Multifactor User Authentication with In-Air-Handwriting and Hand Geometry

Duo Lu, Dijiang Huang, Yuli Deng, Adel Alshamrani CIDSE, Ira A. Fulton School of Engineering Arizona State University

Motivation

Our Objective is

- verifying an **account** that you claim to possess,
- not verifying the **identity** that you claim to be,
- using in-air-handwriting and hand geometry,
- through the gesture interface.

It has **features like a password**:

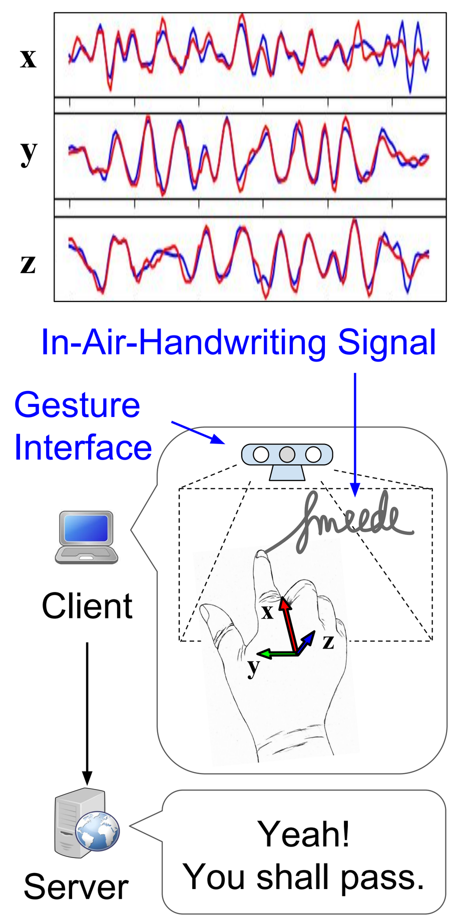
- Created by the user, changeable and revocable;
- The personal identity is not linked to the account.

It also has **features like a biometric**:

- Can not be given to someone else;
- Can not be easily spoofed.

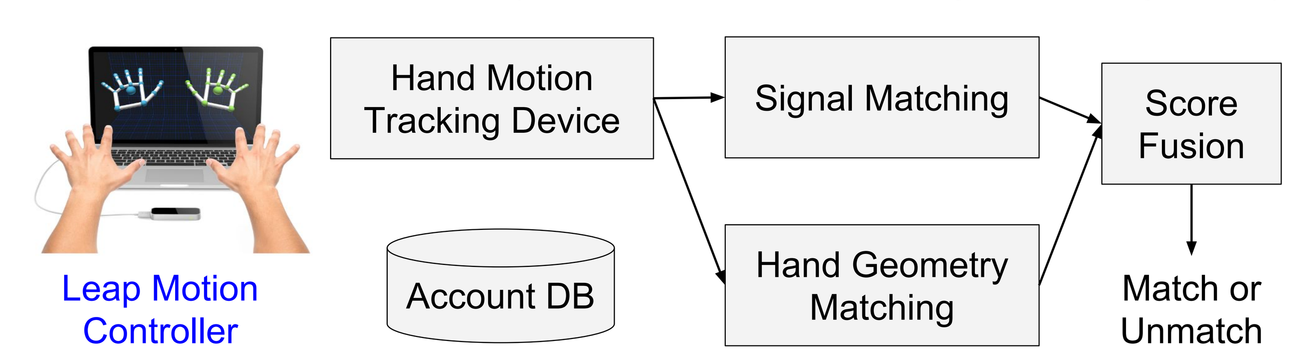
However, there are several technical challenges [6]:

- Hand movement tracking is difficult;
- Minor variations of writing the same content;
- Lack of understanding of the features.



