Building Trustworthy and Accessible Provenance Systems for Physical and Digital Artifacts

Bangjie Sun

PhD Candidate | Research Assistant | National University of Singapore

NUS National University of Singapore | Computing

The story of Salvator Mundi ...

Origin
By Leonardo da Vinci

1958
Sold for only £45

2017
Sold for $450M

Provenance

- Something's origin
- A record of ownership; a guide to authenticity or quality

History | Past ownership | Restorations | Hidden layers

The story of Salvator Mundi ...

Origin

By Leonardo da Vinci

Provenance

The value of an artifact depends on our ability to verify its origin, its authenticity and its history.

Modern society relies on provenance to build trust

Physical Domain

e.g., liquids & medicines

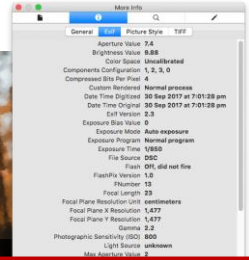
Fragile surface cues

Duplicated & Forged

Labels & Packaging

Digital Domain

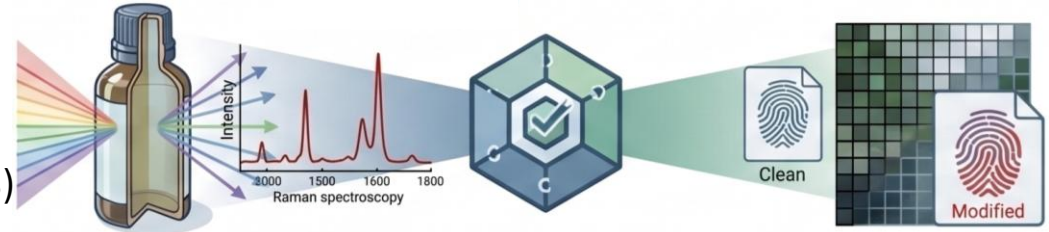
e.g., images & videos



Stripped & Altered

Metadata

Physical Fingerprint: Spectroscopy
(e.g., material properties)



Digital Fingerprint:
(e.g., content-tied traces)

Deployable systems to find fundamental evidence tied to the artifact itself

Extrinsic vs. Intrinsic provenance systems

Physical Domain

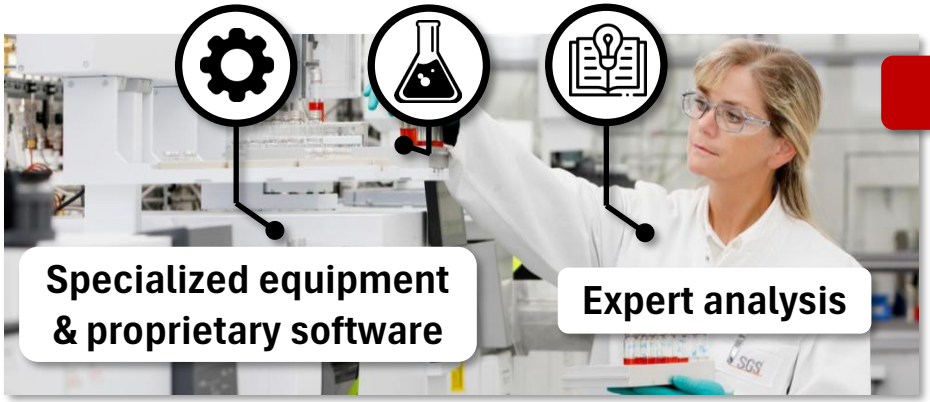
Digital Domain

Extrinsic Provenance

Intrinsic Provenance

Deployable systems to find fundamental evidence tied to the artifact itself

Intrinsic solutions are expensive and inaccessible



Scientific Tools

Democratize Intrinsic Provenance

High-quality RGB cameras

Increasing processing power

With everyday devices

e.g., smartphones, tablets

Intrinsic solutions are expensive and inaccessible

My research focuses on democratizing intrinsic provenance systems with everyday devices.

Research landscape

Extrinsic Provenance

External Labels & Metadata

Blockchain Technology

Database & Logs

Existing Approaches

Intrinsic Provenance

Physical Domain ⟷ **Digital Domain** ⟷ **Latent Domain**

e.g., liquids & medicines

RGB cameras only

Liquid form [MobiSys'22]

Fabric form [SenSys'23]

Powdered form [MobiSys'24]

Low-cost, high-speed sensors; sensor fusion ...

e.g., images & videos

Content capture/creation

Photography [MobiSys'25]

Digital Art *(Ongoing...)*

Content itself

Watermarks [S&P'26]

Perceptual Hashing [ArtSec'26] + *more...*

e.g., embeddings & weights

Inference behavior

Embeddings [MobiSys'26]

Model-as-service

more...

Human-AI collaboration

more...

Our Research Focuses

MUNCHIES
FOOD BY VICE

A Huge Amount of Deadly Fake Booze Was Confiscated from Resorts in Mexico

Death By Fake Alcohol

The ASEAN Post Team
16 January 2021

This file photo shows seized bottles of alcohol displayed before being destroyed by Indonesian customs

In recent months, we have increasingly heard stories of counterfeit or sub-qu
masks, medicines and sanitisers during the pandemic.

Fake honey scandal widens to Australian-sourced brands

A A A 153 View all comments

The Real Reason Your Olive Oil Is Probably Fake

BY MICHAEL SOMMERS / UPD

There are healthy fo
authentic extra virgi
seemingly unlimited
case.

Investigative journal
which blew the lid o
shocked America wh
olive oils sold in the

Food Fraud Costs the Global Food Industry $10-15 Billion Annually

By Chris Cattini on 04-Apr-2016 10:00:00

In 2008, melamine was added to milk and infant formula to increase its protein content. This led to the hospitalisation of around 54,000 infants, 6 deaths from kidney stones and, ultimately, a number of criminal prosecutions, resulting in 2 executions.

Counterfeit liquid food products

- Detrimental health effects to consumers

MUNCHIES
FOOD BY VICE

A Huge Amount of Deadly Fake Booze Was Confiscated from Resorts in Mexico

Regulators seized 10,000 gallons of tainted alcohol from a local supplier after raiding dozens of resorts and nightclubs across Cancun and Playa del Carmen.

By Mike Pearl

16 August 2017, 3:00am Share Tweet Snap

A series of recent police raids in Mexican resort towns have turned up stockpiles of low-quality alcohol produced under "bad manufacturing practices," the *Milwaukee Journal-Sentinel* reports. The official discovery of a rash of fake booze may begin to explain why tourists in the area have recently been experiencing adverse—and in at least one case, fatal—reactions to their all-you-can-drink refreshments.

oney scandal widens to Australian-sourced

Death By Fake Alcohol

The ASEAN Post Team
16 January 2021

This file photo shows seized bottles of alcohol displayed before being destroyed by Indonesian customs in Jakarta. (AFP Photo)

In recent months, we have increasingly heard stories of counterfeit or sub-quality face masks, medicines and sanitisers during the pandemic.

ason Your Olive
ke

ste awful and unhealthy foods that taste
or as intimates refer it: EVOO – which
nefits – if, indeed, it's authentic. Unfortu

ueller is author of the whistleblowing cl
oil trade by exposing how rampant it is
med to *60 Minutes* that "around 75 to 80 percent" of extra virgin
audulent.

