Digit Recognition From Wrist Movements and Security Concerns with Smart Wrist Wearable IoT Devices

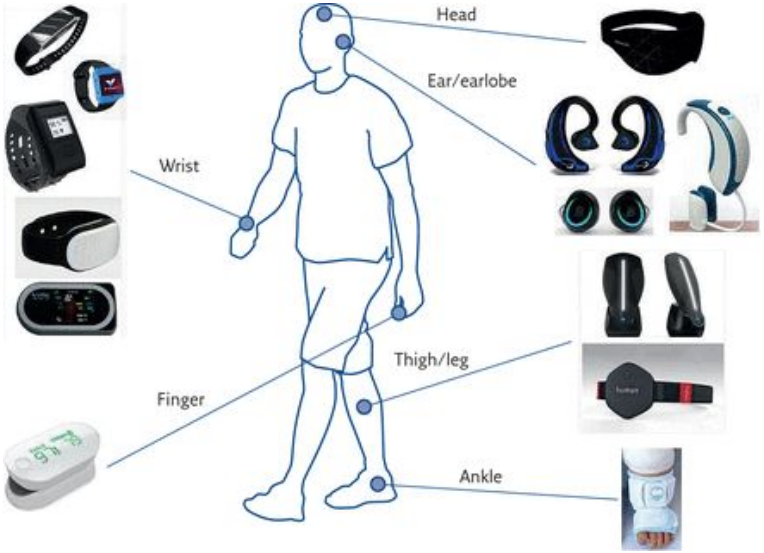
Lambert Leong[1,2], Sean Wiere[2]

[1] University of Hawaii Cancer Center, Honolulu, HI, USA; [2] Molecular Bioscience and Bioengineering,University of Hawaii, Honolulu, HI, USA;

HICSS 2020

Wearable Internet of Things (IoT) devices are becoming more common

- Devices are often worn or placed on the wrist
  - e.g. Apple watch, Fitbit, Samsung watch, etc.
- Most wearable IoT devices contain similar hardware
  - Accelerometer
  - Gyroscope
- Devices and hardware are always listening and recording
  - Lots of data
  - Potential security risks



Aliverti, Breathe, 2017 13: e27-e36

More @ https://www.lambertleong.com/projects/handwriting_hicss

Inspiration and related work

- Wearable IoT devices offer a constant data stream and machine learning has been used to make sense of the data
- Wrist wearable IoT devices have many task recognition use cases
  - E.g. sports activity, fall and seizure detection in healthcare
- Wearable IoT and text related recognition
  - Finger writing - multiple sensors to detect writing and gestures in the air
  - Audio aided segmentation for letter detection when writing on a whiteboard
- Potential security risk with wearable IoT
  - Wearable IoT devices have been shown to be easily compromised
  - Wearers inadvertently mapping secure locations by walking around in them

Xu et al., International Workshop on Mobile Computing Systems and Applications, 2015 , pp. 9–14, ACM

Washington Post, 2018

More @ https://www.lambertleong.com/projects/handwriting_hicss

Digit recognition from wrist movement and security implications

- Goal:
  - Show that it is possible to detect what a user is writing from the motions of their wrist alone
- Hypothesis:
  - Wrist movements and orientation changes are unique to the digit being written and machine learning can be used to accurately classify the written digits
- Security concerns:
  - There are many types of sensitive and personal information is numerical
    - E.g. - social security numbers(SSN), credit card numbers, medical record numbers (MRN)
  - If nefarious entities obtained the data from wearable IoT device sensors they could derive the sensitive information that was written

More @ https://www.lambertleong.com/projects/handwriting_hicss

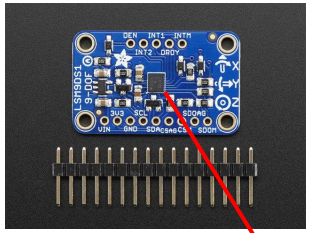
Objective

1. Show that wearable IoT hardware can capture the subtle movements of the wrist during writing
2. Look for uniqueness in the movements of the wrist when writing each digit
3. Use the unique movements to construct a machine learning model to identify the digit being written

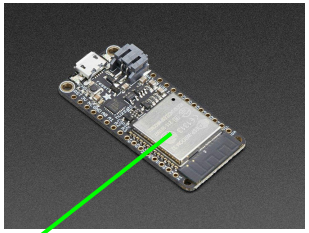
More @ https://www.lambertleong.com/projects/handwriting_hicss

Data collection hardware (obj 1)

