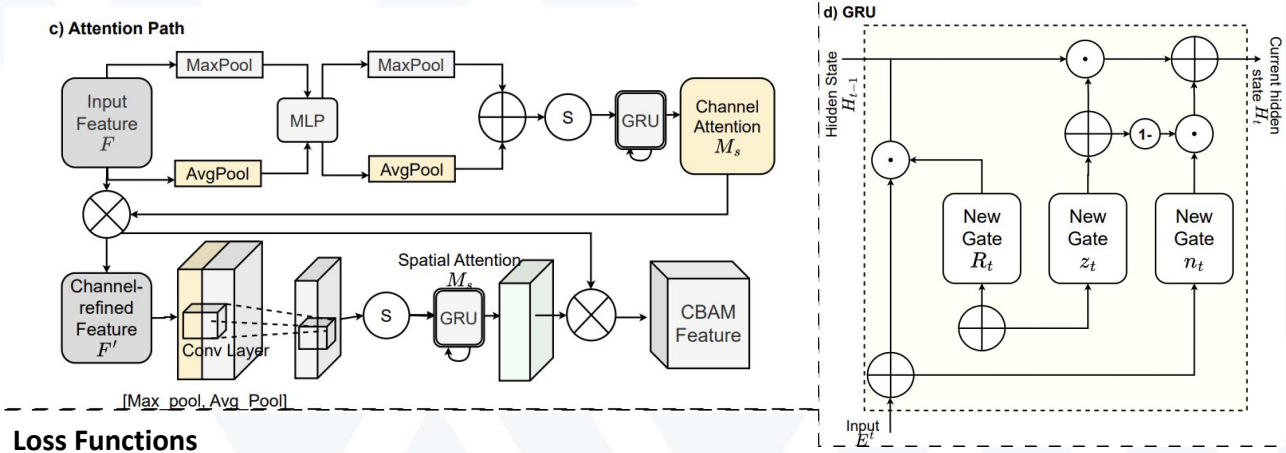
Attention Path with GRU-Enhanced Features

Attention-Based Skip Replacement

Replaces skip connections with an attention-enhanced path.

GRU + CBAM

Combines spatial and temporal attention for richer feature learning.



Loss Functions

- **Focal Loss**

$$\mathcal{L}_{\text{Focal}}(y,\hat{y}) = -\frac{1}{N}\sum_{i=1}^{N}[\alpha(1-\hat{y}_i)^{\gamma}\cdot y_i\cdot\log(\hat{y}_i) + (1-y_i)\cdot(1-\alpha\hat{y}_i)^{\gamma}\cdot\log(1-\hat{y}_i)]$$

- **Contrastive Loss**

$$\mathcal{L}_{\text{Contrastive}} = \frac{1}{2N}\sum_{i=1}^{N}\left[y_i\frac{1}{2}d_i^2 + (1-y_i)\frac{1}{2}\max(0,m-d_i)^2\right]$$

Experimental Setup

Dataset	Spoofing Types	Genuine Samples	Spoofing Samples
CLARKSON	Ecoflex, Photopaper, Playdoh, Woodglue	5,886	4,324
COLFISPOOF	Gelatin, Gelafix, Glue, Latex, Mouldable Clay	0	7,200
IIITD	Print Attack, Photopaper, Playdoh	4,096	8,192

Evaluation Metrics

- **APCER** – Spoof samples misclassified as real

$$\text{APCER} = \frac{\text{Number of misclassified attack samples}}{\text{Total number of attack samples}}$$

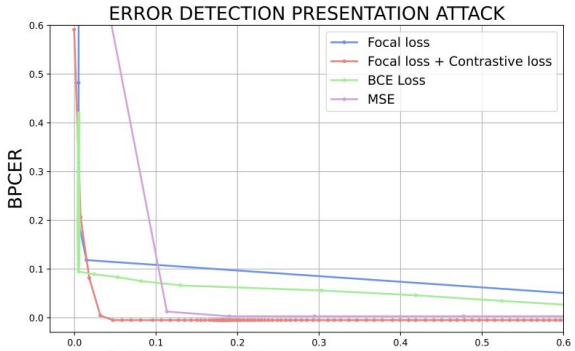
- **BPCER** – Real samples misclassified as spoof

$$\text{BPCER} = \frac{\text{Number of misclassified real samples}}{\text{Total number of real samples}}$$

- **ACER** – Average of APCER and BPCER

$$\text{ACER} = \frac{\text{APCER} + \text{BPCER}}{2}$$

Performance and Results



Training Dataset	Testing Dataset	APCER (%)	BPCER (%)
CLARKSON	COLFISPOOF	0.4	0.11
IIITD	CLARKSON	0.3	0.12
COLFISPOOF	CLARKSON	0.5	0.10

Dataset	Fold 1	Fold 2	Fold 3	Fold 4	Fold 5	Average
CLARKSON [19]	1.5%	1.2%	1.1%	1.3%	1.4%	1.3%
COLFISPOOF [12]	0.09%	0.07%	0.08%	0.09%	0.08%	0.08%
IIITD [34, 22]	0.21%	0.19%	0.20%	0.21%	0.22%	0.21%

Dataset	Method	APCER (%)	BPCER (%)	ACER (%)	Spoof Types (APCER %)
CLK	DenseNet-121 [19]	88.03	0.18	44.11	Eco (0), PH (88.03), PL (0.14), WO (0)
	NASNetMobile [19]	82.15	9.04	45.60	Eco (0), PH (82.15), PL (0.71), WO (5.96)
	ResNet [25]	88.03	0.18	44.11	Eco (0), PH (9.43), PL (0.14), WO (0)
	GRU-AUNet (Ours)	**1.2**	**0.09**	**0.65**	Eco (0), PH (0), PL (0.17), WO (0)
CFS	ResNet-50 [20]	45.33	3.33	24.33	GEL (13.32), GFX (NA), GLU (NA), LAT (NA), MC (NA)
	DenseNet-201 [20]	94.72	3.33	49.03	GEL (15.33), GFX (NA), GLU (NA), LAT (NA), MC (NA)
	ResNet [25]	0	.09	0	GEL (0), GFX (0), GLU (0), LAT (0), MC (0)
	GRU-AUNet (Ours)	**0.0**	**0.09**	**0.04**	GEL (0), GFX (0), GLU (0), LAT (0), MC (0)
IIITD	ResNet18 [16]	NA	NA	NA	PA (NA), PH (NA), PL (NA)
	DenseNet-121 [17]	NA	NA	NA	PA (NA), PH (NA), PL (NA)
	GRU-AUNet (Ours)	**0.21 (PH)**	**0.09**	**0.15**	PA (0), PH (0.21), PL (0)

Conclusion

- Contactless biometric systems are vulnerable to spoofing attacks like ecoflex and **photopaper**, which pose serious risks. PAD is vital for secure, hygienic authentication.
- **GRU-AUNet** achieved **1.2% APCER** and **0.09% BPCER** on **CLARKSON**, outperforming DenseNet-121 (**88.03%**) and NASNetMobile (**82.15%**).
- It achieved **0% APCER** on **COLFISPOOF**, resisting attacks like ecoflex, latex, and playdoh.
- On **IIITD**, it maintained **0.21% APCER**, significantly improving detection of **photopaper**, the most challenging spoof (previously over 80%).
- Cross-dataset and 5-fold results confirmed strong generalization and stability across spoof types.

Q&A

THANK YOU