Food Fraud Costs the Global Food Industry $10-15 Billion Annually

By Chris Cattini on 04-Apr-2016 10:00:00

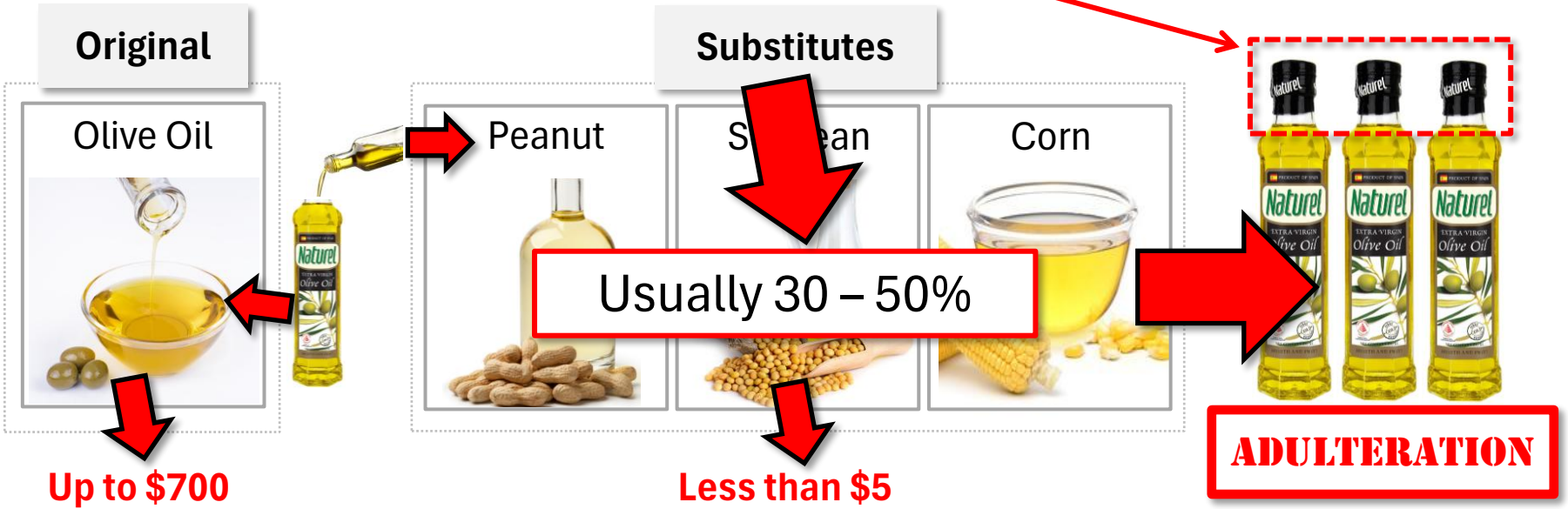
In 2008, melamine was added to milk and infant formula to increase its protein content. This led to the hospitalisation of around 54,000 infants, 6 deaths from kidney stones and, ultimately, a number of criminal prosecutions, resulting in 2 executions.

Counterfeit liquid food products

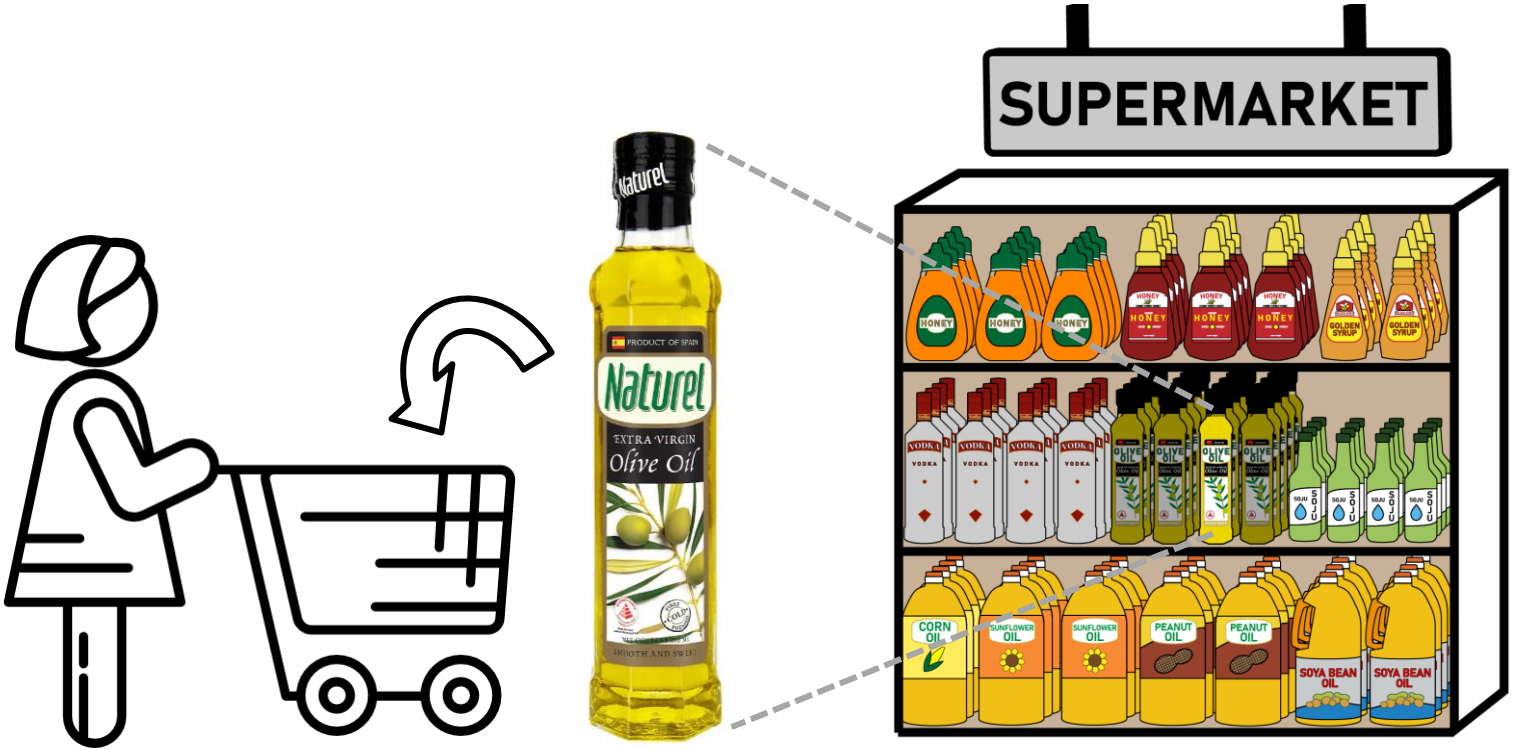
- Detrimental health effects to consumers
- Significant monetary loss to manufacturers

