Enhanced In-air Signature Verification via Hand Skeleton Tracking to Defeat Robot-level Replays

Zeyu Deng, Long Huang, Chen Wang

Department of Computer Science

Louisiana State University

Email: zdeng6@lsu.edu, lhuan45@lsu.edu, chenwang1@lsu.edu

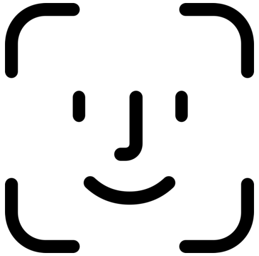
ACSAC 2023

Current Authentication Methods

- **Knowledge-based secret**
  - PIN/password
  - Patterns

Static Authentication Input:
- **Can be lost, stolen, forgotten**
- **Can be spoofed and replicated**

- **Physiologic**
  - Fingerprint
  - Iris



Emerging Behavioral Biometric Authentication

- **Verifying dynamic motion characteristics**
  - Gait patt
  - Body mo
  - Keystrok

Hard to be copied or reproduced

Less dependent on dedicated hardware

- **In-air 3D signature is one representative of behavioral biometrics**

In-air 3D signature

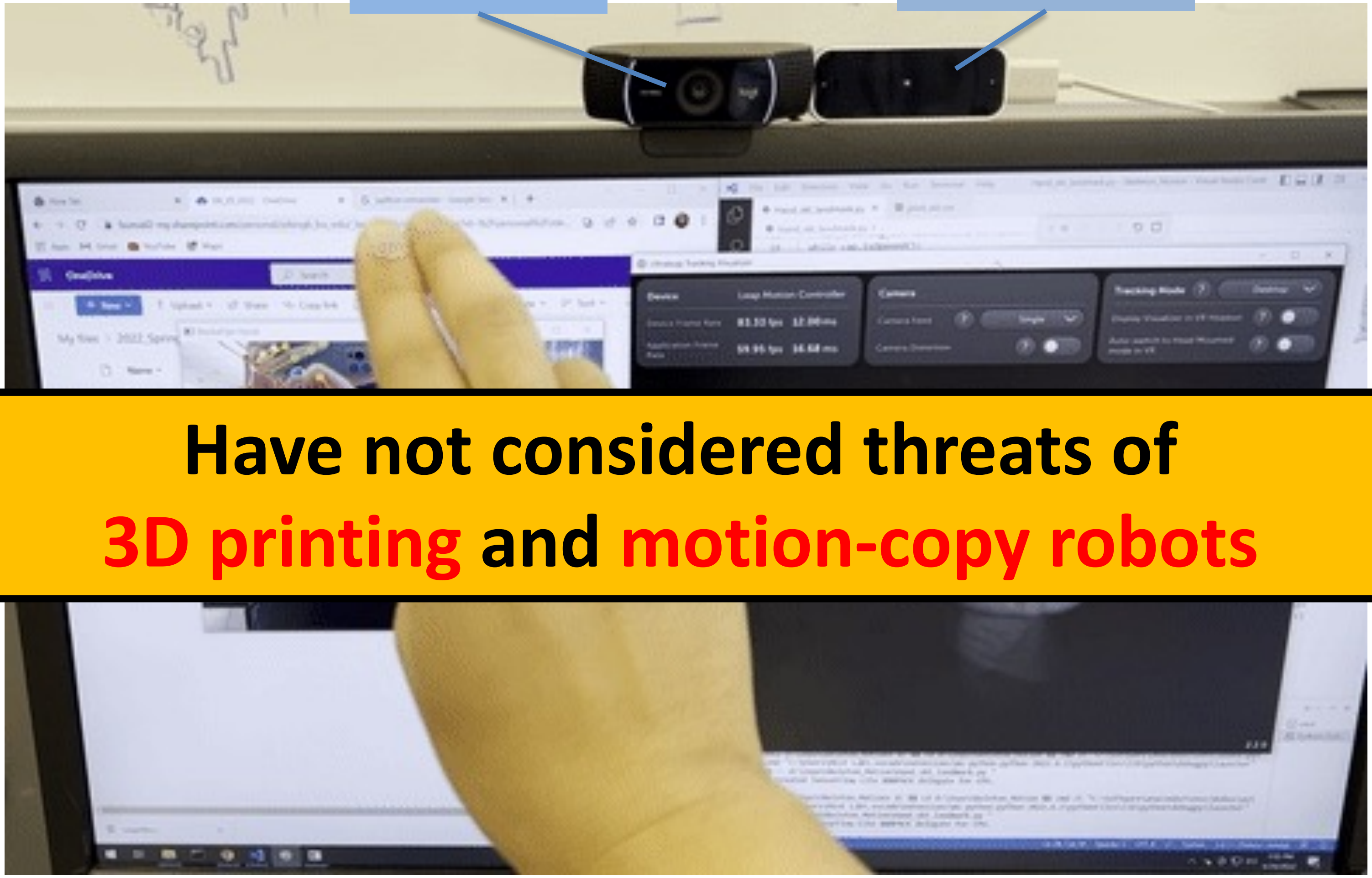
- **Representative behavioral biometric authentication**
- **Inherits the traditional signature's legal effect**
- **Enhanced security**
  - 3D handwriting curves
  - Signing behaviors
- **Eliminates the need for a writing surface**
- **Supported by existing hand-tracking interfaces**

Current hand-tracking interfaces

RGB camera

or

Depth Camera



Have not considered threats of 3D printing and motion-copy robots

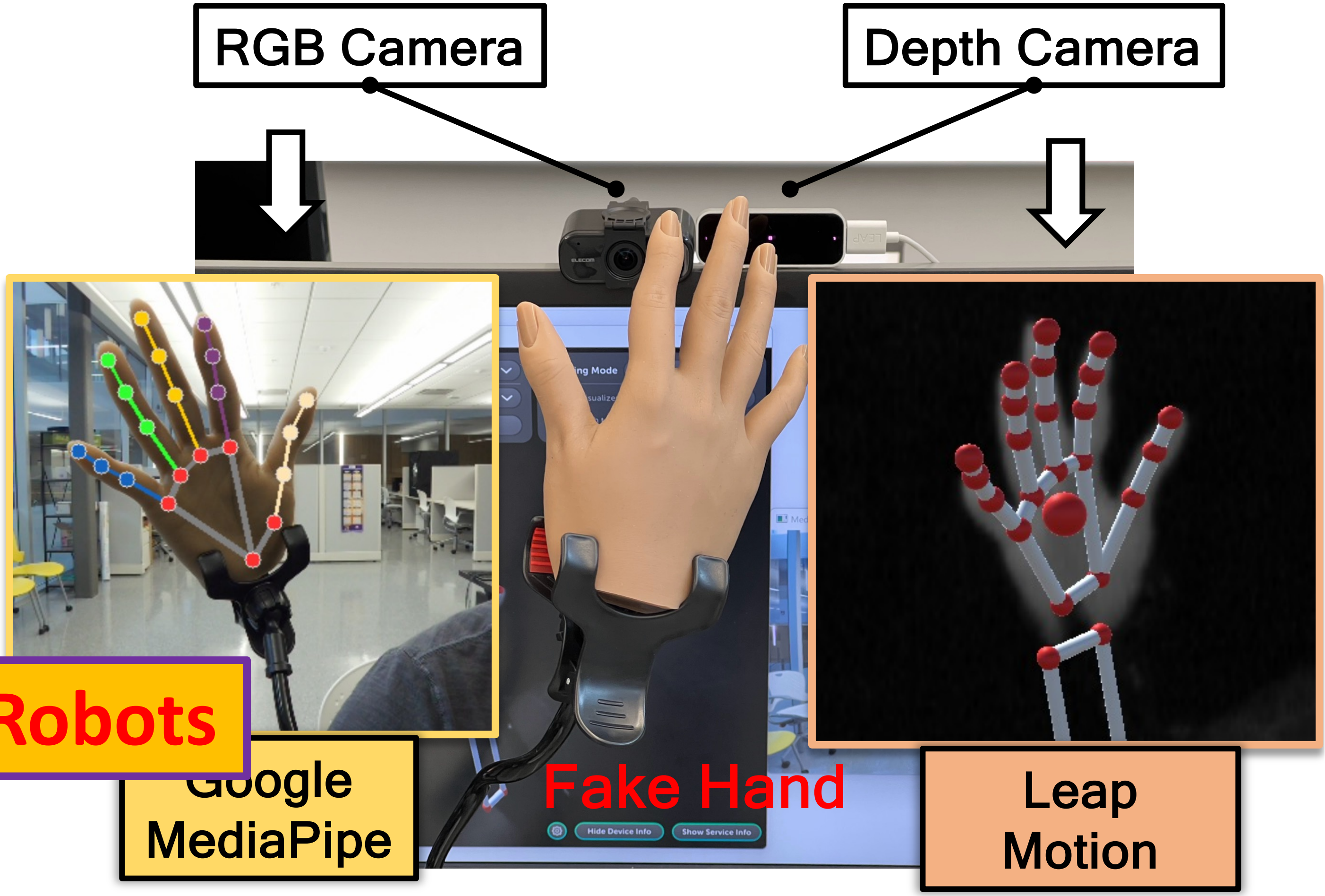
Vulnerabilities of Hand Tracking Interfaces

