# Fingerprint Spoof Detection: Temporal Analysis of Image Sequence


**Tarang Chugh**

PhD, Michigan State University

Applied Scientist @ Amazon Inc.

**Prof. Anil K. Jain**

University Distinguished Professor

Michigan State University


 IARPA R&D Contract No. 2017 - 17020200004

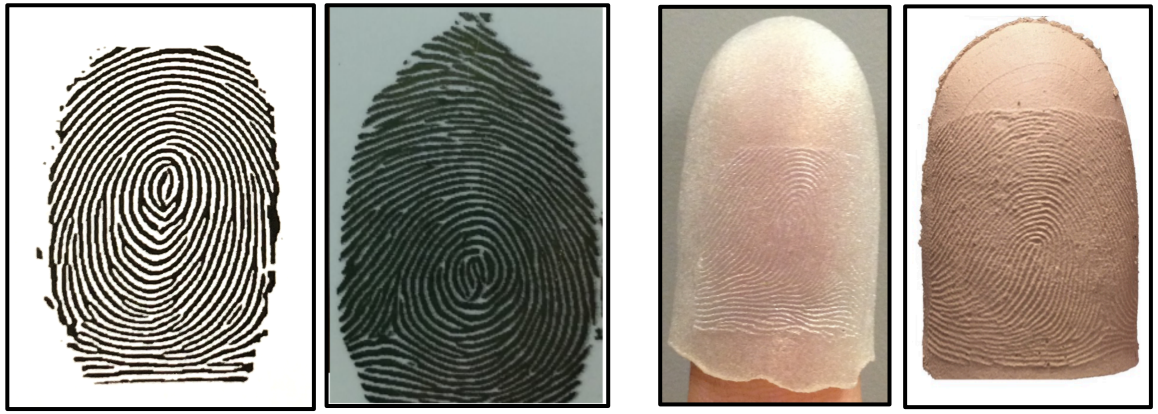
# Fingerprint Presentation Attack Detection

*“presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system”*

- ISO standard IEC 30107-1:2016(E)

Silicone Gelatin Latex Body Paint Play Doh

**Gummy Fingers**

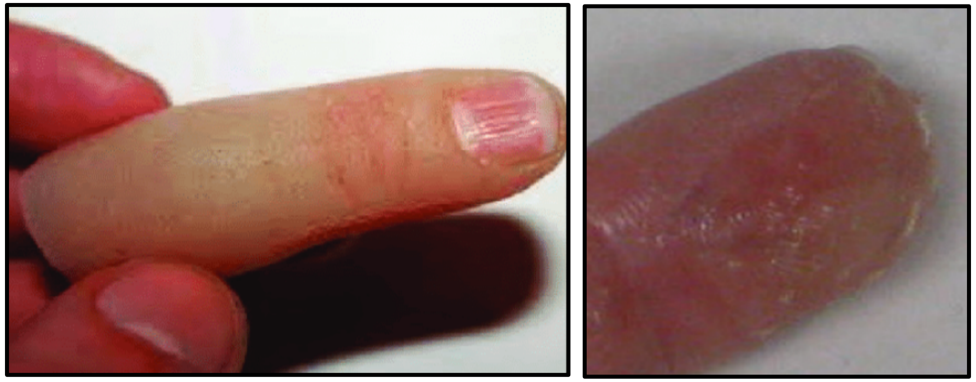


2-D Printed Spoofs 3-D Printed Spoofs

**Printed Fingerprint Targets**

Transplanted skin from sole Acid Burns Stitched Fingers

**Altered Fingers**



**Cadaver Fingers**

# Existing Approaches

- Hardware-based
  - Blood Flow
  - Body Odor
  - Skin Distortion
  - Multi-spectral, multi-view, and OCT scanners

- Software-based
  - Anatomical Features (pore location and their distribution)
  - Physiological Features (perspiration)
  - Texture-based Features
    - Hand-crafted: Weber Local descriptor, Local-contrast phase descriptor
    - Machine-learned: Deep Neural Network-based features