Adulteration is the main source of counterfeits

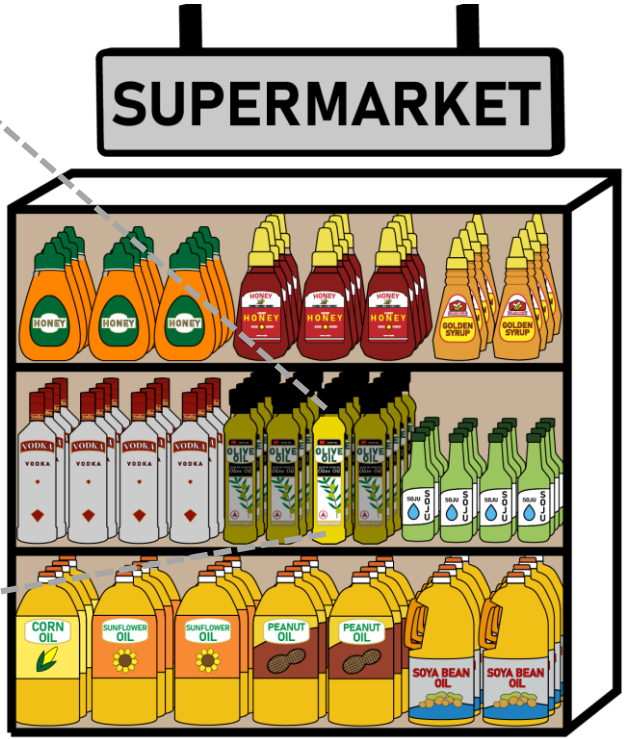
- Replace a large portion of liquid content with substitutes
- Package in authentic bottles and **seal** to factory standards



Use case: verify authenticity of olive oil



Use case: verify authenticity of olive oil

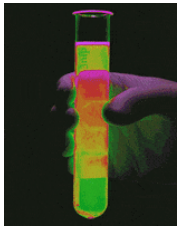


How can you tell which one is authentic?

State-of-the-art solutions

- Industrial and laboratorial solutions

Optical-based



Mechanical-based

Disadvantage:

- Require **costly** and **specialized** equipment
- Require **opening** of the bottle to take liquid **samples**

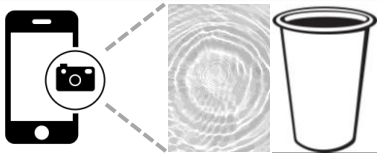
State-of-the-art solutions

- Academic proposals

Wireless signals

[Ha, NSDI'20]

Smartphone vibration



[Yue, MobiSys'19]

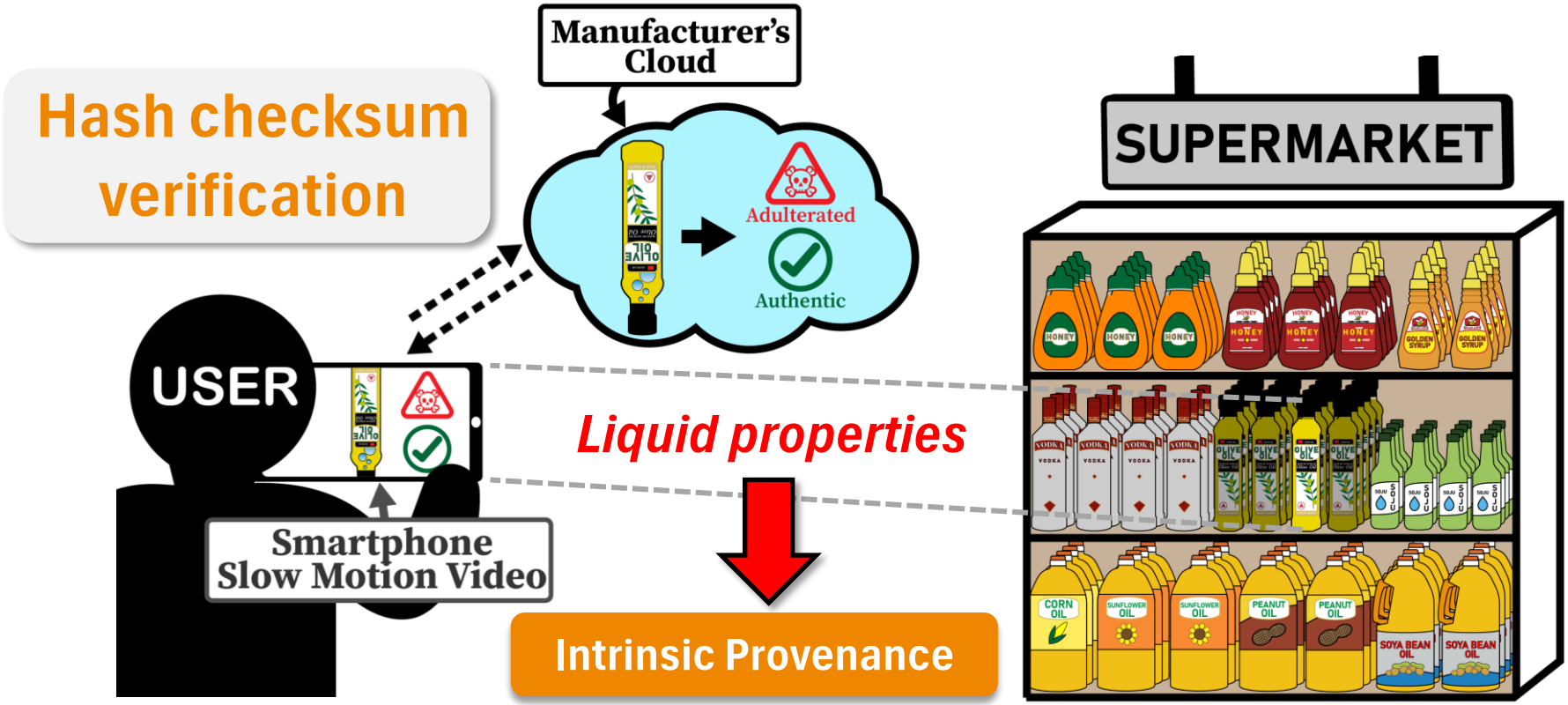
[Huang, MobiCom'21]

Disadvantage:

- Require **additional** and **specialized** equipment
- Require **opening** of the bottle and **controlled** settings

Can we verify authenticity without opening bottles and using only commodity devices?