- ❑ Rely on the hand-like shape to recognize/track the hand

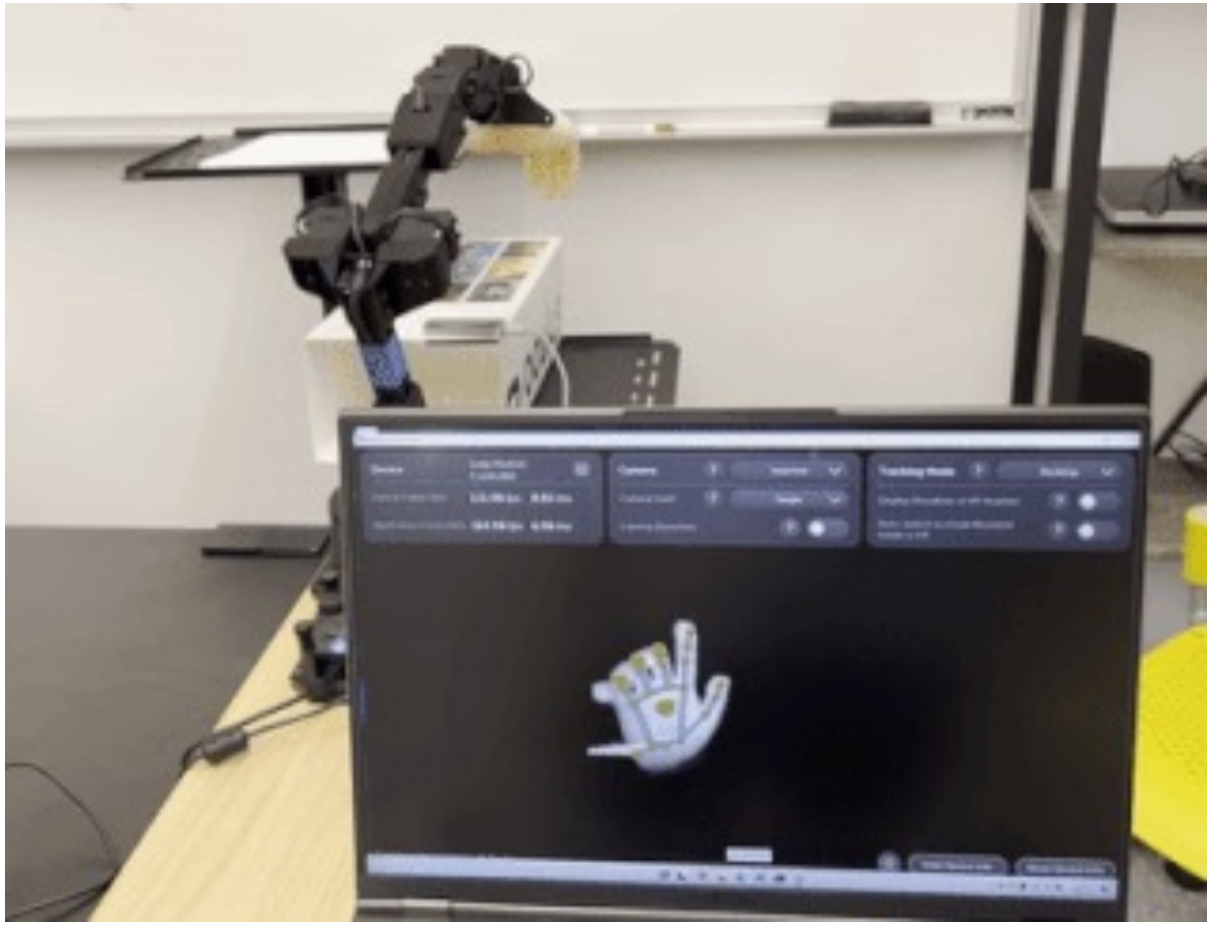
Forged by 3D Printed Hand

- ❑ In-air signature is based on a single-point trajectory

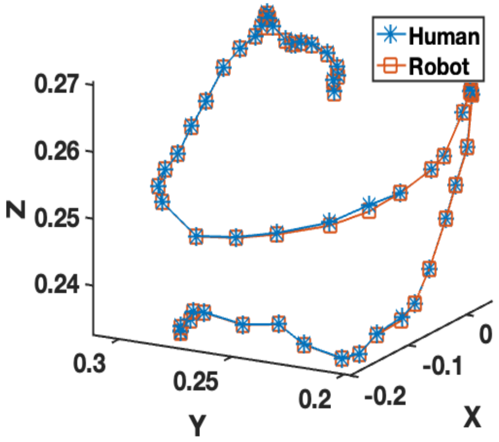
Reproduce by Motion-copy Robots



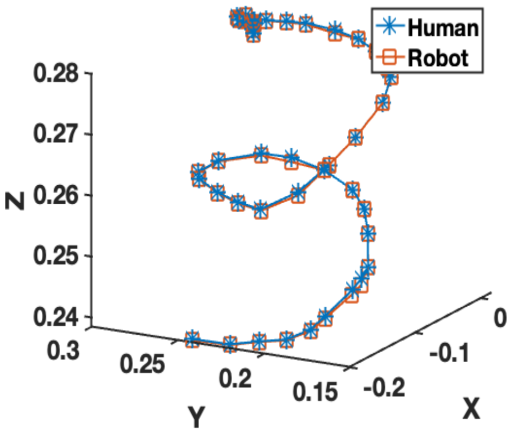
Attack Strategy: Point-to-Point Robot Replay



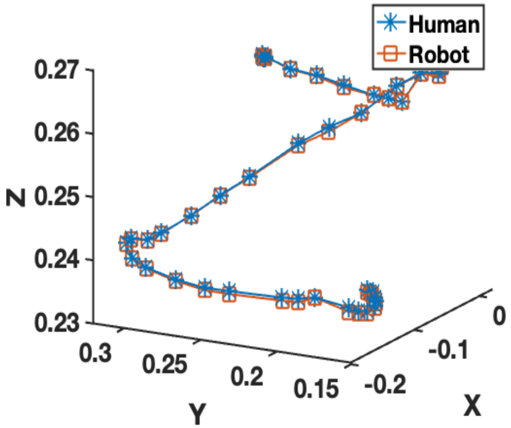
Write an ``S''



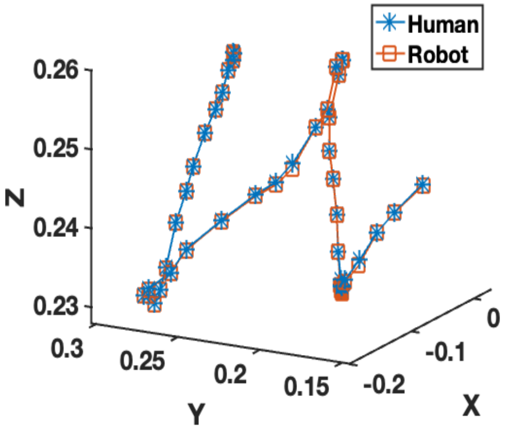
Write a ``3''



Write a ``Z''

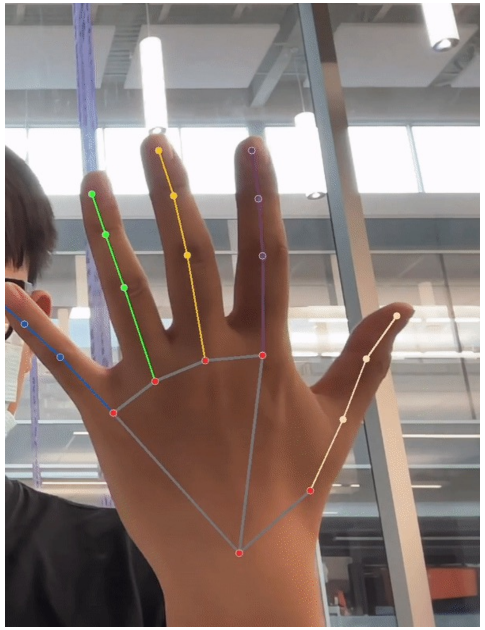


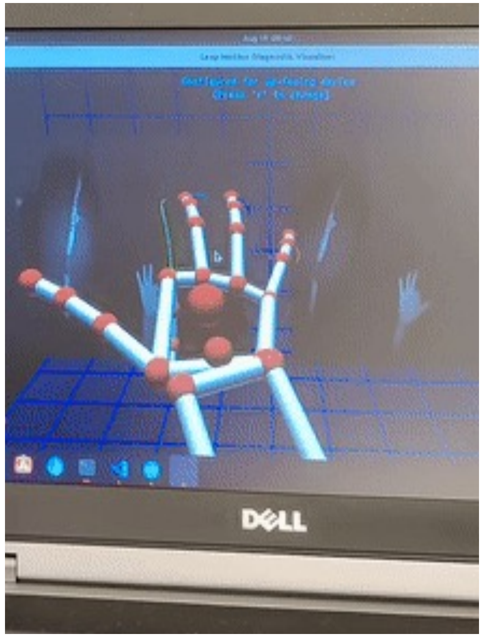
Write a ``W''