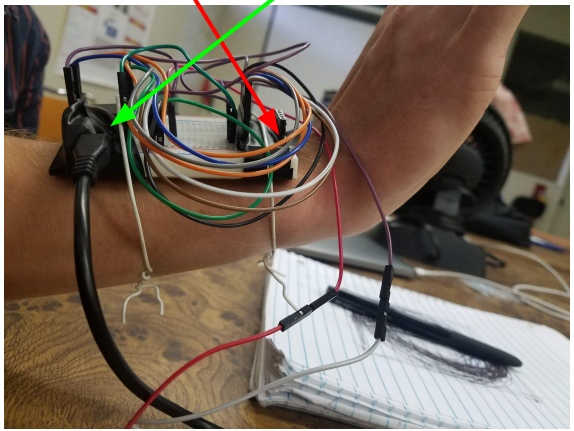
- Hardware
  - LSM9DM - inertial measurement unit (IMU)
    - Accelerometer
    - Gyroscope
  - ESP32 microcontroller board
- Data Collection
  - Participants wore our device on their wrist while the wrote the digits zero and one
    - Digits had to be written within a 10 x 10 cm square
    - Right handed participants
- Final Dataset - 400 writing samples
  - 200 writing samples of the digit zero
  - 200 writing samples of the digit one



LSM9DM



ESP32



More @ https://www.lambertleong.com/projects/handwriting_hicss

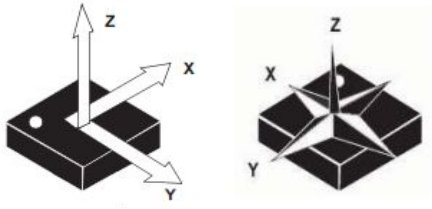
Objective

1. Show that wearable IoT hardware can capture the subtle movements of the wrist during writing
2. Look for uniqueness in the movements of the wrist when writing each digit
3. Use the unique movements to construct a machine learning model to identify the digit being written

More @ https://www.lambertleong.com/projects/handwriting_hicss

Data preprocessing and feature engineering (obj 2)

- Device output:
  - x, y, z acceleration
  - x, y, z tilt/pitch angle
  - Total time



Hardware output specs

Metrics	Axis	Value Type	Feature Count
Acceleration	x,y,z		3
Pitch Angle	x,y,z		3
Time		Total	1
Total Features			**7**

Original output features

- Engineered features
  - **Goal:** uncouple features from writing time
  - Calculated velocity from acceleration
  - Calculated displacement/distance from velocity

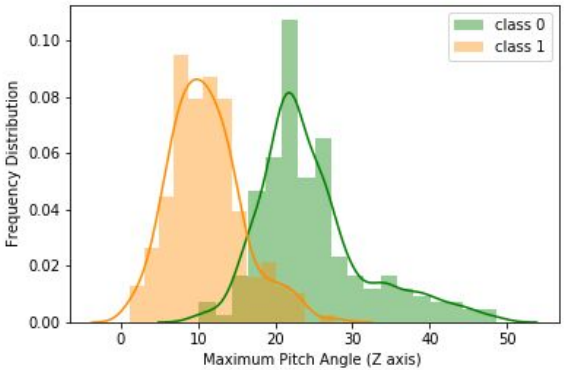
Metrics	Axis	Value Type	Feature Count
Acceleration	x,y,z	Minimum, Mean, Maximum	9
Pitch Angle	x,y,z	Minimum, Mean, Maximum	9
Velocity	x,y,z	Minimum, Mean, Maximum	9
Displacement	x,y,z	Total	4
Total Features			**31**

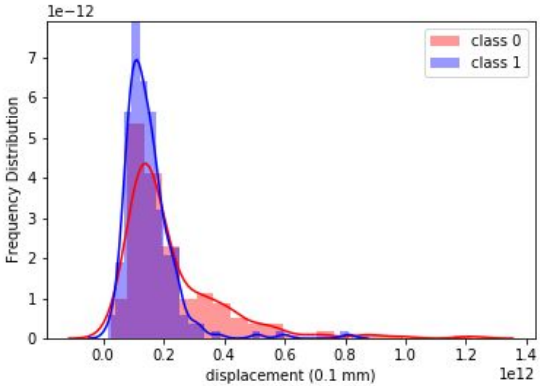
Engineered features

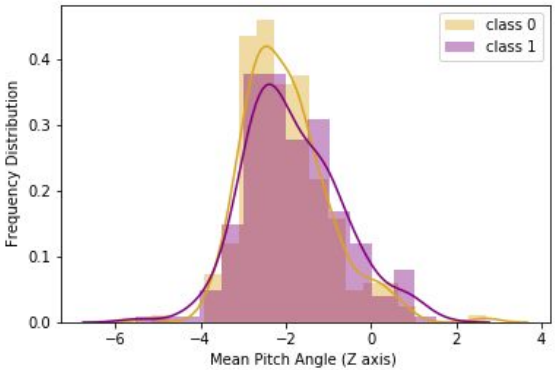
More @ https://www.lambertleong.com/projects/handwriting_hicss