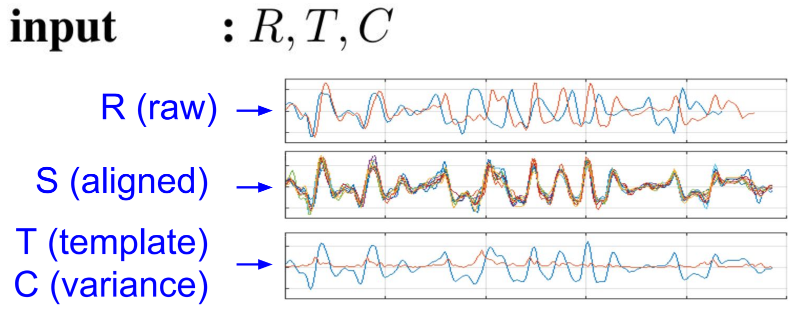
Proposed Approach

Multifactor user authentication system with in-air-handwriting and hand geometry.



Signal Matching Algorithm

input : R, T, C



T and C are generated at registration:

$T_{ij} = mean(S_{ij}^1, S_{ij}^2, ..., S_{ij}^k)$,

$C_{ij} = var(S_{ij}^1, S_{ij}^2, ..., S_{ij}^k)$.

parameter: p, q, th_1, th_2

preparation
$R' \leftarrow \text{preprocess}(R)$.
$S \leftarrow \text{align}(T, R')$.

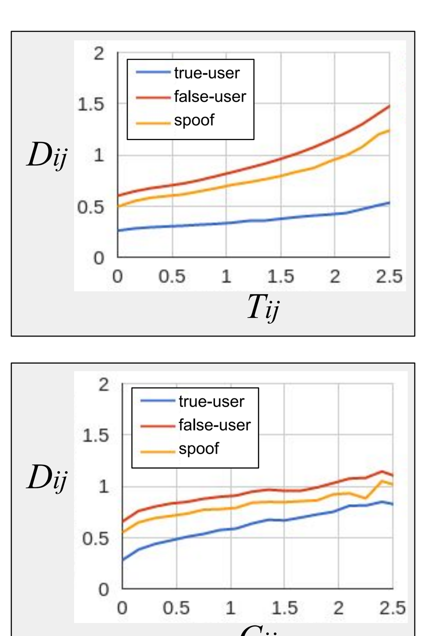
element-wise distance
$D \leftarrow \text{abs}(T - S)$.

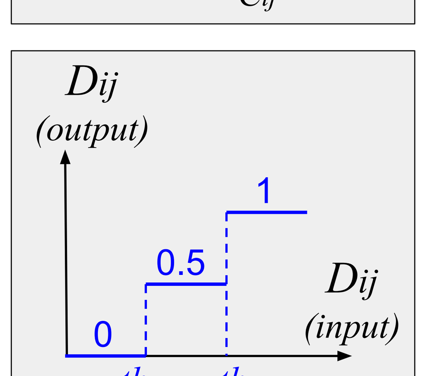
scaling [10]
$P \leftarrow \text{inverse}(\mathbf{1} + p \times T)$
$Q \leftarrow \text{inverse}(\mathbf{1} + q \times C)$
$D \leftarrow \text{multiply}(D, P)$.
$D \leftarrow \text{multiply}(D, Q)$.

Threshold-Then-Vote (TTV)

for i = *1 to l* **do**
  for j = *1 to d* **do**
    if $D_{ij} < th_1$ **then**
      $D_{ij} \leftarrow 0$
    else if $D_{ij} > th_2$ **then**
      $D_{ij} \leftarrow 1$
    else
      $D_{ij} \leftarrow 0.5$
    end
  end
end