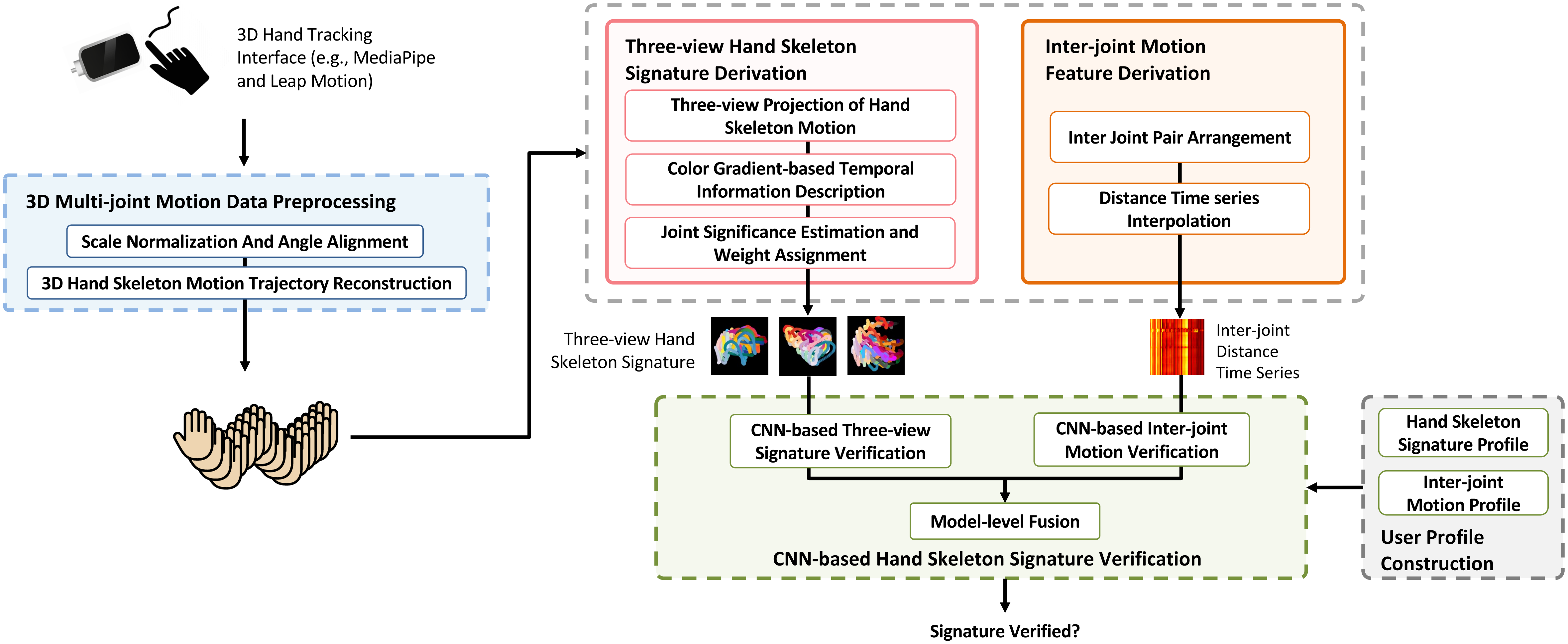
Defense Against Robot Replays

- **Current robots are still not able to copy hand-joint-level motions**
- **Novel hand joint-level authentication**
  - Extend the dimension of in-air signatures from a single point to multiple hand joints
  - Leverage the hand's kinematic structure motions to prevent robot replays



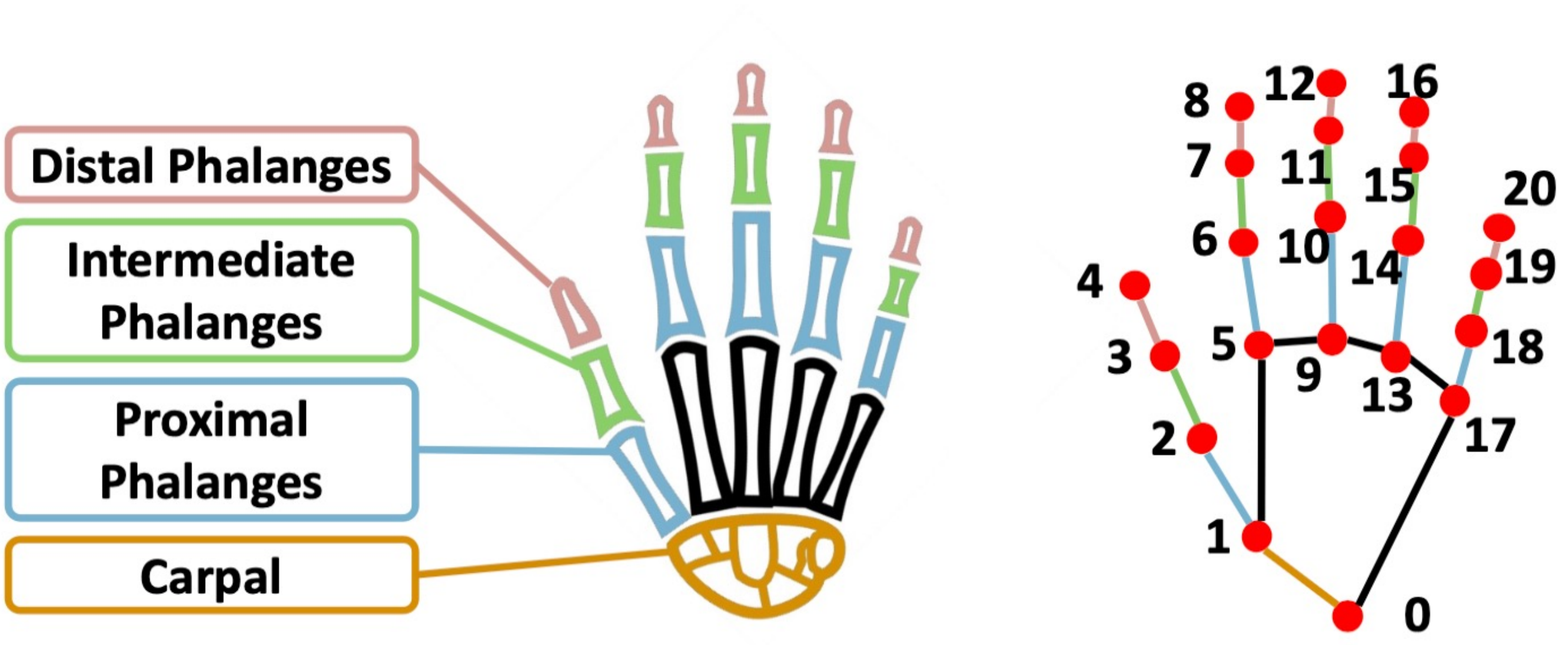


3D Hand Skeleton Signature System



Hand Skeleton Motion Data Extraction

- 3D landmarks of a hand captured by visual sensor
- Examine 3D in-air signatures based on a novel graphical representation



Multi-joint Data Normalization and Alignment

❑ Camera placement

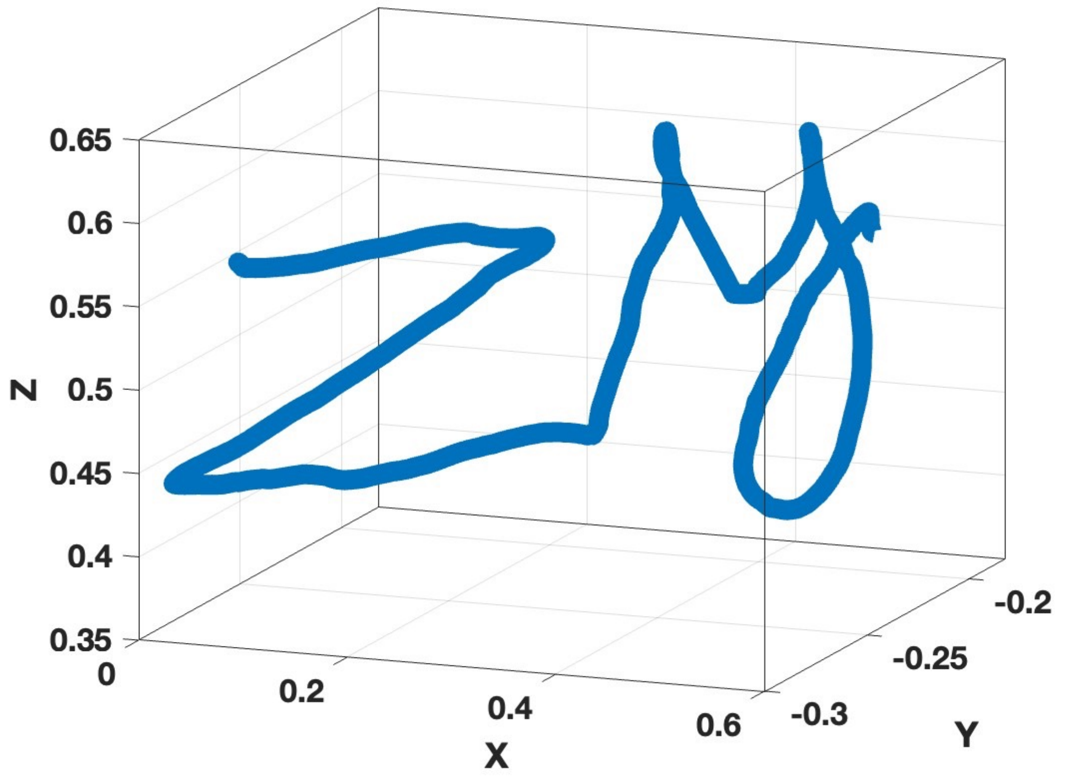
- Predefined direction alignment
- Hand size normalization