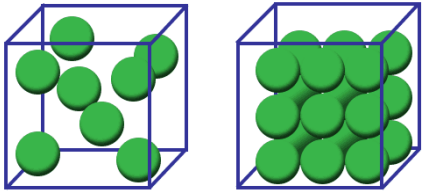
Our Work: *LiquidHash*



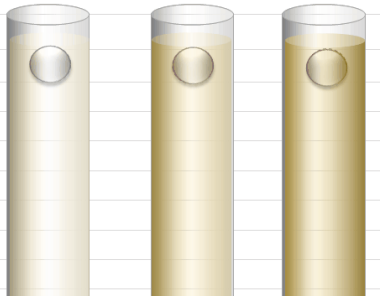
Liquid properties

- Unique **liquid properties** in each type of liquid

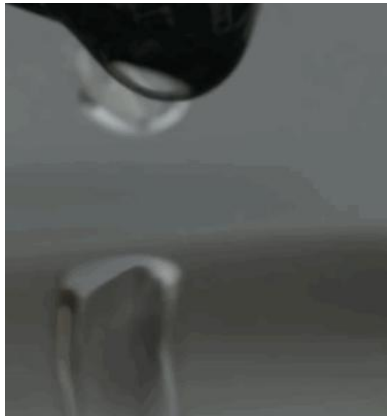
Density



Viscosity

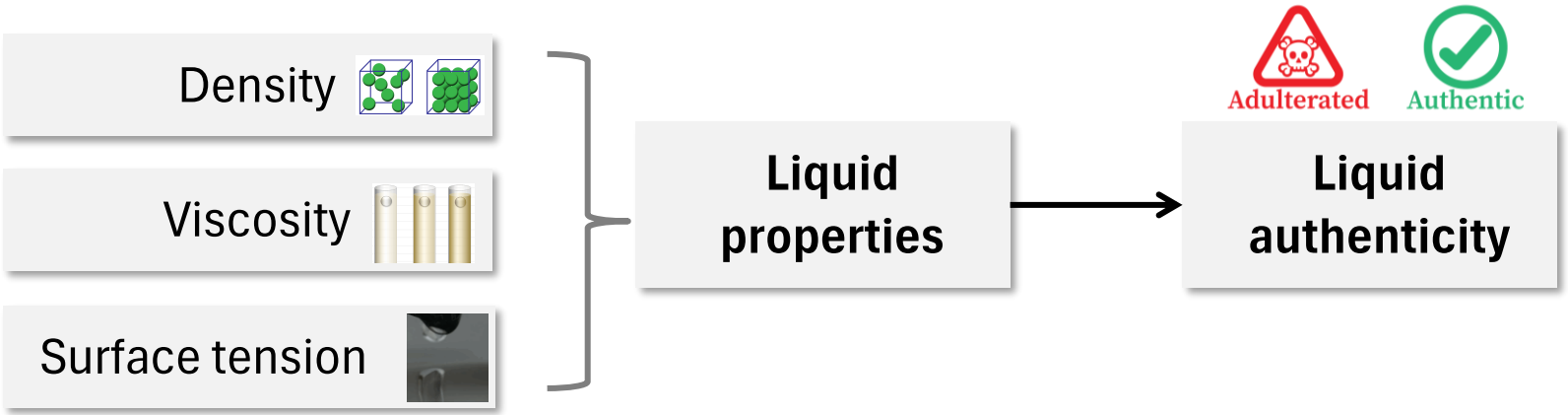


Surface tension



Liquid properties

- Unique **liquid properties** in each type of liquid



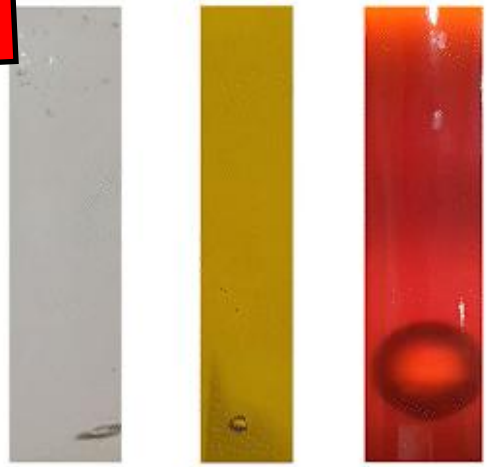
Liquid properties

- Unique **liquid properties** in each type of liquid
- Using cameras to directly **measure** liquid properties is not practical

What do we do with this setup?