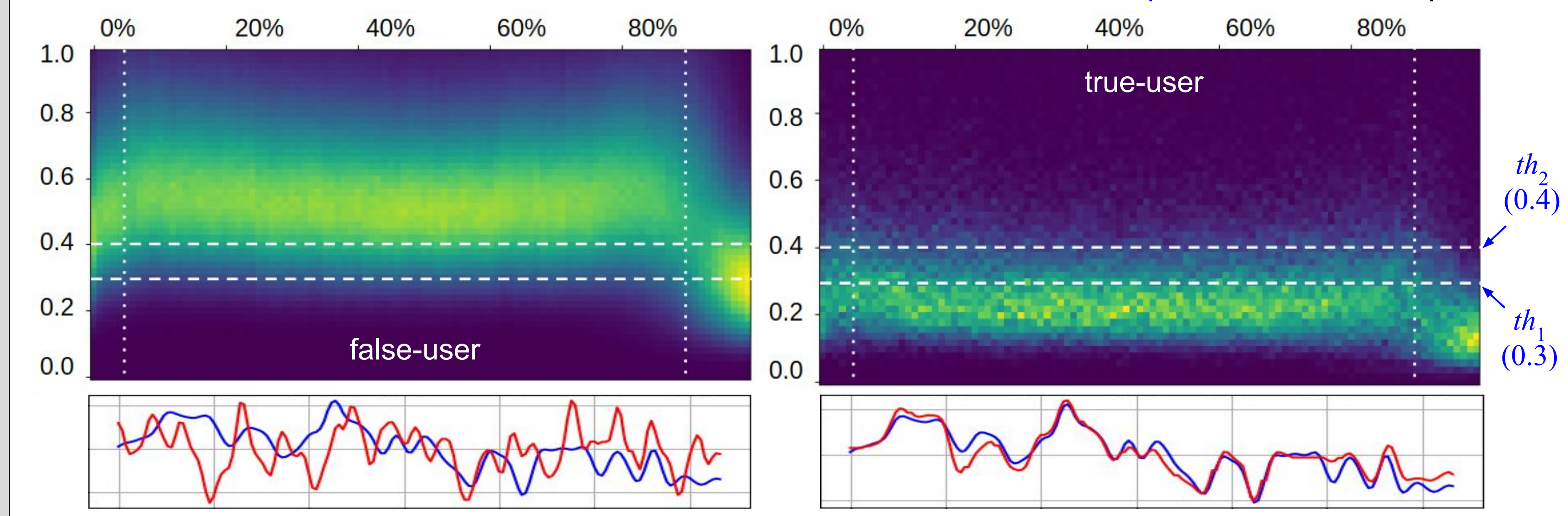
output : $dist(S, T) \leftarrow \frac{1}{l \times d} \sum_i^l \sum_j^d D_{ij}$