❑ Inconsistent signature curve

- Trajectory normalization

❑ Varying signing speed

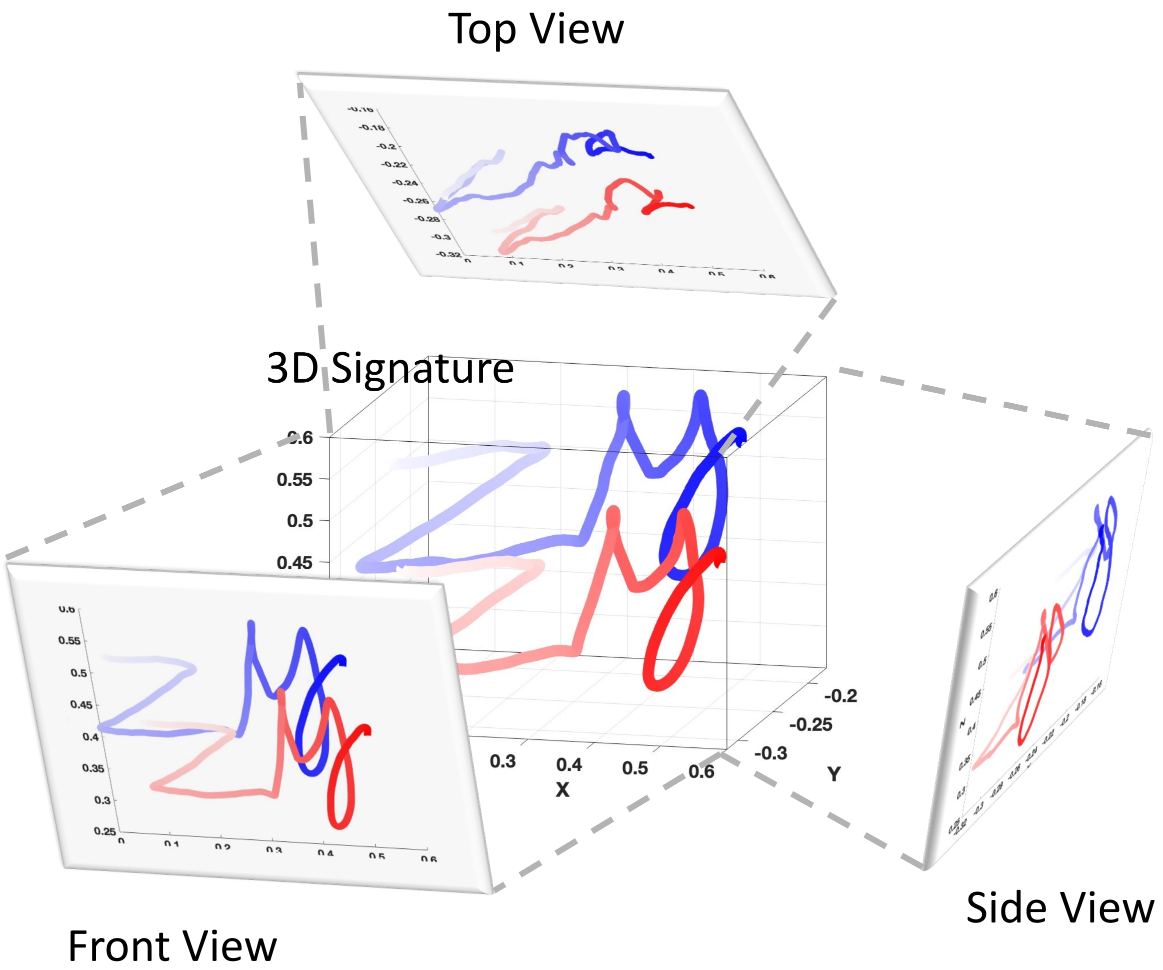
- Trajectory interpolation



Joint-level Motion Features Presentation

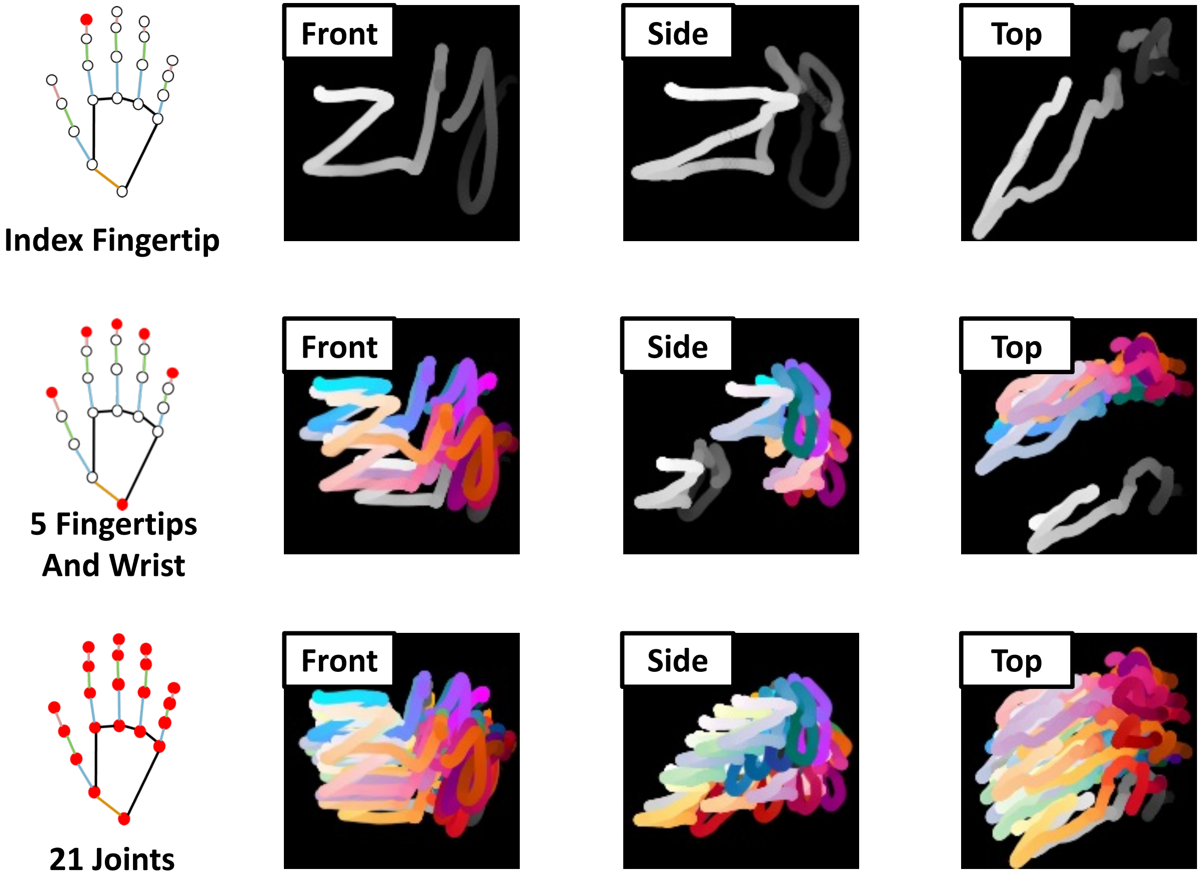
- **Hand skeleton signature**
  - Signature trajectory
  - Signing behavior
  - Hand geometry

- **Integrate time information**
- **Examine from 3 different perspectives**



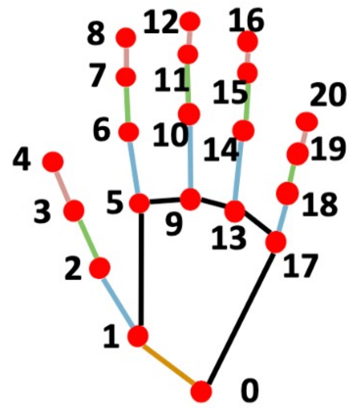
Three View-based Biometric Feature Presentation

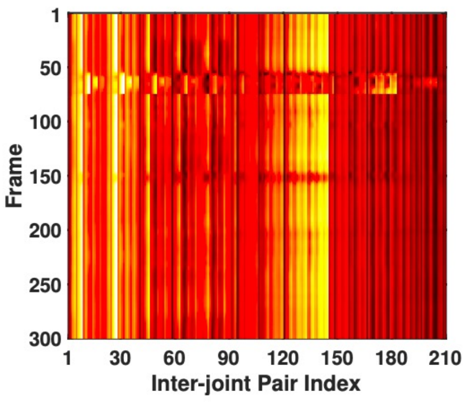
- ❑ **Presenting spatial information**
  - – Three-view projection
- ❑ **Presenting temporal Information**
  - – Gradient color from light to dark
- ❑ **Joint significance weight assignment**



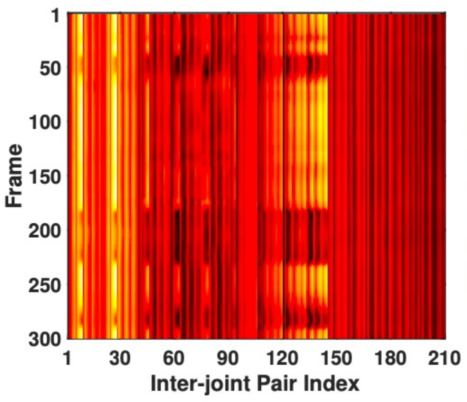
Inter-joint Motion Feature Derivation

- **Relative distance relationships between hand joints**
  - Distinguish users
  - Indicate human or robot replay
- **Inter-joint motion profile: variance over time**

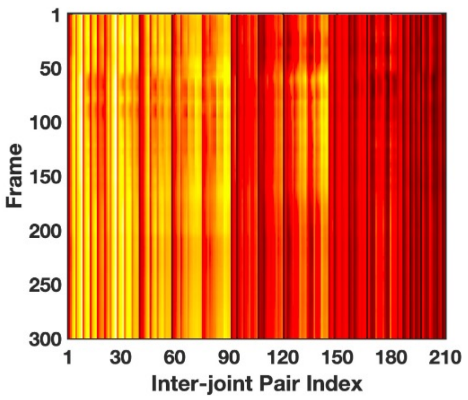




(a) User 1.



