Vocal Resonance as a Passive Biometric

Rui Liu, Cory Cornelius*, Reza Rawassizadeh, Ron Peterson, David Kotz
Department of Computer Science, Dartmouth College and *Intel Labs

MOTIVATION

Body Area Networks:
- Devices continuously track health- and lifestyle- related conditions
- They discover, recognize each other and share secrets
- They can automatically identify the wearer

Goal: Automatically authenticate the wearable devices

BIOMETRICS

- *Universal*: Everybody possesses it
- *Unique*: It should be individually unique in a population
- *Permanent*: It remains invariant over a relevant time scale
- *Measurable*: It is captured by some sensor quantitatively
- *Unobtrusive*: We are able to unobtrusively measure it
- *Accurate*: Our authentication result is nearly-always correct

VOCAL RESONANCE

- Voice as heard through the vocalizer's body

HYPOTHESES

- Vocal resonance is a biometric (having all the properties above)
- Body voice and air voice are distinguishable

DATA COLLECTION

- 29 subjects: 18 male and 11 female
- 2 audios: *The Rainbow passage* and *The Wind in the Willows*
- 2 visits: a period of about 2 weeks between 2 data collection for each subject

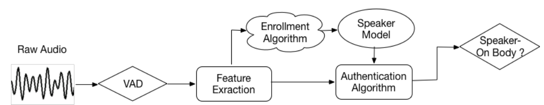
IMPLEMENTATION

- Raspberry Pi Zero W
  - 1 GHZ, single-core ARM CPU
  - 512 MB RAM
- External USB sound card
- Contact piezo microphone
- Remote Server for DNN algorithm

METRICS

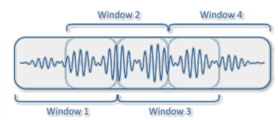
- Identification:
  - Precision: Fraction of audio samples that are identified correctly as the target user
- Verification:
  - Positive: correct user and body, Negative: otherwise
  - False Accept Rate: Fraction of negative cases where we accept
  - False Reject Rate: Fraction of positive cases where we reject
  - Balanced Accuracy: Balanced accuracy on positive and negative samples

SYSTEM PIPELINE



SIGNAL PROCESSING

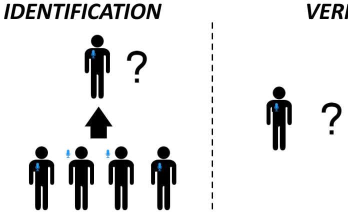
- Voice Activity Detector discards non-speech
- Extract features from sliding windows of audio signals
- Features include 26 MFCCs



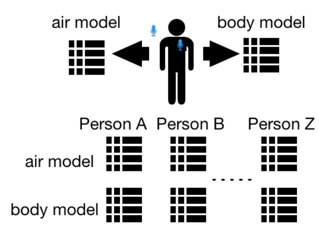
Windows are rectangles with margins
Overlaps are solid fills

AUTHENTICATION ALGORITHMS

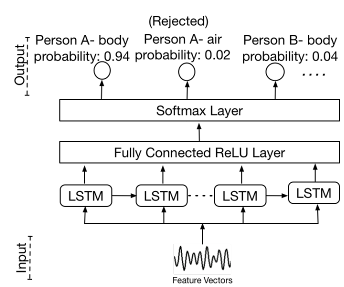
IDENTIFICATION / VERIFICATION



GMM



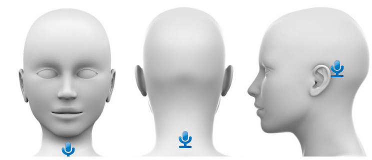
DNN



RESULTS

	GMM	DNN
Precision(identification)	**0.914**	0.817
BAC(verification)	**0.976**	0.929
FAR(verification)	0.047	**0.030**
FRR(verification)	**0.001**	0.030

DIFFERENT PLACEMENTS



	throat	neck	ear
Precision(identification)	**0.914**	0.895	0.913
BAC(verification)	**0.976**	0.957	**0.976**
FAR(verification)	**0.047**	0.0843	0.048
FRR(verification)	**0.001**	0.002	0.009

CONCLUSION

- We can use vocal resonance as a passive biometric, and it achieves high accuracy in terms of identification and verification problems
- We can even use the vocal resonance through neck/ear to authenticate a variety of wearable devices
- The DNN method requires a stable network connection to the remote server
- GMM works good for most of the occasions

FUTURE WORK

- Try vocal resonance through other parts of body, e.g., wrist, chest, even ankle

ACKNOWLEDGEMENTS

This work is an activity of ISTS at Dartmouth College funded by NSF under award numbers CNS-0910842 and CNS-1329686, and by the Department of Health and Human Services (SHARP program) under award number 90TR0003-01

REFERENCES

[1] C. Cornelius and D. Kotz. Recognizing whether sensors are on the same body. Journal of Pervasive and Mobile Computing, 8(6):822–836, Dec. 2012
[2] C. Cornelius, R. Peterson, J. Skinner, R. Halter, and D. Kotz. A wearable system that knows who wears it. In Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys), pages 55–67, June 2014