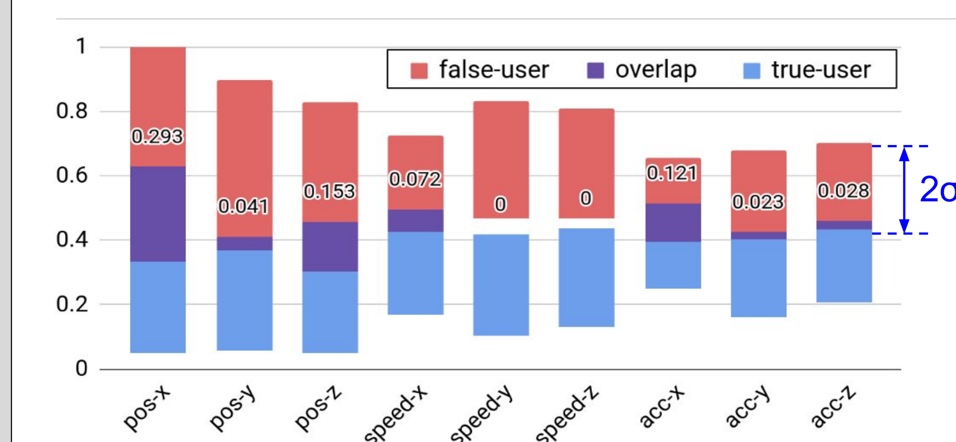


Signal Feature Analysis

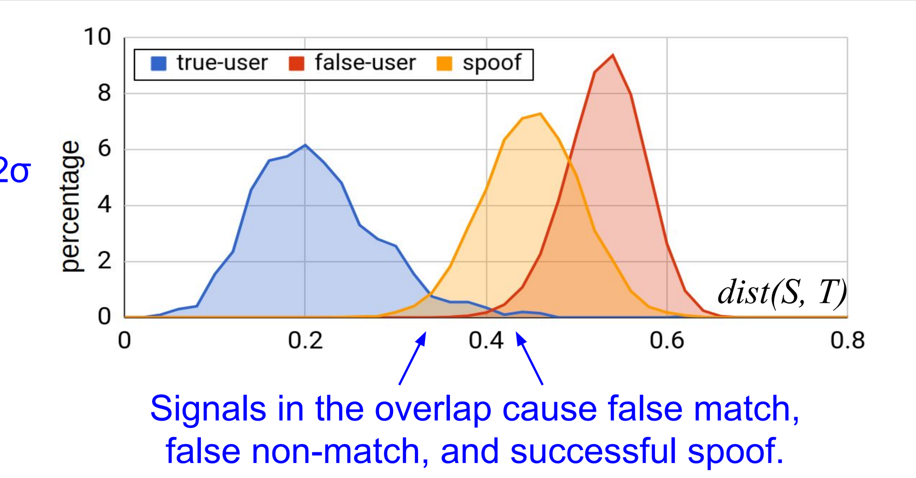
true-user: S and T are from the same account; false-user: different accounts; spoof: S is from the impostors



Distribution of element-wise distance in time (rows of D), i.e., $p(\frac{1}{d} \sum_j^d D_{ij} | c)$



Distribution of element-wise distance in sensor axes (cols of D), i.e., $p(\frac{1}{l} \sum_i^l D_{ij} | c)$

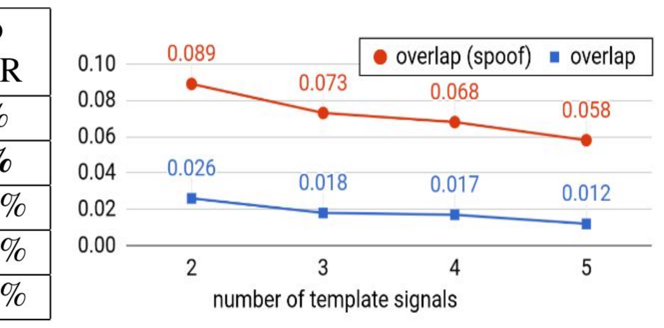


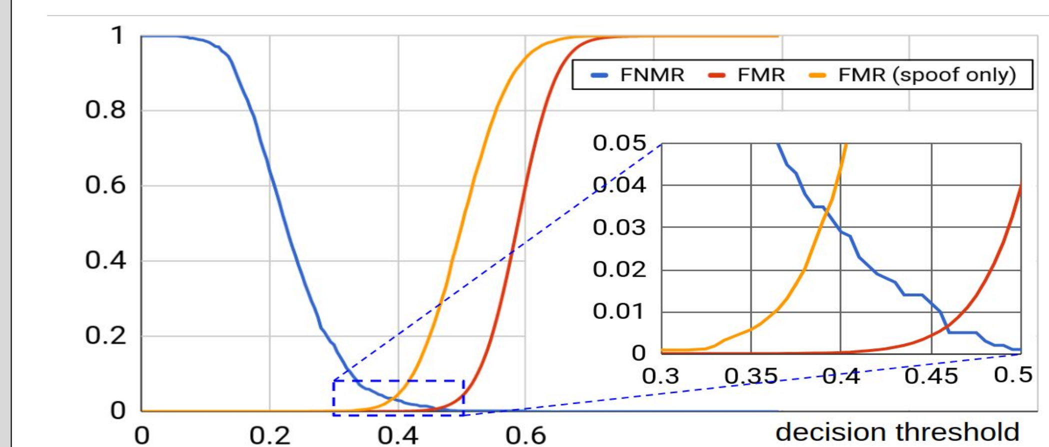
Distribution of signal distance, i.e., $p(dist(S, T) | c)$