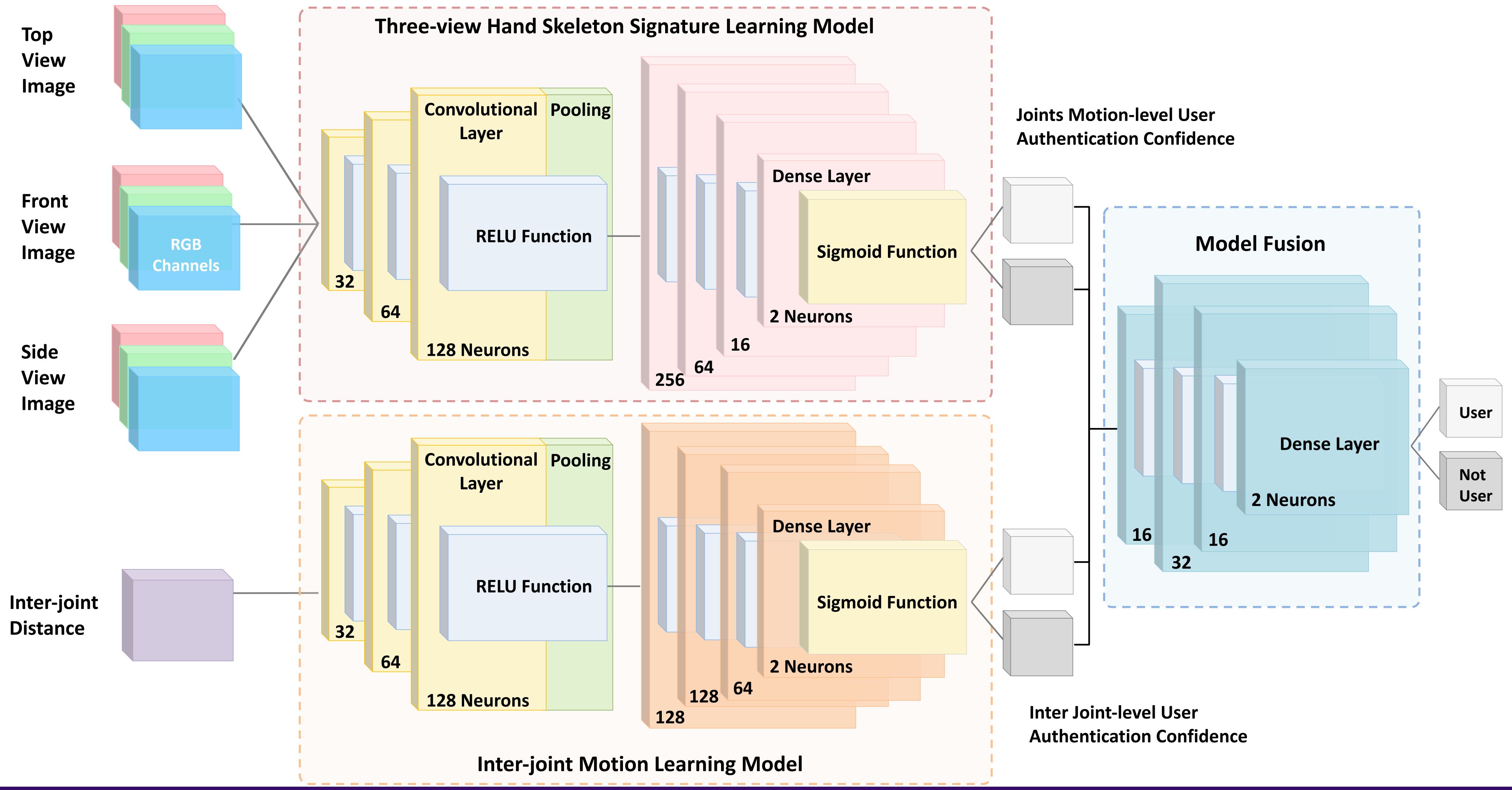
(b) User 2.



(c) User 1 replayed by a robot & 3D-printed hand.

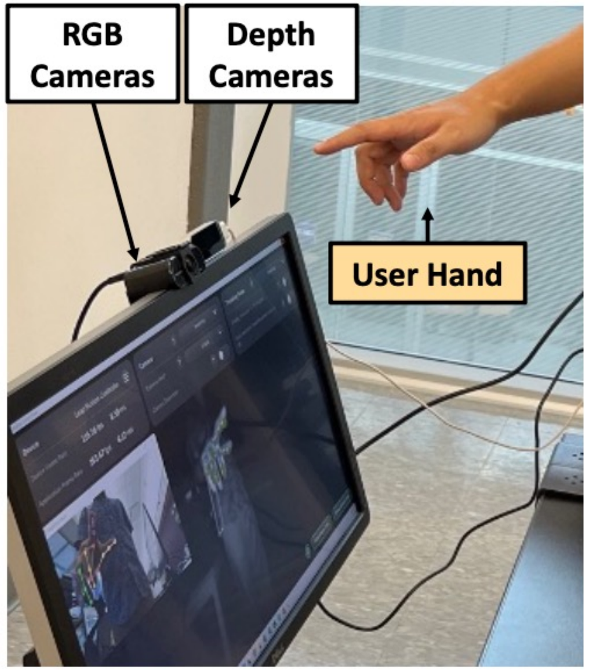
Joint	Avg. Score	Joint	Avg. Score
0	1.82	11	3.22
1	2.23	12	4.62
2	2.55	13	1.02
3	3.59	14	1.40
4	4.51	15	2.28
5	0.75	16	3.09
6	1.57	17	1.35
7	4.43	18	1.47
8	8.38	19	2.01
9	0.78	20	2.41
10	1.40		

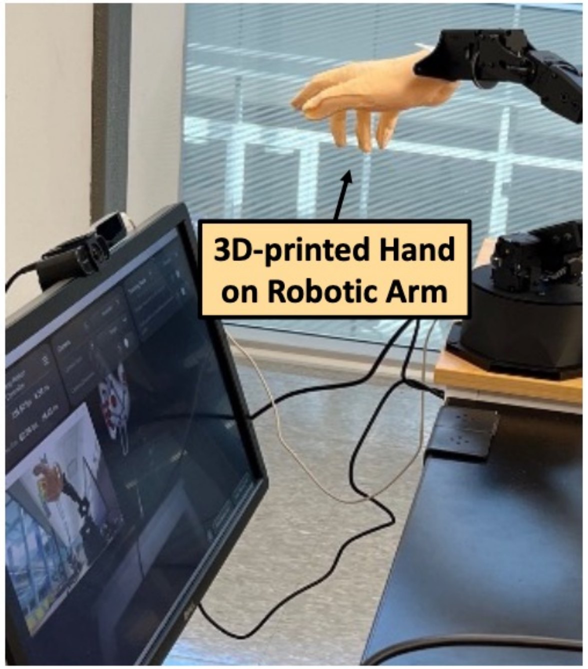
CNN-based Authentication Algorithm

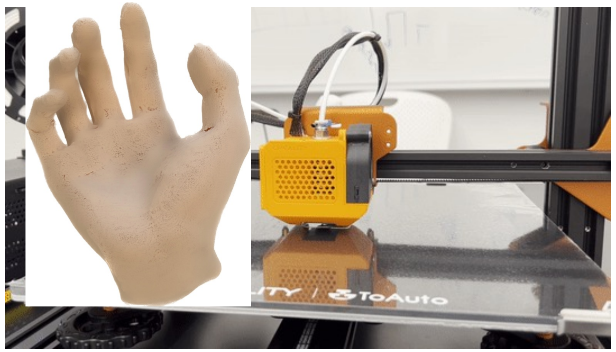


Experimental Setup

- **Commercial hand-tracking interfaces**
  - Google MediaPipe
  - Leap Motion
- **Off-the-shelf Devices**
  - Regular RGB camera (ELECOM Webcam)
  - Depth camera (Leap Motion Controller)
- **Data collection**
  - 25 participants
  - Name initials and ``ABC''
- **Robot replay attack Implementation**
  - Hidden camera for eavesdropping
  - A low-cost robotic arm for replay - PincherX 150
  - 3D-printed hand of the user