# Proposed Approach

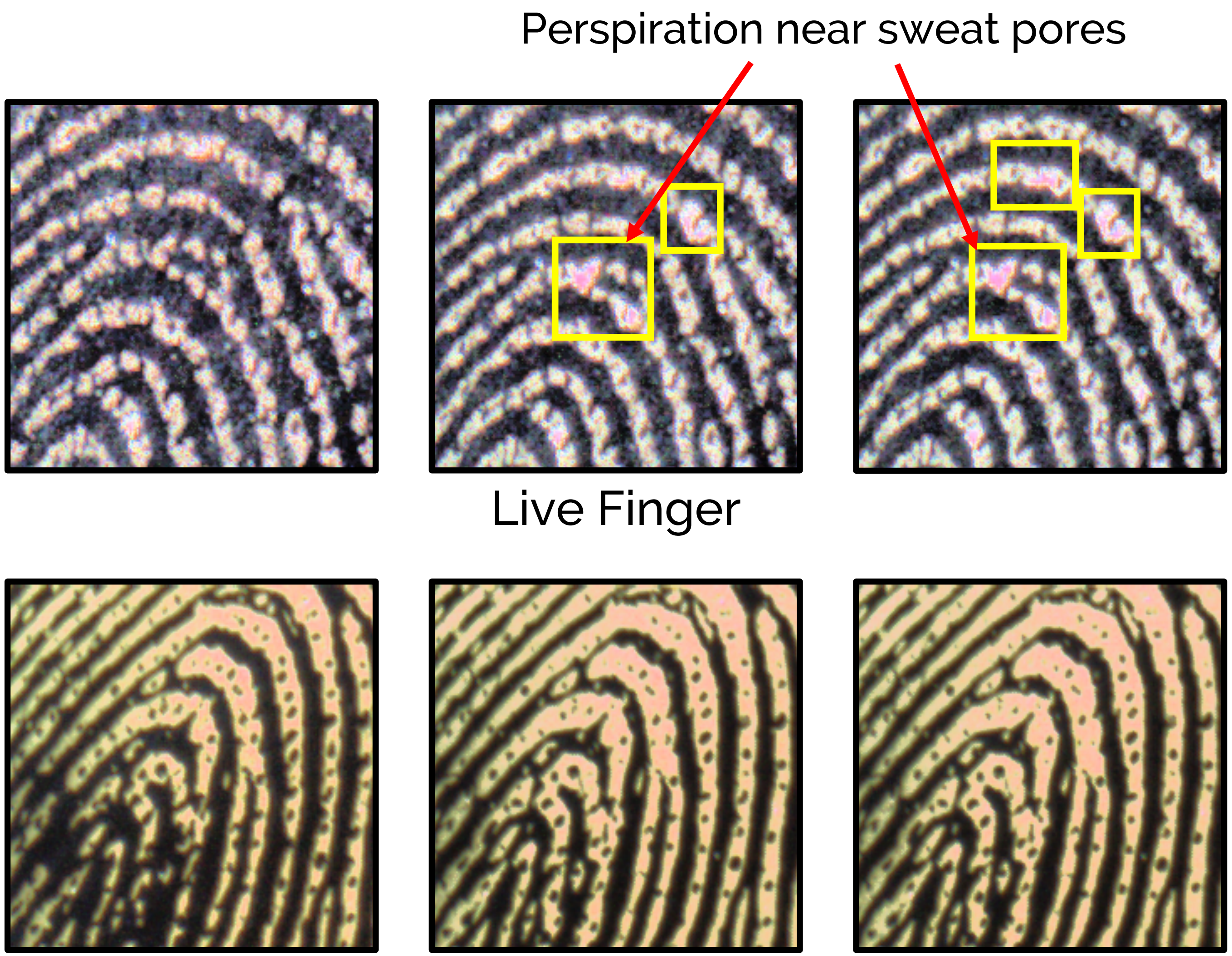
## Spatio-temporal dynamics

- Perspiration
- Skin blanching
- Skin distortion

## Domain Knowledge

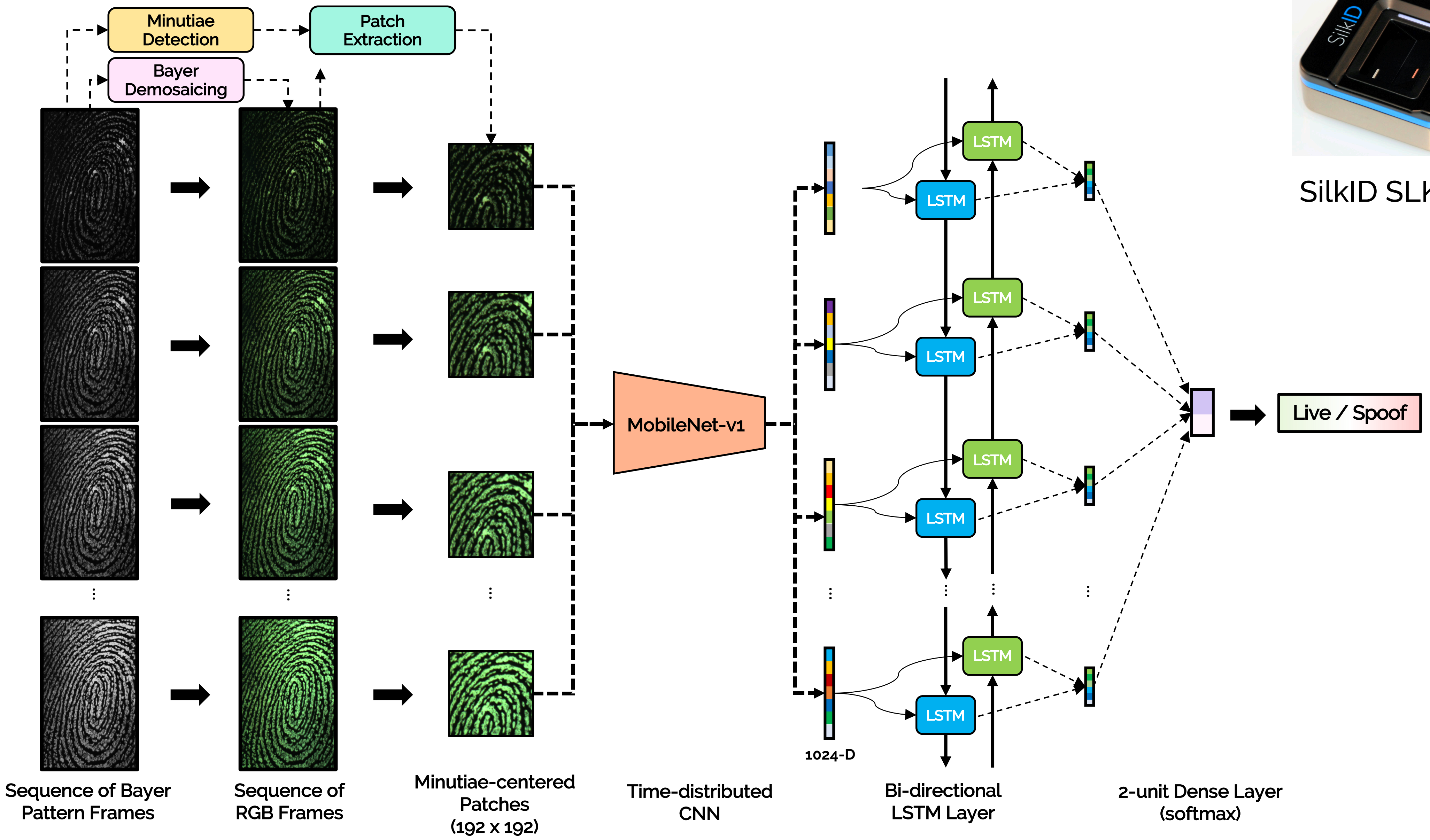
- Spurious minutiae in spoof fabrication process
- Hard to replicate friction ridge information near minutiae with high fidelity

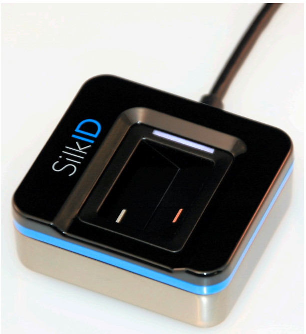
## End-to-end automatic feature extraction and learning



Spoof Finger (Pigmented Third Degree Silicone)