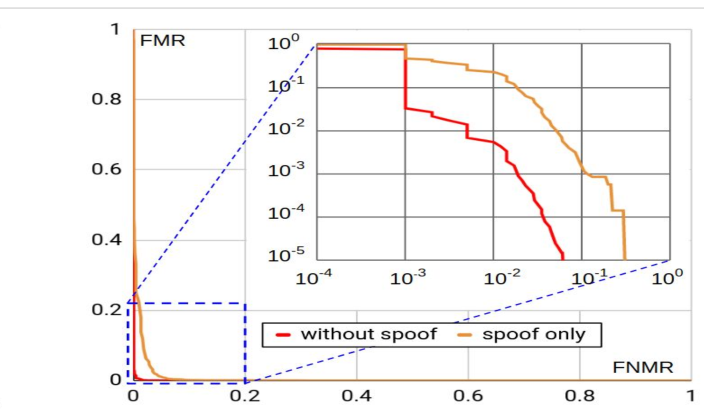
- Signals generated by the same user writing the same content are similar, and hence, they have small distances.
- Human users are better at maintaining speed and force (i.e., acceleration) than position, in y and z axes.

Empirical Results

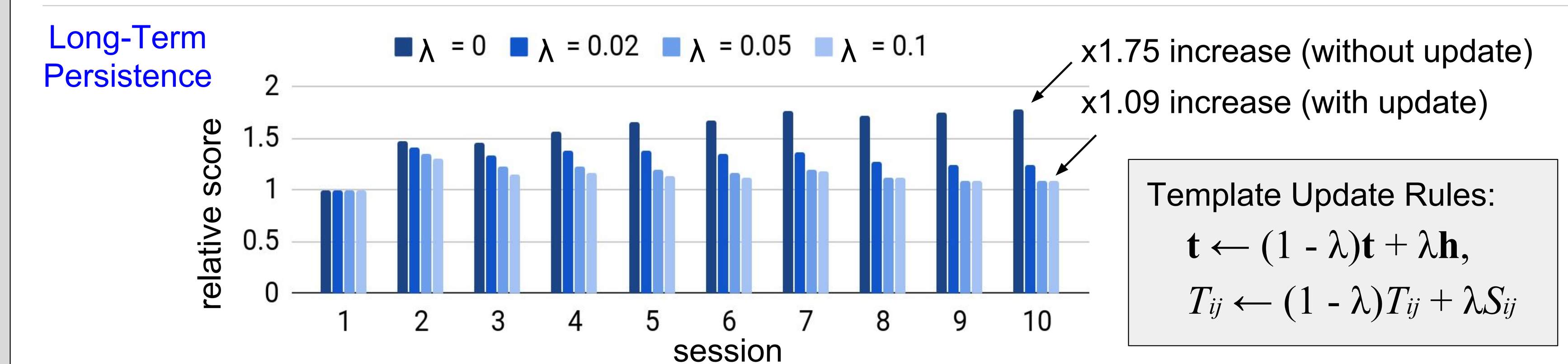
	Algorithm	EER	EER (spoof)	FMR 10K	FMR 100K	Zero -FMR
5 signals at registration	TTV	0.8%	3.7%	3.9%	6.9%	9.1%
	FUSION	**0.6%**	**3.4%**	**3.6%**	**6.2%**	**6.3%**
	DTW	1.3%	4.8%	7.8%	20.0%	22.0%
2 signals at registration	FUSION†	1.3%	5.0%	8.4%	13.0%	18.0%
	DTW†	2.0%	6.5%	11.0%	15.0%	17.0%







Receiver Operating Characteristic (ROC)



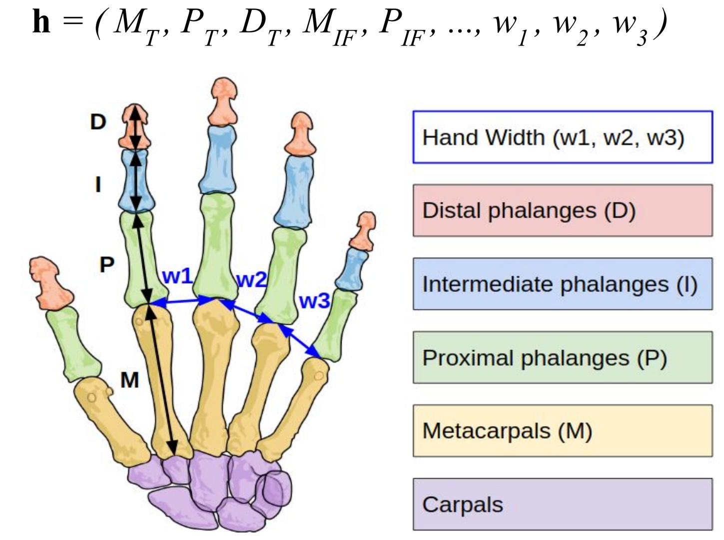
Observations on performance improvement and performance limitation:

- Preprocess provides robustness against poor signal quality and minor variation in writing behavior.
- Threshold-Then-Vote (TTV) prevents locally mismatched signal segments for legitimate users.
- Score fusion further prevents some false matches with additional hand geometry information.
- A few signals at registration may not be enough for the inherent complexity of the writing behavior.

Hand Geometry Matching and Analysis

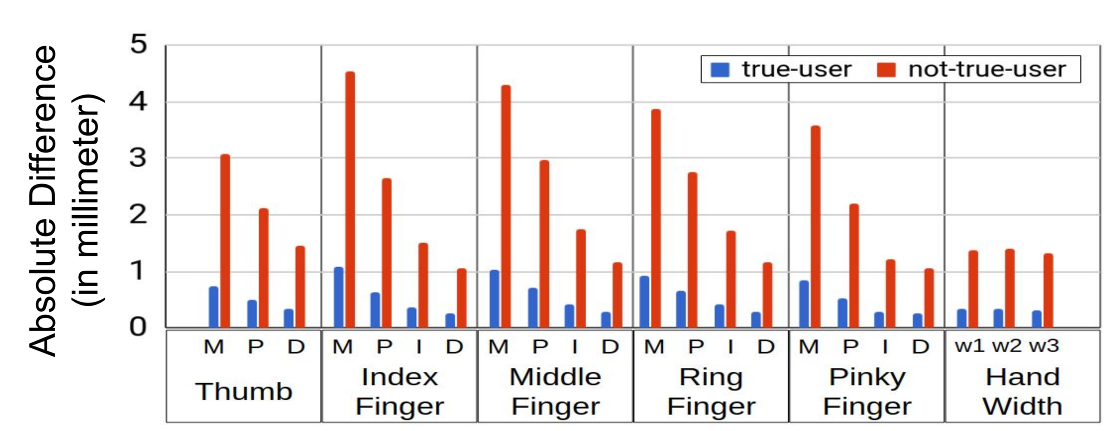
22 Hand Geometry Features:

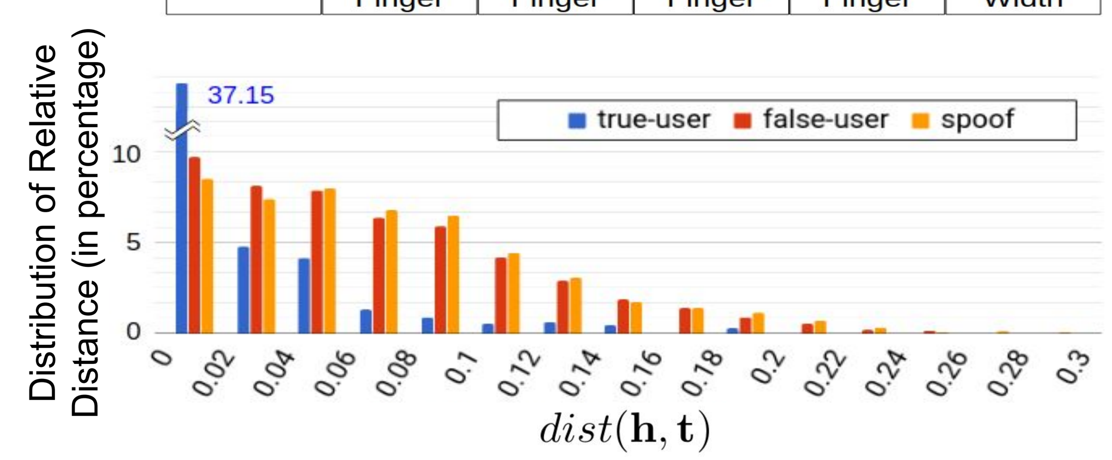
$\mathbf{h} = (M_T, P_T, D_T, M_{IF}, P_{IF}, ..., w_1, w_2, w_3)$