Bubble characteristics

- **Bubble characteristics** are a model of liquid properties



Vodka

Olive Oil

Honey

Size

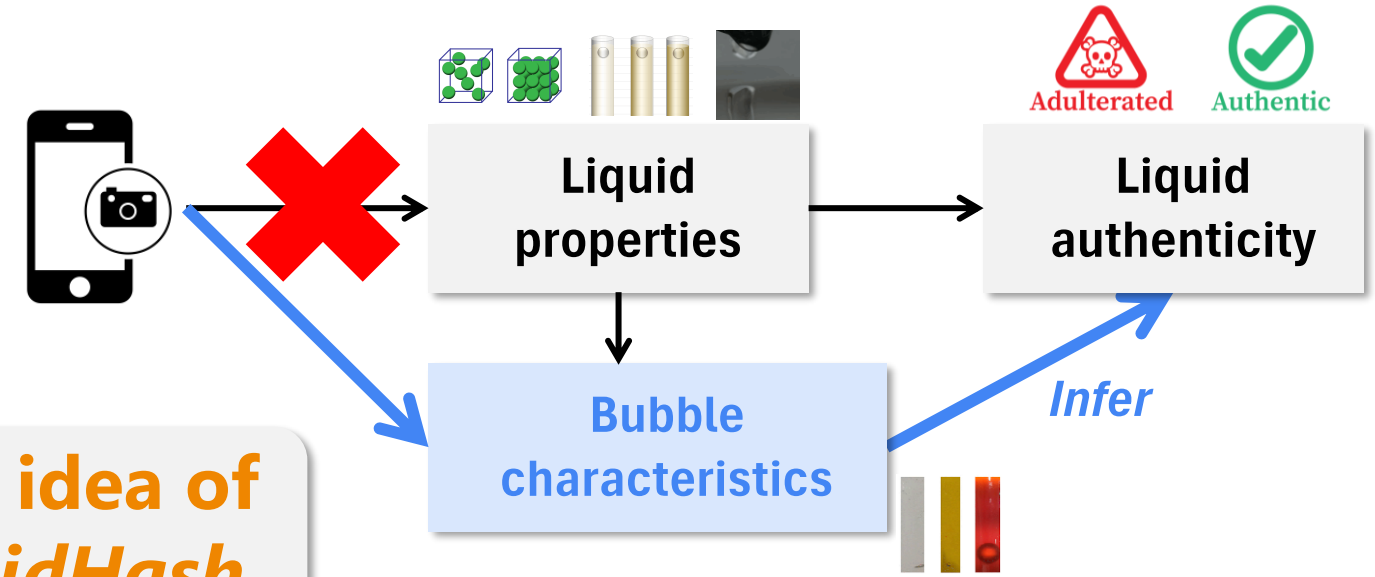
Shape

Speed

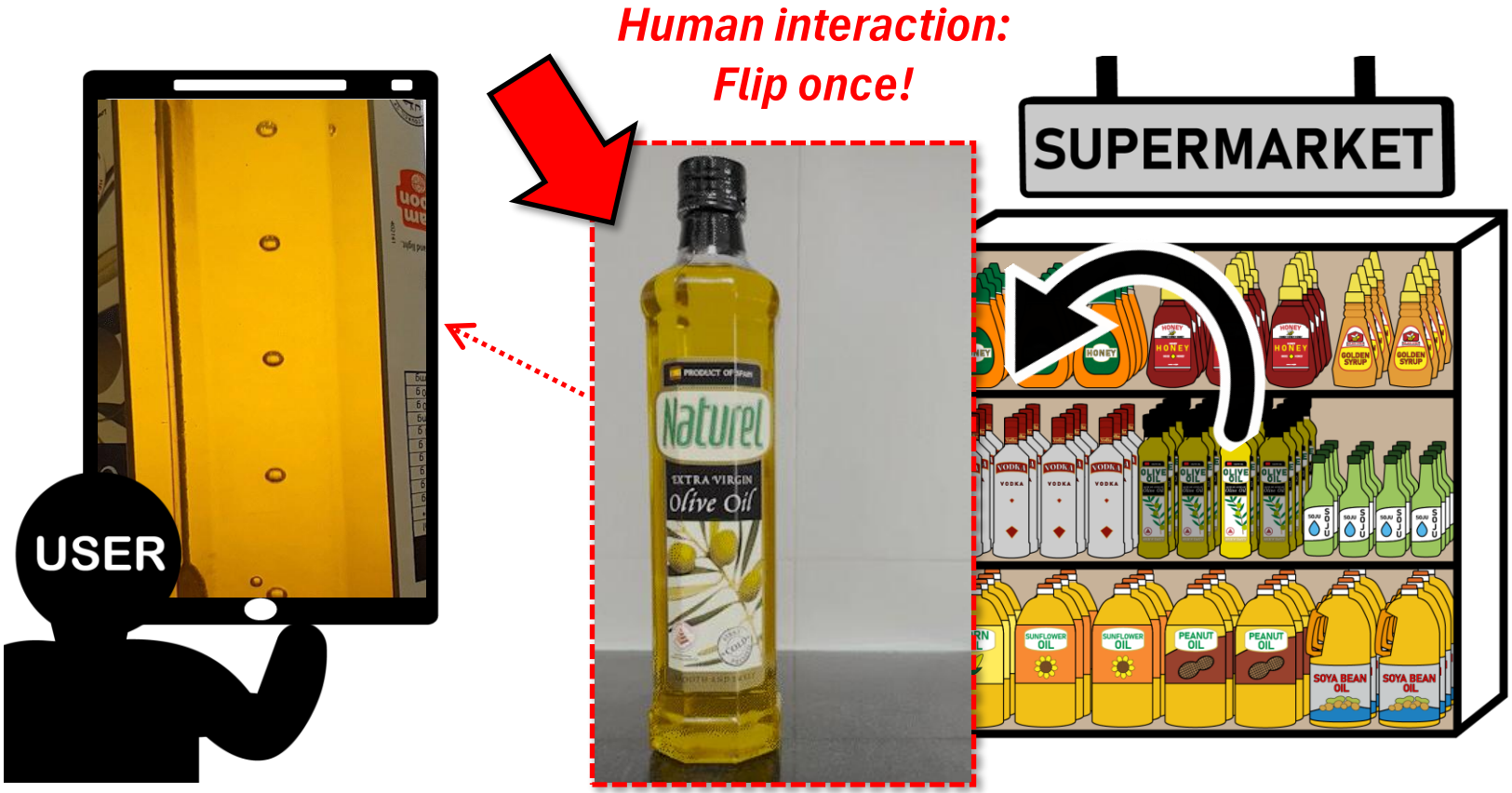
Bubble characteristics

Bubble characteristics

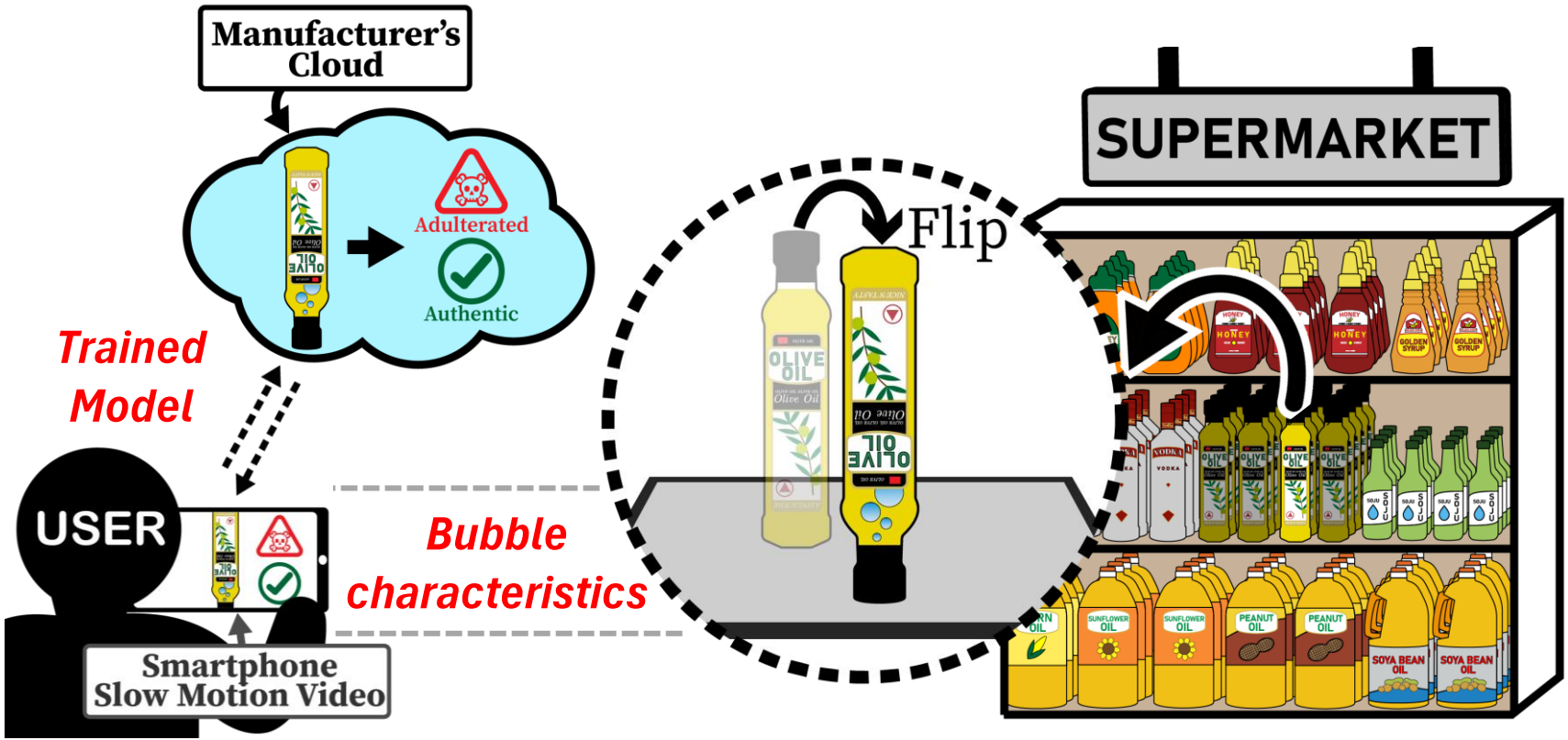
- **Bubble characteristics** are a model of liquid properties
- Capture bubbles to infer liquid authenticity