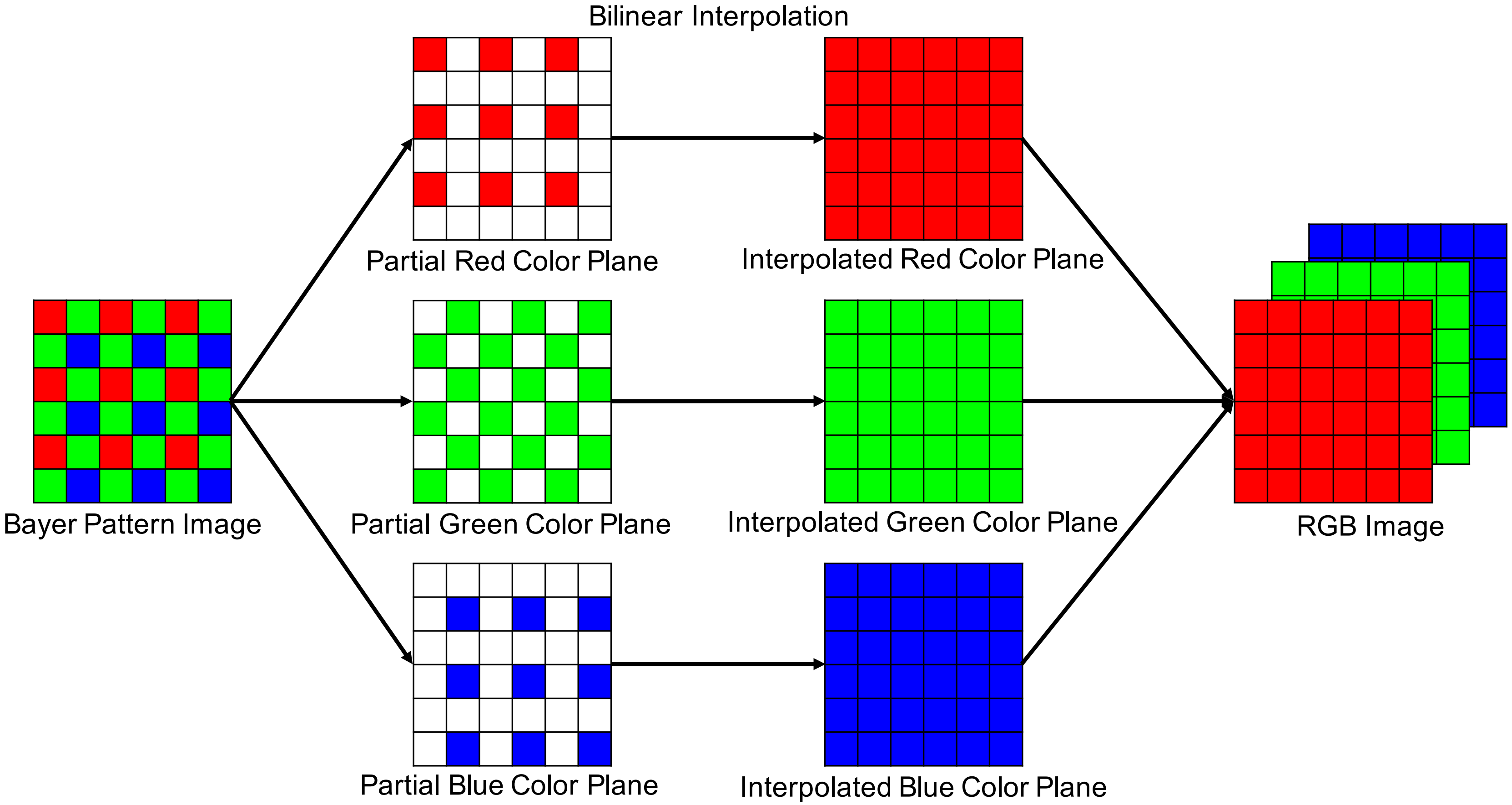
# Proposed Approach



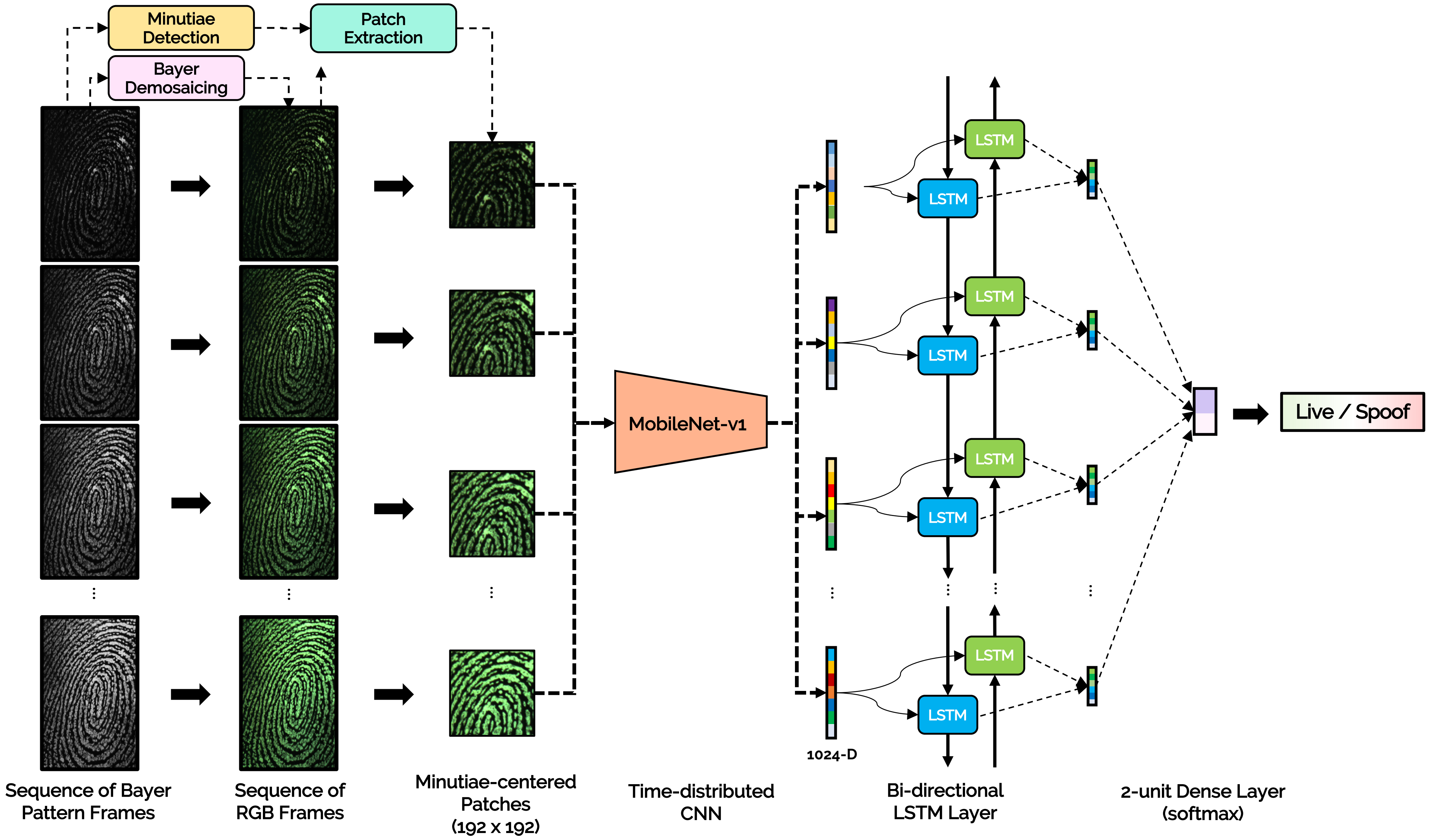

SilkID SLK20R

# Proposed Approach




Bayer Demosaicing

# Proposed Approach

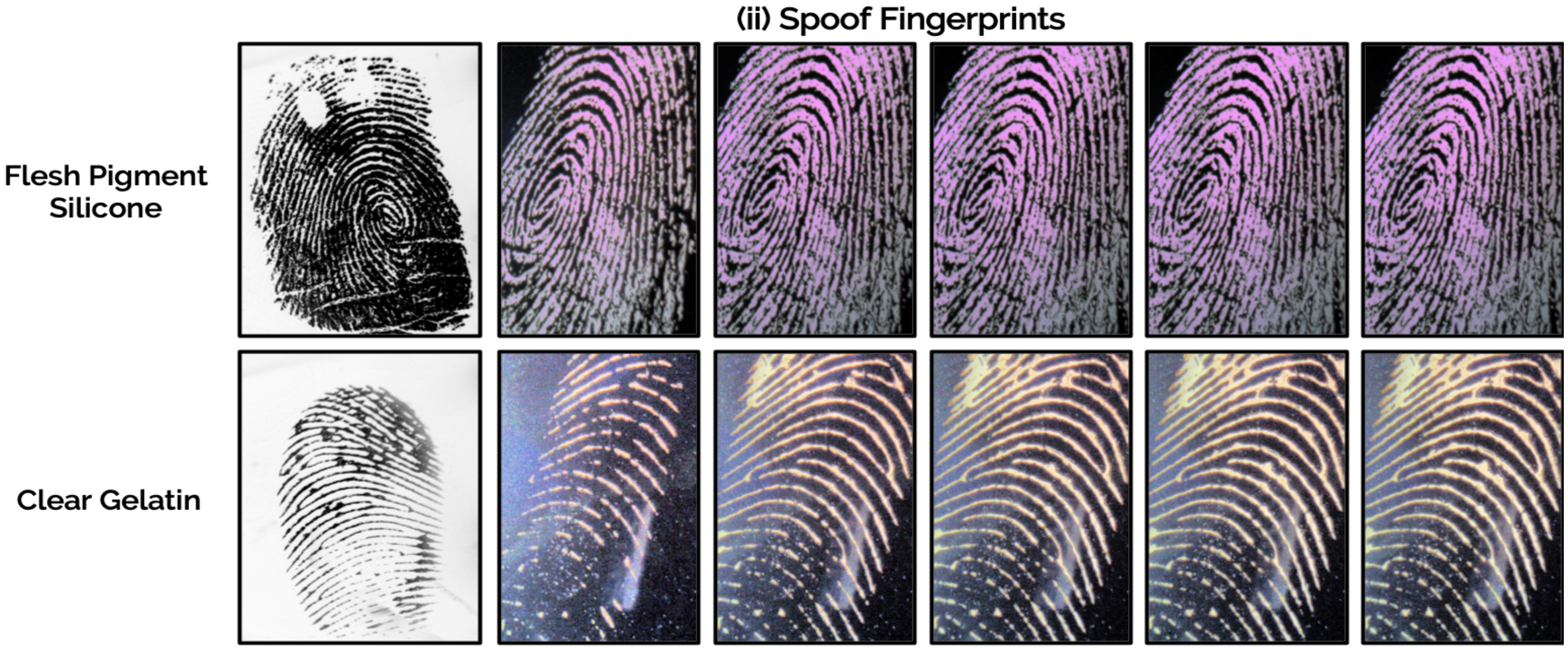


# Experimental Results

- Large Dataset
  - 26,650 Live frames from 685 subjects (1,333 unique fingers)
  - 32,910 Spoof frames (7 spoof materials, 14 variants)

# Experimental Results

- Large Dataset
  - 26,650 Live frames from 685 subjects (1,333 unique fingers)
  - 32,910 Spoof frames (7 spoof materials, 14 variants)



# Experimental Results

Proposed approach achieved state-of-the-art performance in both **Known-material** and **Unknown-material** experiments

| Experiment | SOTA Static Approaches (CNN) | | | Proposed Dynamic Approaches (CNN-LSTM) | | |
|---|---|---|---|---|---|---|
| | Whole-Image | Slim-Res CNN [1] | Fingerprint Spoof Buster [2] | Seq. of whole images | Seq. of Centre of Gravity patches | Seq. of minutiae-based patches |
| **Known-material** | 96.90 | 98.05 | 99.11 | 98.94 | 99.04 | 99.25 |
| **Unknown-material** | 57.31 | 79.85 | 81.65 | 80.62 | 85.75 | 86.20 |