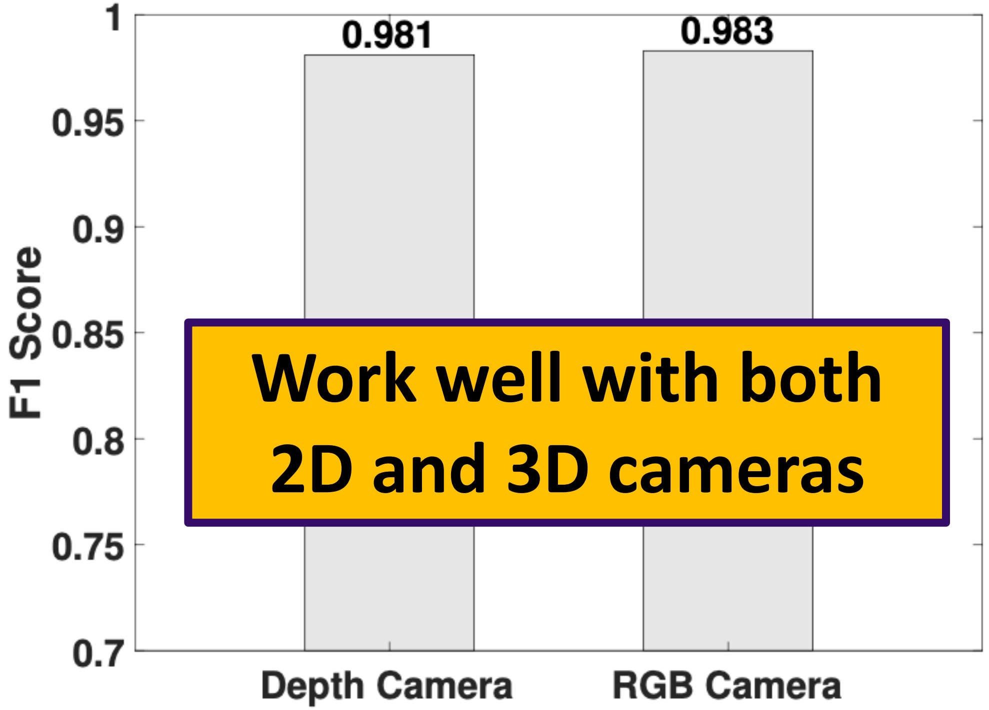






User Verification Performance

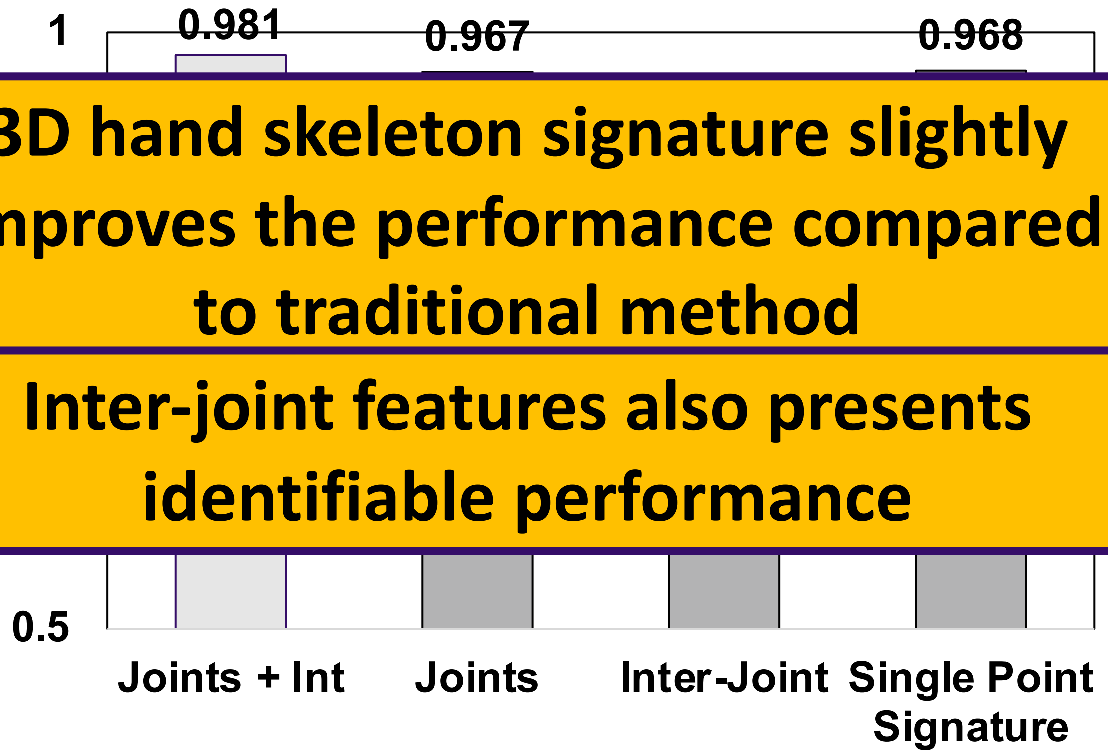
Different Motion Capture Devices



Work well with both 2D and 3D cameras

Multi-joint vs. Single-point

Joint vs. Inter-joint

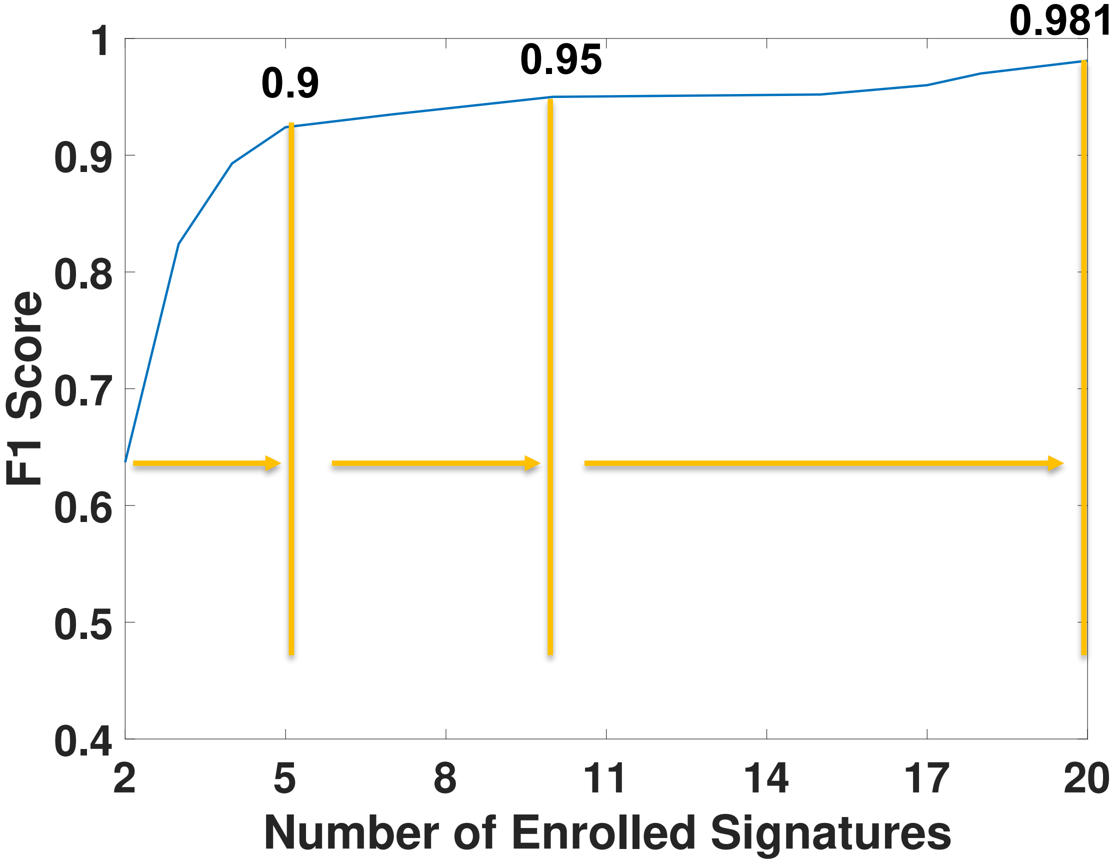


3D hand skeleton signature slightly improves the performance compared to traditional method

Inter-joint features also presents identifiable performance

Enrollment Efforts

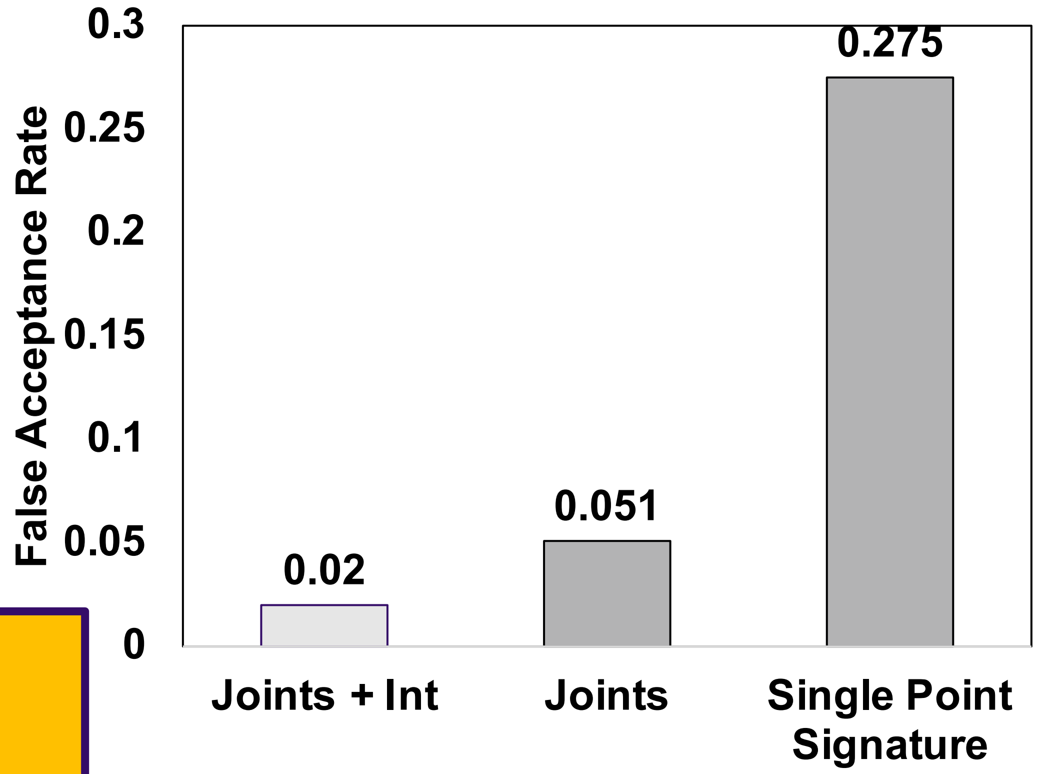
- Increasing the training data size improves the system's performance but requires higher enrollment efforts.