Feature exploration and principal components analysis (obj 2)

- Principal components analysis (PCA) revealed that the top three principal components explain 99.99% of the variance
  - Maximum z axis pitch angle
  - Total x displacement
  - Mean z axis pitch angle

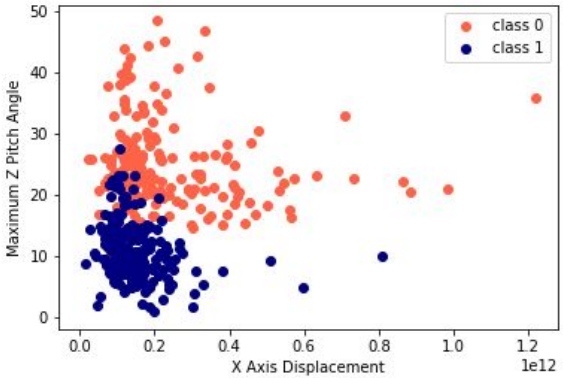


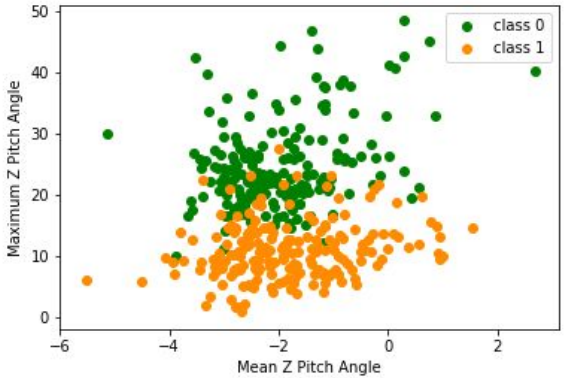


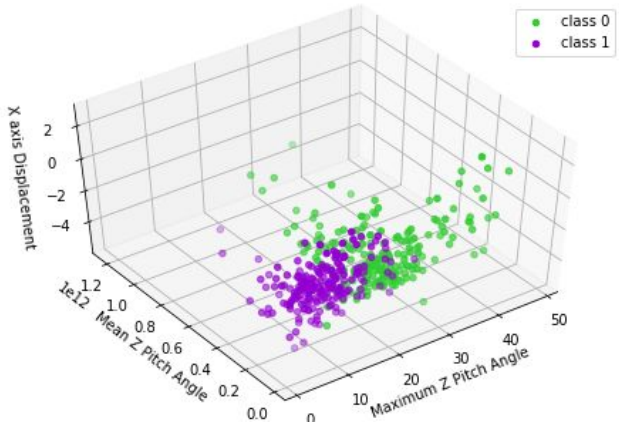


More @ https://www.lambertleong.com/projects/handwriting_hicss

Class separability exploration







Take home message:

More dimensions/features seem to lead to more separability

More @ https://www.lambertleong.com/projects/handwriting_hicss

Objective

1. Show that wearable IoT hardware can capture the subtle movements of the wrist during writing
2. Look for uniqueness in the movements of the wrist when writing each digit
3. Use the unique movements to construct a machine learning model to identify the digit being written

More @ https://www.lambertleong.com/projects/handwriting_hicss

Machine learning model building (obj 3)

- Data Split:
  - Train, Validation, Test - 60%, 20%, 20%
- Modeling:
  - Extreme gradient boosting (xgboost python package)
- Hyper parameters:
  - Tuned using 5 fold cross-validation (CV)
    - Number of estimators
    - Decision tree building algorithm
    - Maximum tree depth
    - Learning rate

Final tuned parameters	
Number of estimators	1000
Tree building algorithm	hist
Max tree depth	1
Learning rate	0.1

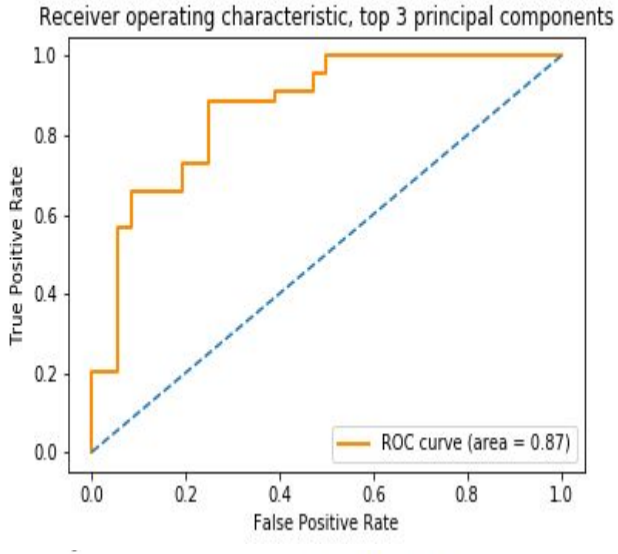
More @ https://www.lambertleong.com/projects/handwriting_hicss