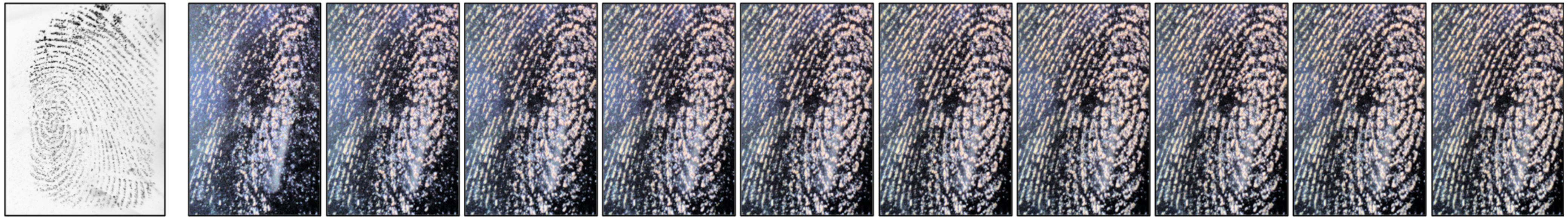
Performance numbers are reported in **True Detection Rate (%) at False Detection Rate** = **0.2%**

Spoof detection time is **< 400ms** on a Nvidia GTX 1080 Ti GPU

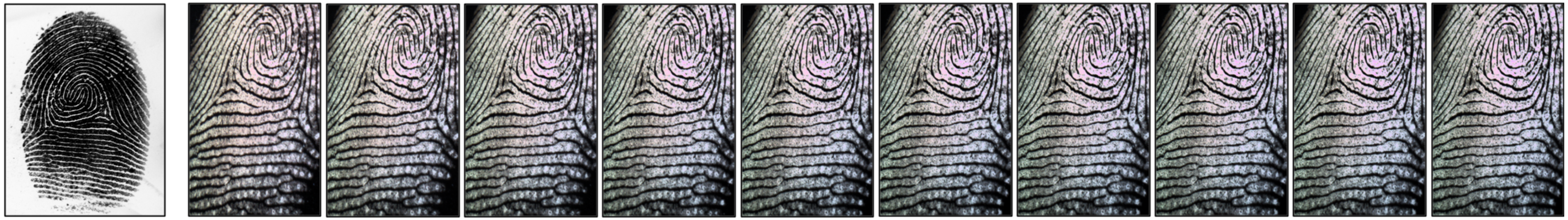
[1] Y. Zhang, D. Shi, X. Zhan, D. Cao, K. Zhu, and Z. Li. Slim-Res CNN: A Deep Residual Convolutional Neural Network for Fingerprint Liveness Detection. IEEE Access, 7:91476–91487, 2019.
[2] T. Chugh, K. Cao, and A. K. Jain. Fingerprint Spoof Buster: Use of Minutiae-centered Patches. IEEE Transactions on Information Forensics and Security, 13(9):2190–2202, 2018.

# Challenging Cases

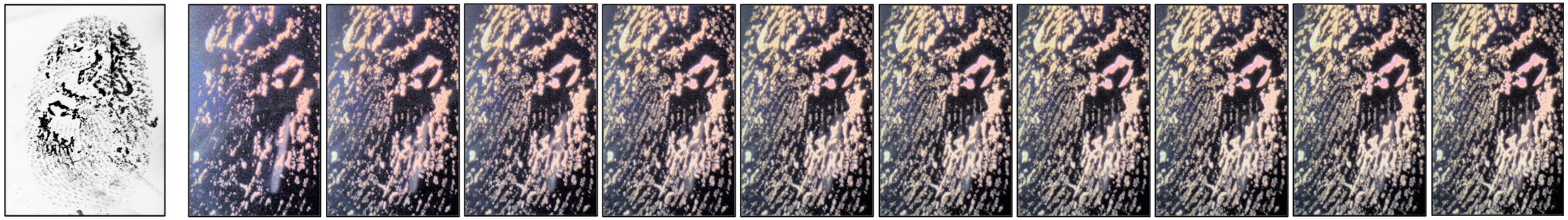
Spoof Fingerprint
(Third degree)



Live Fingerprint



A spoof and a live finger incorrectly classified by static approaches but correctly classified by the proposed dynamic approach.



A heavily damaged live finger is incorrectly classified by all both static and dynamic approaches.

# Thank You