Our Work: *LiquidHash*

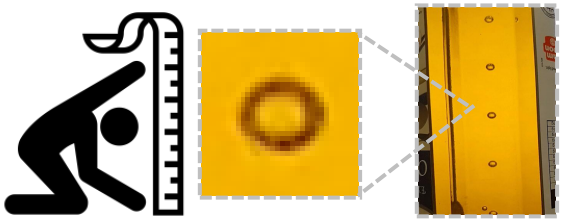


Our Work: *LiquidHash*



Challenge #1: multiple sources of noise

- Noise in measuring bubble characteristics in each test



- Noise due to **human behavior**

① Rotation Motion

② Camera Placement

- Noise due to **liquid movement**

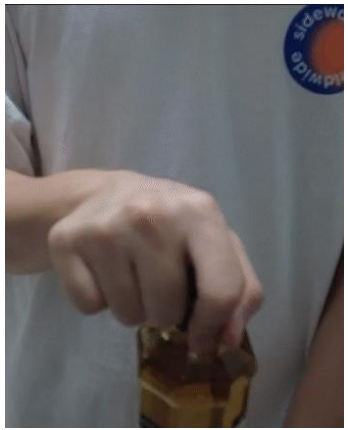
③ Bubble Shapes

④ Bubble Trajectories

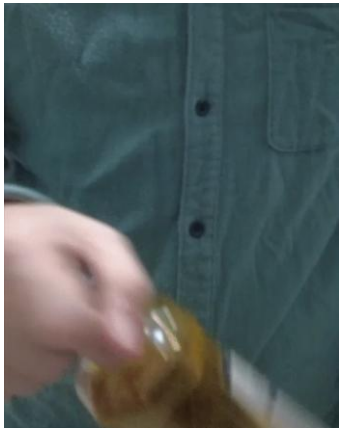
Challenge #1: multiple sources of noise

- Noise due to **human behavior**