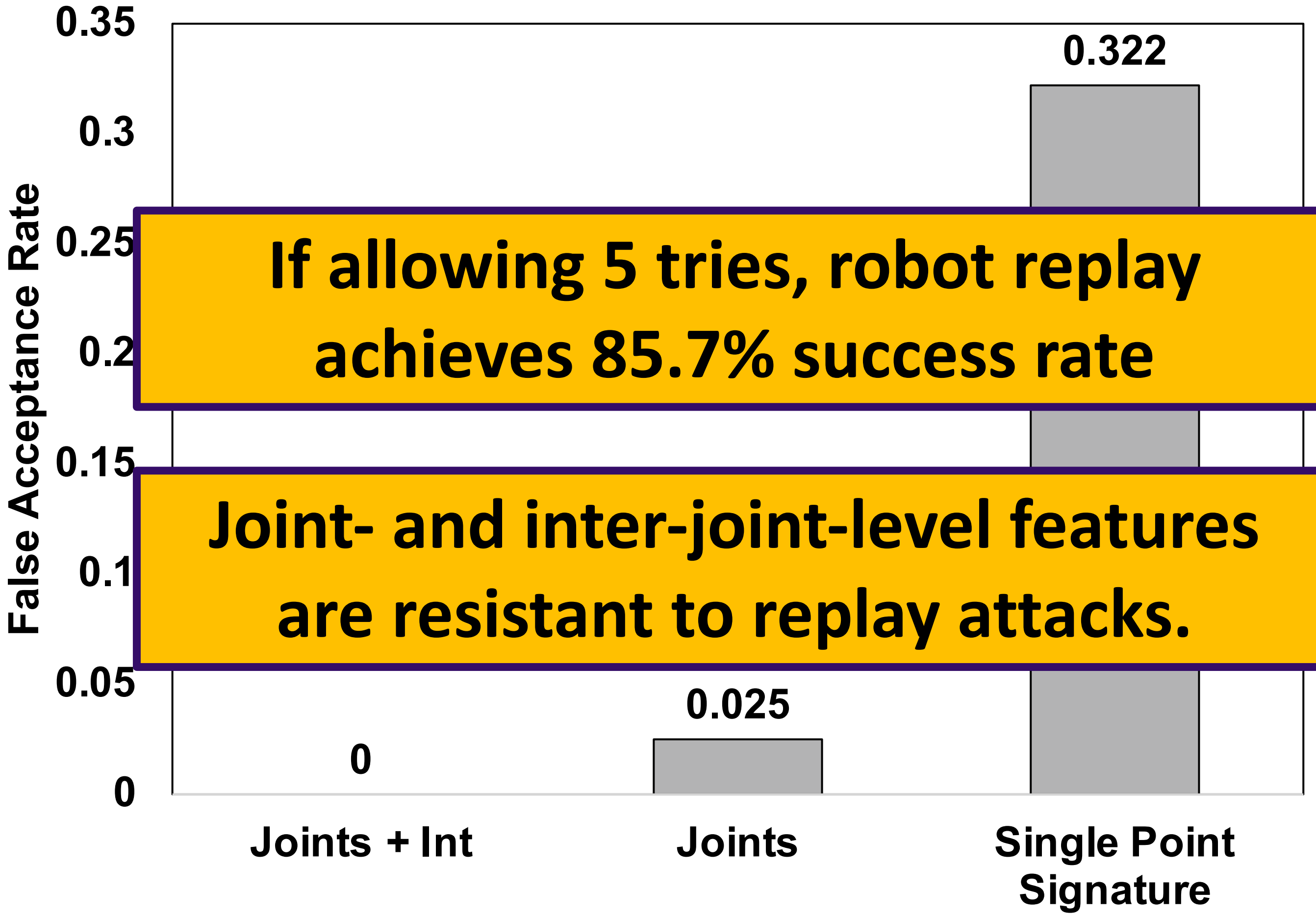
Security Under Impersonation Attacks

- Traditional single-point signature
  - Relatively easy to imitate by an adversary
  - Suffers highly from the visual tracking errors incurred by occlusion or self-occlusion

Multiple joints compensate for the partially occluded hand and examines hand skeletons' inherent behaviors



Performance Under Robot Replay Attacks



If allowing 5 tries, robot replay achieves 85.7% success rate

Joint- and inter-joint-level features are resistant to replay attacks.

Conclusion

- Introduce the 3D hand skeleton signature verification system to address emerging motion-copy robot threats
- Propose a novel three-view presentation method to describe hand skeleton motions
- Develop a CNN-based algorithm to verify in-air signatures at both the hand joint level and inter-joint level
- Implement a physical motion-copy robotic arm and demonstrate a new attack that exploits robots and 3D printing
- Experiments show 3D hand skeleton signature system achieves high performance and defeats robot replay attacks

