TYPING Biometrics for User Authentication – a One-shot Approach

Hannes Lindström
halindst@stanford.edu

Josef Malmström
josefmal@stanford.edu

Introduction

- Keystroke dynamics is the time series data describing when and which keys are pressed and released as someone is typing on a keyboard.
- By applying methods from behavioral biometrics, this data has been proven to be an effective unique identifier of a person and can therefore be used for authentication [1].
- Plenty of previous work on this problem (e.g. using neural nets, Gaussian mixtures) but these methods fail to generalize to unseen users.
- Can we find an approach that generalizes by utilizing metric learning?
- Relevant metrics:
  FAR = False Acceptance Rate = FPR
  FRR = False Rejection Rate = FNR

Dataset

- Large scale typing dataset from a 2016 study [2].
- Raw typing data from 148 users, both free text and transcribing for 150 minutes each.

key	event	time stamp
R	KeyDown	63578429797235
E	KeyDown	63578429797313
O	KeyUp	63578429797313

Baseline Models

- **GMMs:**
  FAR = 14.6 %, FRR = 6.7 %
- **CNN Classifiers (OVR):**

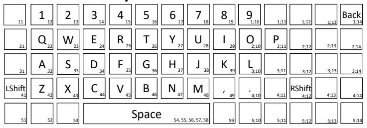
Results for 5 random users

error type	1	2	3	4	5
FAR	17 %	8 %	9 %	23 %	0.1 %
FRR	8 %	9 %	6 %	11 %	23 %

Feature Representation

- **Digraph** = Sequence of two key presses.
- **Digraph feature representation:**
  $\phi = [KD, H_1, H_2, PP, RP] \in \mathbb{R}^5$
  KD = Distance between keys.
  H_i = Hold time of i^{th} key.
  PP = Press-to-press time.
  RP = Release-to-press time.

Key distance model



Sample KD: Y → O = (2-2) + (10 – 7) = 3

- A **typing sample** is a sequence of digraphs. We use samples of length 100.
- One sample: $x^{(i)} \in \mathbb{R}^{5\times 100}$

Results

- Models were trained on data from 30 random users.
- Test data sampled from the same 30 users as well as from 30 random, and previously unseen, users.
- Two prediction methodologies:
  - Predict by comparing to the embedding of a single reference sample.
  - Compare with the embeddings of five different reference samples and predict based on the majority vote.

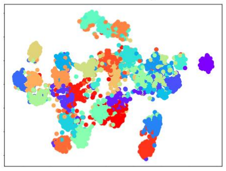
Seen Users

error type	single	5 majority
FAR	8.69 %	7.63 %
FRR	12.29 %	6.61 %

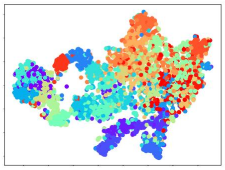
Unseen Users

error type	single	5 majority
FAR	12.05 %	10.14 %
FRR	19.75 %	15.26 %

t-SNE of training data

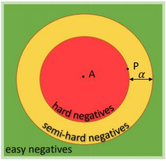


t-SNE of unseen users

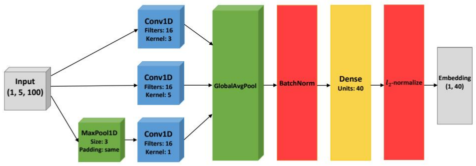


Method

- **Key idea:** Learn an embedding of typing samples into a lower dimensional space, where samples from the same user are close and samples from different users are distant.
- **Triplet learning:** Form triplets (**A**nchor, **P**ositive **N**egative), where **A**,**P** are samples from the same user, and **N** is a sample from a different user.
- Train an **embedding network** using the triplet loss:
  $\mathcal{L} = \max(\|A_e - P_e\|_2 - \|A_e - N_e\|_2 + \alpha, 0)$
- Problem: Most triplets already yield zero loss which results in small gradients. Solution: Online mining for **semi-hard triplets.**

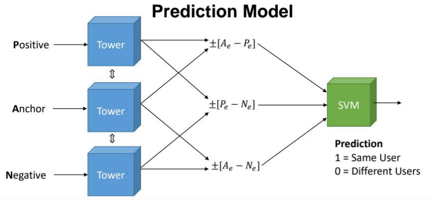


Embedding Network



- When the tower model is trained, we train an SVM on the elementwise difference between embeddings:

Prediction Model



Discussion and Future Work

- We see that our approach is on par with other methods in terms on FAR and FRR.
- This method generalizes reasonably well to users that were not in the training set. Using a single sample from a previously unseen user, we can output decently accurate predictions. The performance is then only further improved as more samples are collected.
- Key aspects of the approach:
  - Online triplet-mining in order to improve convergence.
  - Inception-style embedding network in combination with the choice of feature representation results in embeddings that accurately represent the data without overfitting.
- Future work: Extend the system to work well on users that switch between different keyboards.

References

[1] P. S. Teh et. al. "A survey of keystroke dynamics biometrics." TheScientificWorldJournal vol. 2013, p. 408280, 11 2013. [Online]. Available: https://www.ncbi.nlm.nih.gov/pubmed/24298216%20http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=PMC3835878

[2] Y. Sun, H. Ceker, and S. Upadhyaya, "Shared Keystroke Dataset for Continuous Authentication," in 8th IEEE International Workshop on Information Forensics and Security , Abu Dhabi, UAE, 2016. [Online]. Available: https://cubs.buffalo.edu/research/datasets