① Rotation Motion

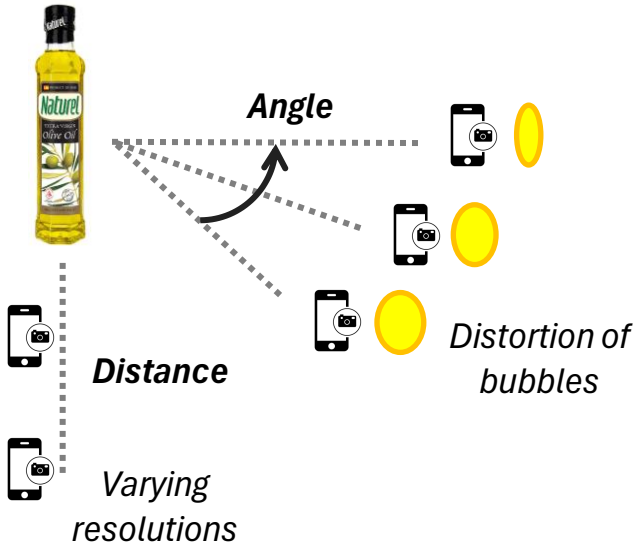


*Test **1***



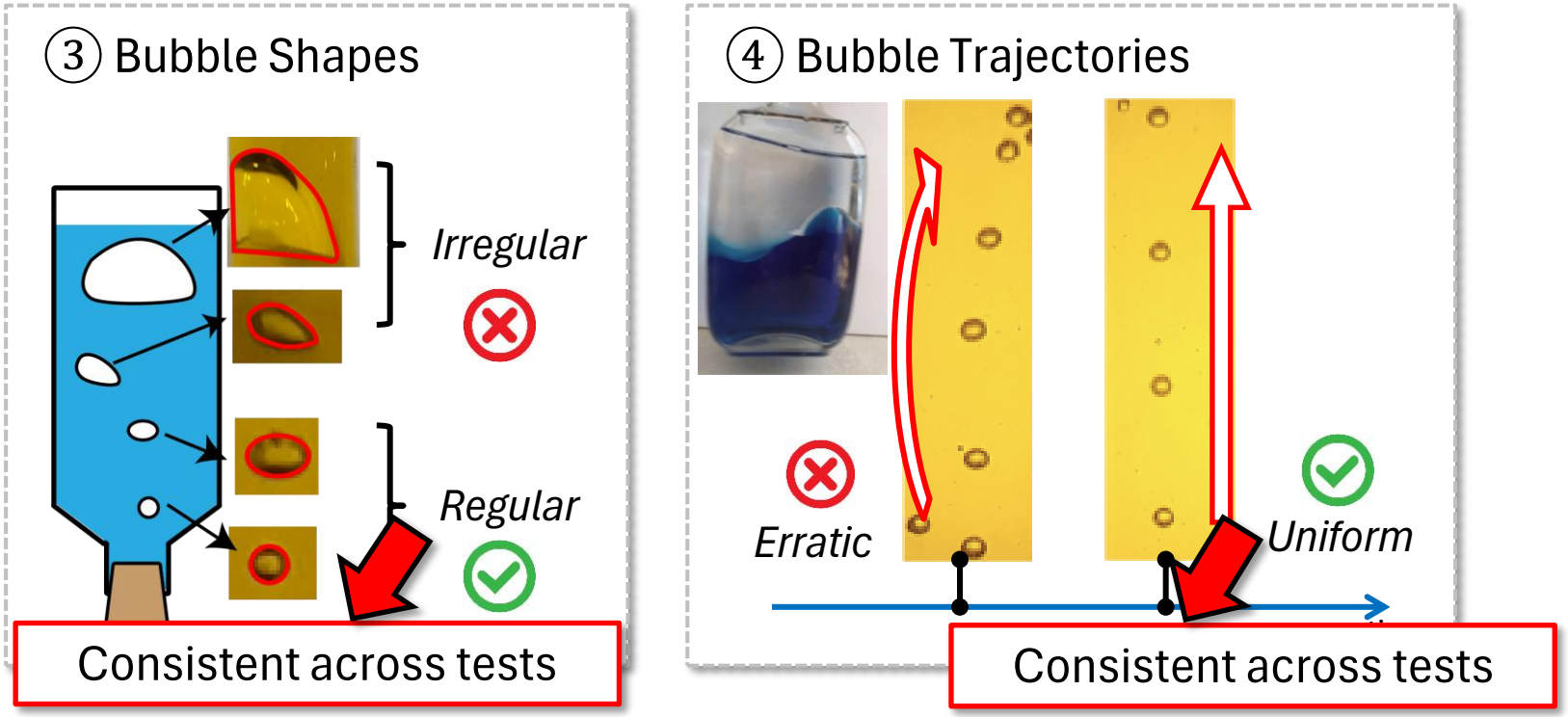
*Test **2***

② Camera Placement



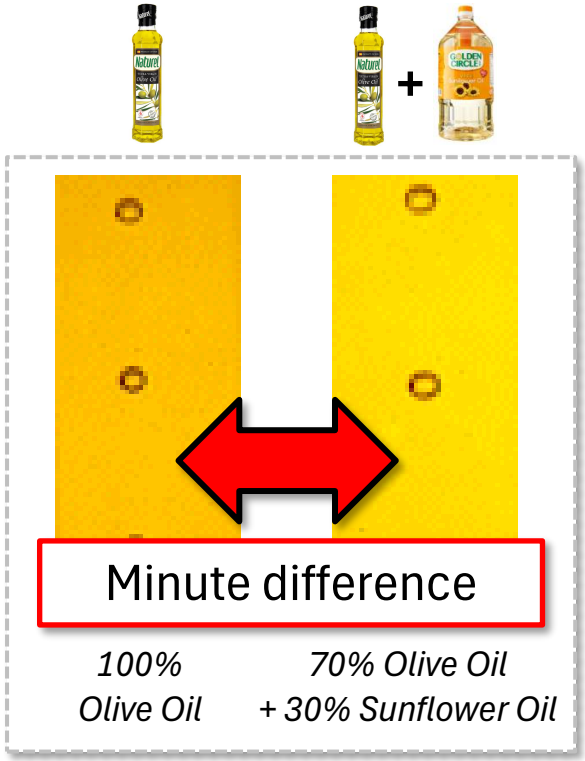
Challenge #1: multiple sources of noise

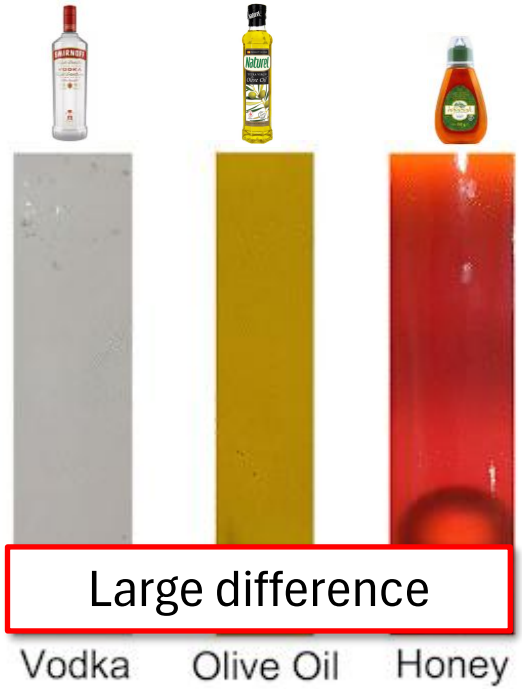
- Noise due to **liquid movement**



Challenge #2: minute differences in characteristics

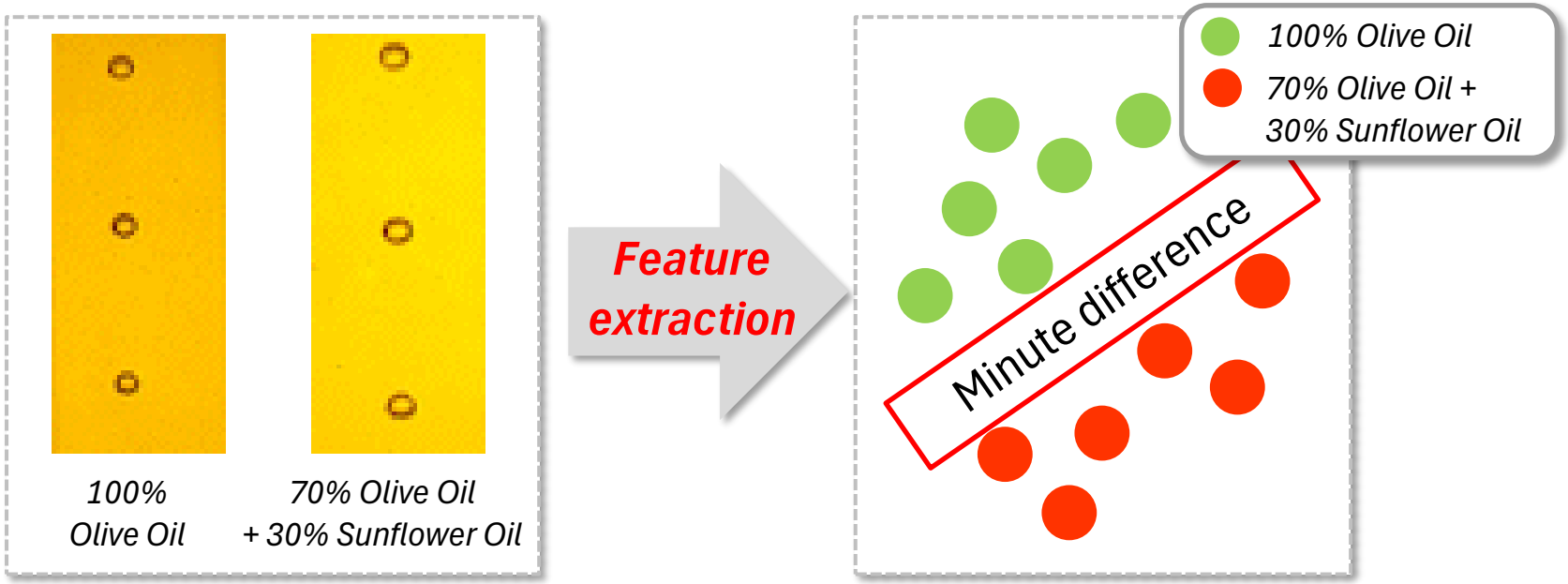
- Difference in bubble characteristics could be **minute**