PCA vs Full Feature model

- PCA model:
  - Trained on the 3 features that relate to the top 3 principal components
- Full Feature model:
  - Trained on all 31 features
- Both models were trained and built using the training set with 5 fold CV
- Final models were evaluated on the hold out test set 20%
  - Area under the receiver operating characteristic (AUROC) was use to compare the performance of the two final models

More @ https://www.lambertleong.com/projects/handwriting_hicss

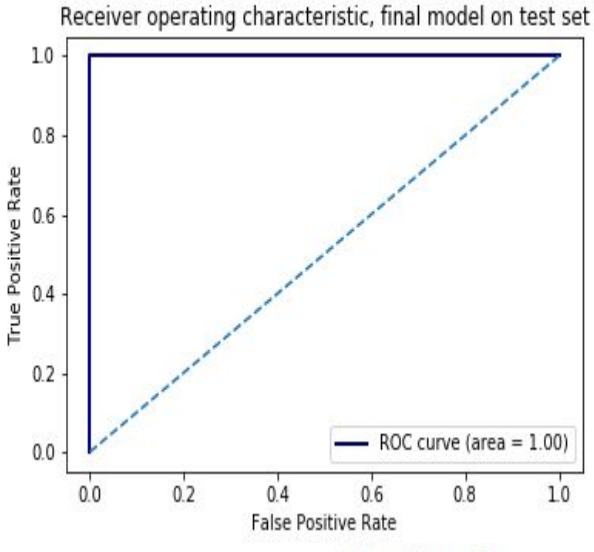
PCA



		Predicted	
		Digit 0	Digit 1
Actual	Digit 0	33	3
	Digit 1	8	36

PCA performance confusion matrix

Full Feature



		Predicted	
		Digit 0	Digit 1
Actual	Digit 0	36	0
	Digit 1	0	44

Full Feature performance confusion matrix

More @ https://www.lambertleong.com/projects/handwriting_hicss

Satisfied objectives

1. We demonstrated that wearable IoT hardware can pick up on the subtle movements during writing
2. With PCA and feature engineering we were able to identify separability or uniqueness between movements associated with the writing digit zero and the digit one
3. PCA and Full Feature models were built and performed well when predicting the written digits in the test set

More @ https://www.lambertleong.com/projects/handwriting_hicss

Real time predictions

- Full Feature model was retrained on the entire dataset (400 samples)
- Model was loaded on to our device
- 10 new participants wore the device and were randomly assigned a digit (zero or one) to write
  - 5 writing samples of the digit zero
  - 5 writing samples of the digit one

		Predicted	
		Digit 0	Digit 1
Actual	Digit 0	5	0
	Digit 1	0	5

Real time Full Feature performance confusion matrix

Model	Accuracy (%)	Digit 0 Precision (%)	Digit 0 Recall (%)	Digit 0 F1 Score (%)	Digit 1 Precision (%)	Digit 1 Recall (%)	Digit 1 F1 Score (%)
PCA	86.25	80.49	91.67	85.74	92.31	81.82	86.75
Full Feature	100.00	100.00	100.00	100.00	100.00	100.00	100.00
Real Time, Full Feature	100.00	100.00	100.00	100.00	100.00	100.00	100.00

More @ https://www.lambertleong.com/projects/handwriting_hicss

Conclusion

- It is possible for the hardware in most wrist wearable IoT devices to pick up on subtle writing movements
- Machine learning models can be built to identify what is being written by users
- Sensitive information can be obtained without the users knowledge

Future work:

- Expand work to more digits and include alphabetical characters
  - More complex modeling options are available
    - E.g. Neural networks and deep learning
- Exploration into how models apply to left handed users
- More labeled data is needed to increase the strength of models

More @ https://www.lambertleong.com/projects/handwriting_hicss

Thank You

Special Thanks to:

Daniel Jenkins, PhD
Peter Sadowski, PhD
Ryan Tanaka, MS
Nori Leong, MEd, MEA, MLIS
John Shepherd, PhD
John-Paul Bingham, PhD

Models at:

https://github.com/LambertLeong

Presentation and Project Info at:

https://www.lambertleong.com/projects/handwriting_hicss

More @ https://www.lambertleong.com/projects/handwriting_hicss