gracias thank you merci

danke

obrigado

eskerrik asko

ευχαριστώ

дзякуй

Hvala

Kiitos

спасибо

met dank

go raibh maith agat

धन्यवाद

grazie

хвала

mahalo

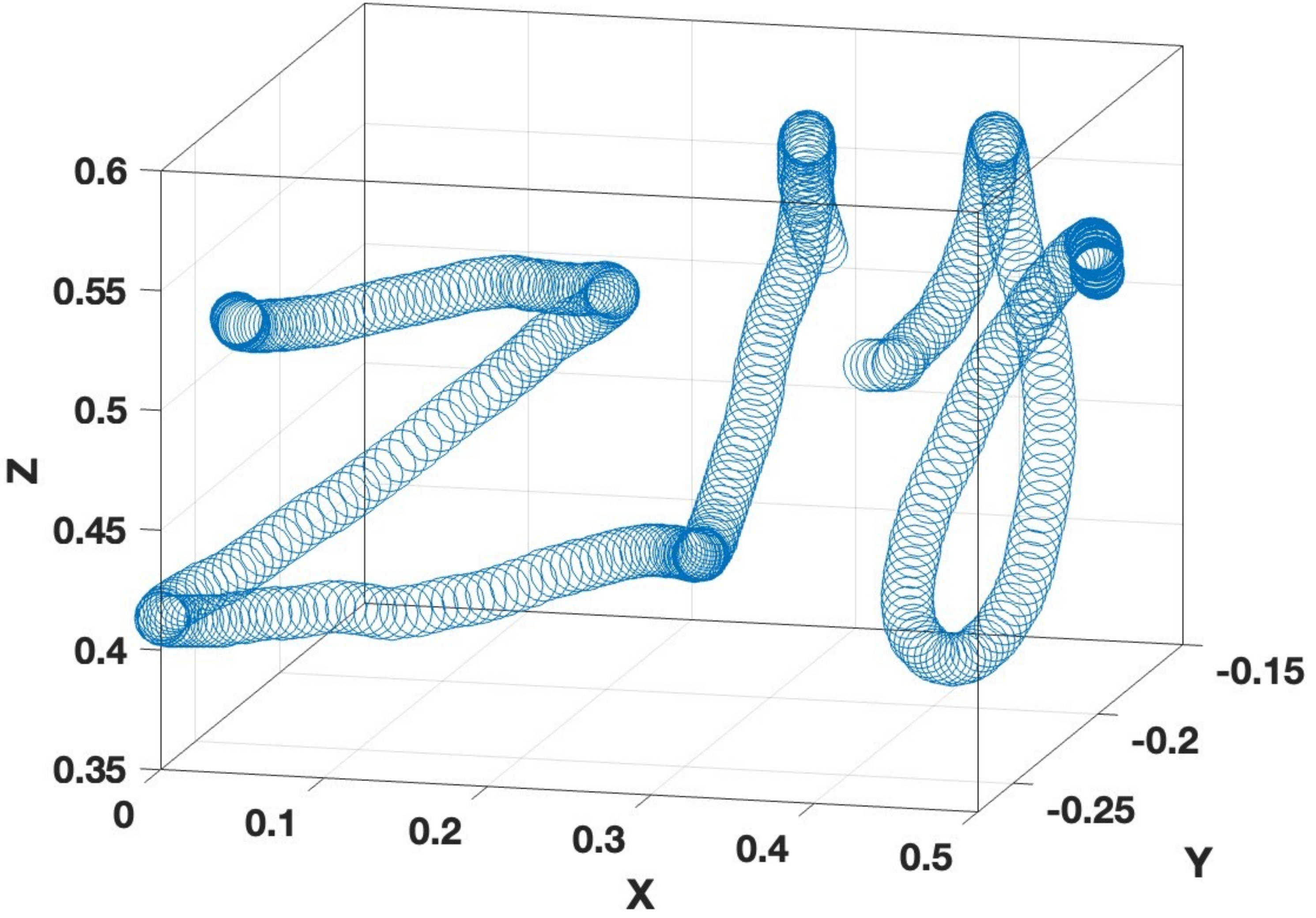
감사해요 谢谢 ありがとう

Mobile and Internet SecuriTy (MIST) Lab

Back up

Signing Behavior

- ❑ Varying speed at turning
- ❑ Minute non-straight line



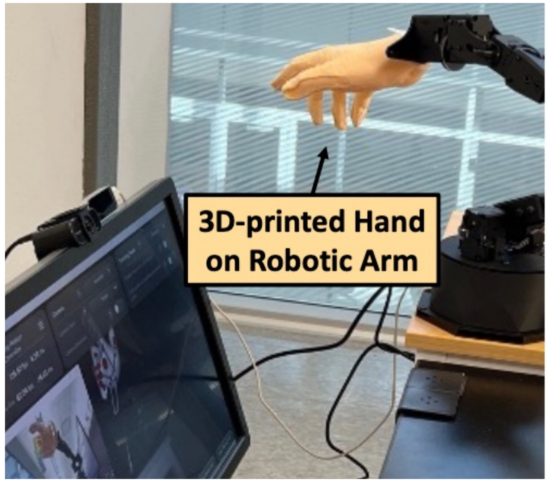
Attack Setup

❑ **Impersonation Attack**

- Obtain the user's name and signing behavior data
- Observe and mimic

❑ Physical Robot Replay

- Access to both the user's 3D hand skeleton model and signature trajectory samples
- 3D scanner and 3D printer

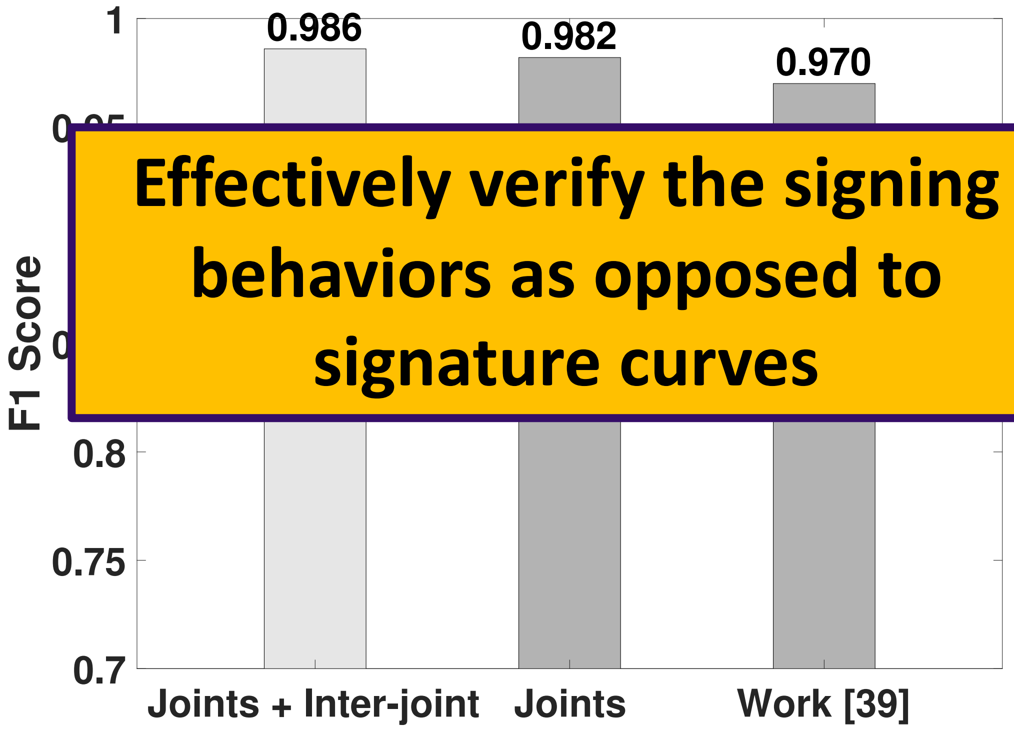


❑ Simulated Robot Relay

- Virtual hand model that precisely followed the user's hand motion data

Verification Performance: Standardized Content

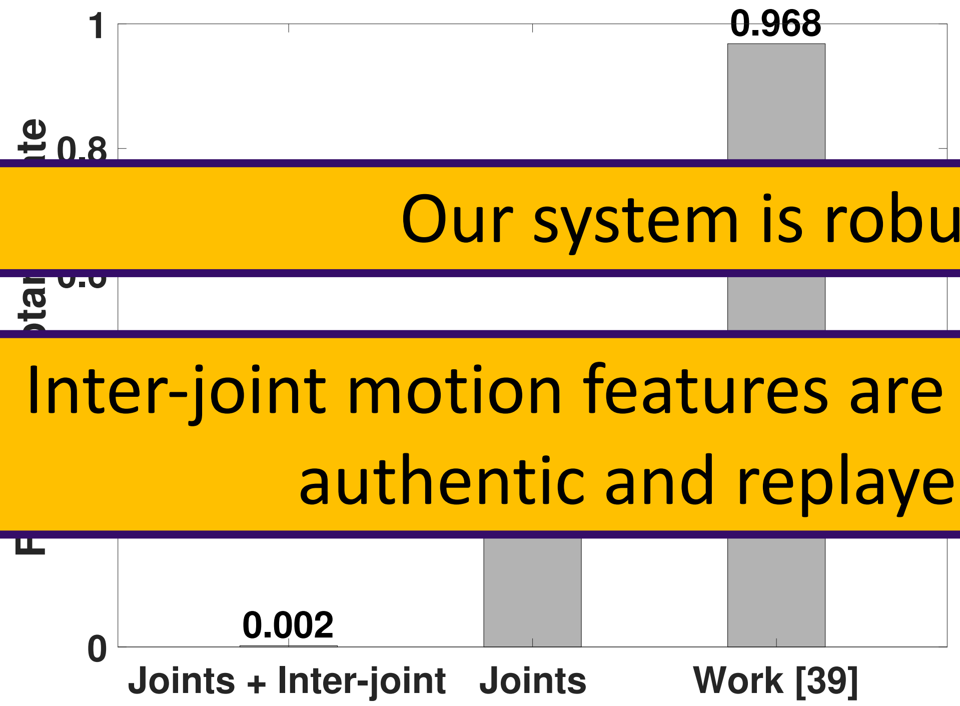
Write out the letters "ABC"



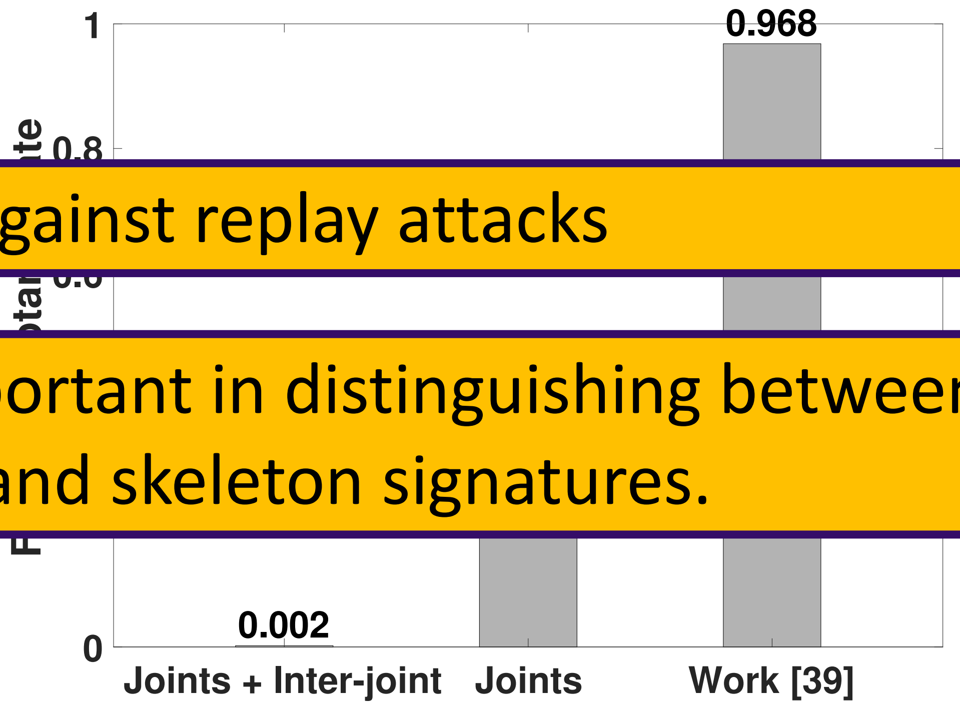
Effectively verify the signing behaviors as opposed to signature curves

Performance Under Simulated Attacks

General Hand Model



User's Hand Model



Our system is robust against replay attacks

Inter-joint motion features are important in distinguishing between authentic and replayed hand skeleton signatures.

Question List

- **3D input?**
  - CNN is most efficient with 2D images
  - Three different perspective, like in 3D modeling
  - Enables us to examine each view more closely
- **Robot capability?**
  - Advancing attack vs. defense
  - Commercial devices consider cost
- **Light condition?**