Template: $\mathbf{t} = mean(\mathbf{h}^1, \mathbf{h}^2, ..., \mathbf{h}^k)$

Distance: $dist(\mathbf{h}, \mathbf{t}) = \frac{1}{22} \sum_i \frac{\mathbf{h}_i - \mathbf{t}_i}{\mathbf{t}_i}$



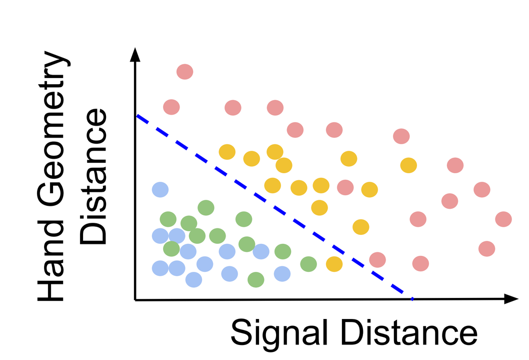


Score Fusion and Decision Making

$$score = dist(S, T) + w_1 dist(\mathbf{h}, \mathbf{t}) + w_2 |l_T - l_R| / l_T$$

- if score < decision_threshold : **accept**.

  else : **reject**.
- decision_threshold can be adjusted to trade off security and convenience.
- w_1 and w_2 are parameters. (w_1 = 0.4, w_2 = 0.05)



Dataset and Preprocessing

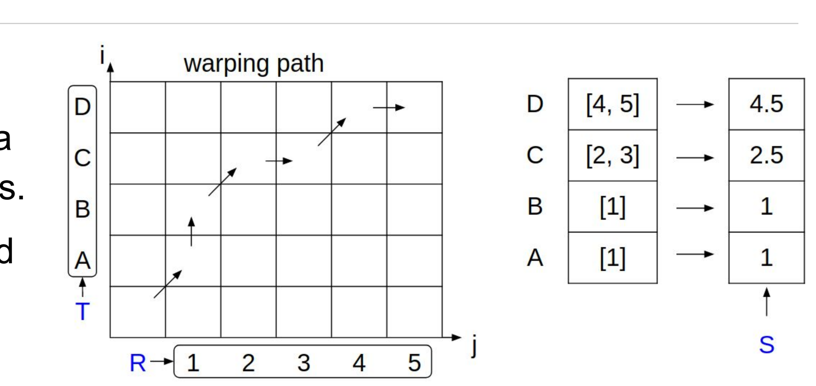
- 200 passcodes created and written by 100 users, 5 + 5 repetitions to simulate sign-up and sign-in.
- 7 impostors write the same content (all 200 passcodes) as legitimate users write, 5 repetitions each.
- 44 passcodes by 22 users are tracked for 4 weeks, on average twice a week, 5 repetitions each time.

Preprocessing Steps:

Step 1) Interpolate missing samples;
Step 2) Derive velocity and acceleration;
Step 3) low-pass filtering (< 10 Hz);
Step 4) Trim the start and the end when hand stays still;
Step 5) Hand posture normalization (pointing to x-axis);
Step 6) Down-sample the signal to 50 Hz;
Step 7) Amplitude normalization (individually on each axis).

Signal Alignment Steps:

- First, run dynamic time warping on R and T to obtain a warping path, with a window constraint of ±50 samples.
- Then each sample of the aligned signal S is calculated by taking the average of a range of samples in the original signal mapped to T on the warping path.



Conclusions and Future Work

Conclusions: Multifactor authentication with in-air-handwriting and hand geometry has **good potentials**.

Limitations:

- Constraints on user behavior, e.g., user must write within the field of view of the camera.
- Parameter tweaking and template protection on the server.
- User needs to remember the content of the in-air-handwriting (same as password).

Future Work:

- An in-depth study on the influence of passcode content, length, and strength.
- Larger dataset, more users, longer tracking time (several weeks).
- Advanced score fusion mechanism (beyond weighted sum).