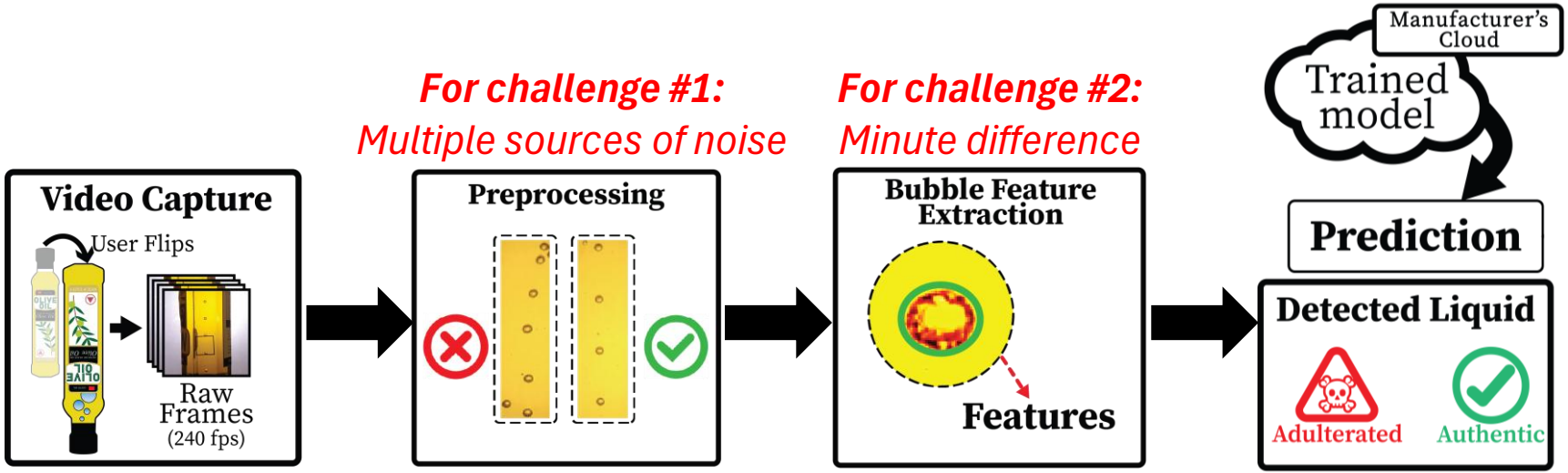
Challenge #2: minute differences in characteristics

- Difference in bubble characteristics could be **minute**
- Require fine-grained and accurate **feature extraction**

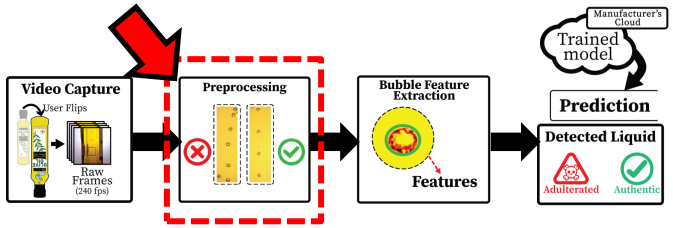


System Design of *LiquidHash*

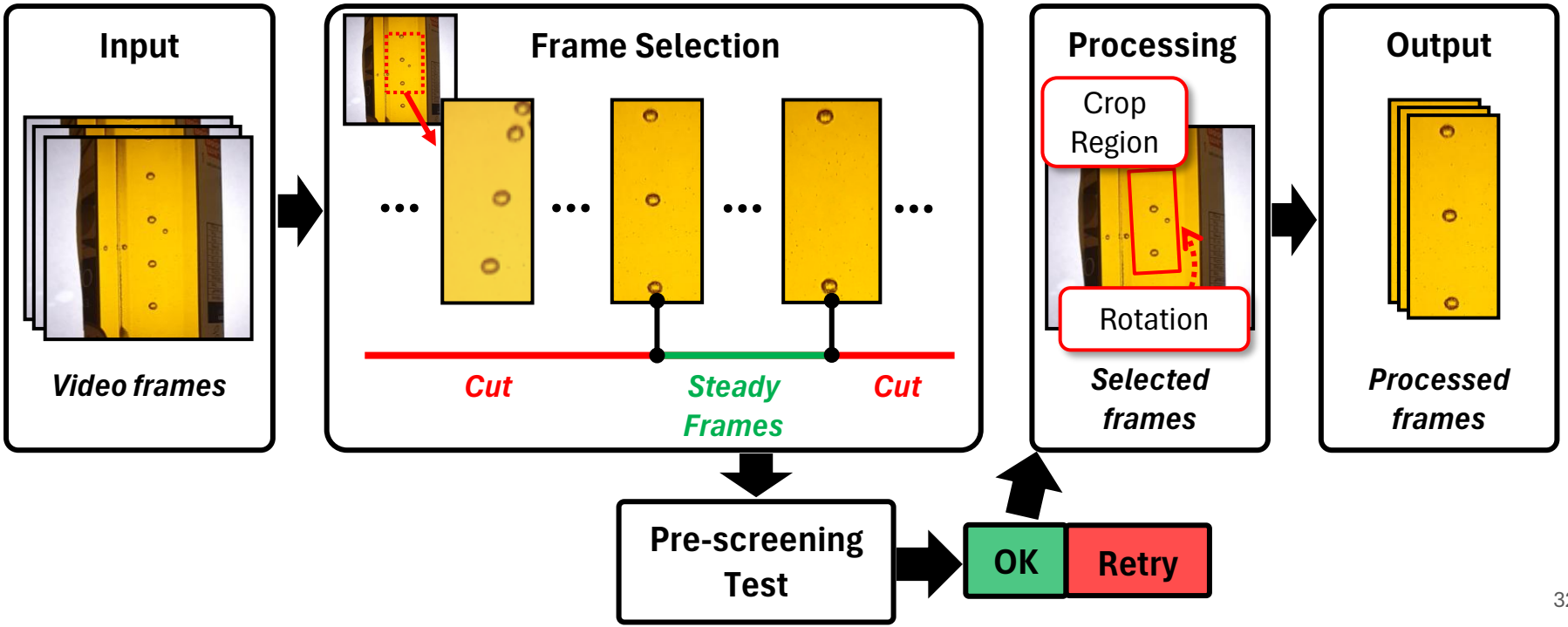
Goal: To verify authenticity leveraging observed bubble characteristics



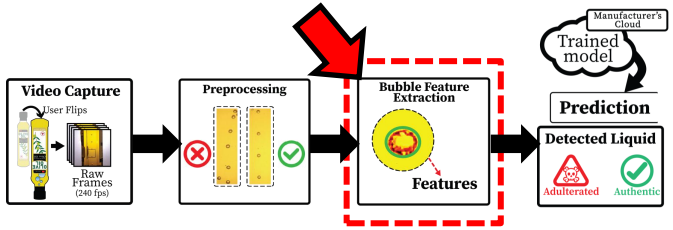
Pre-processing



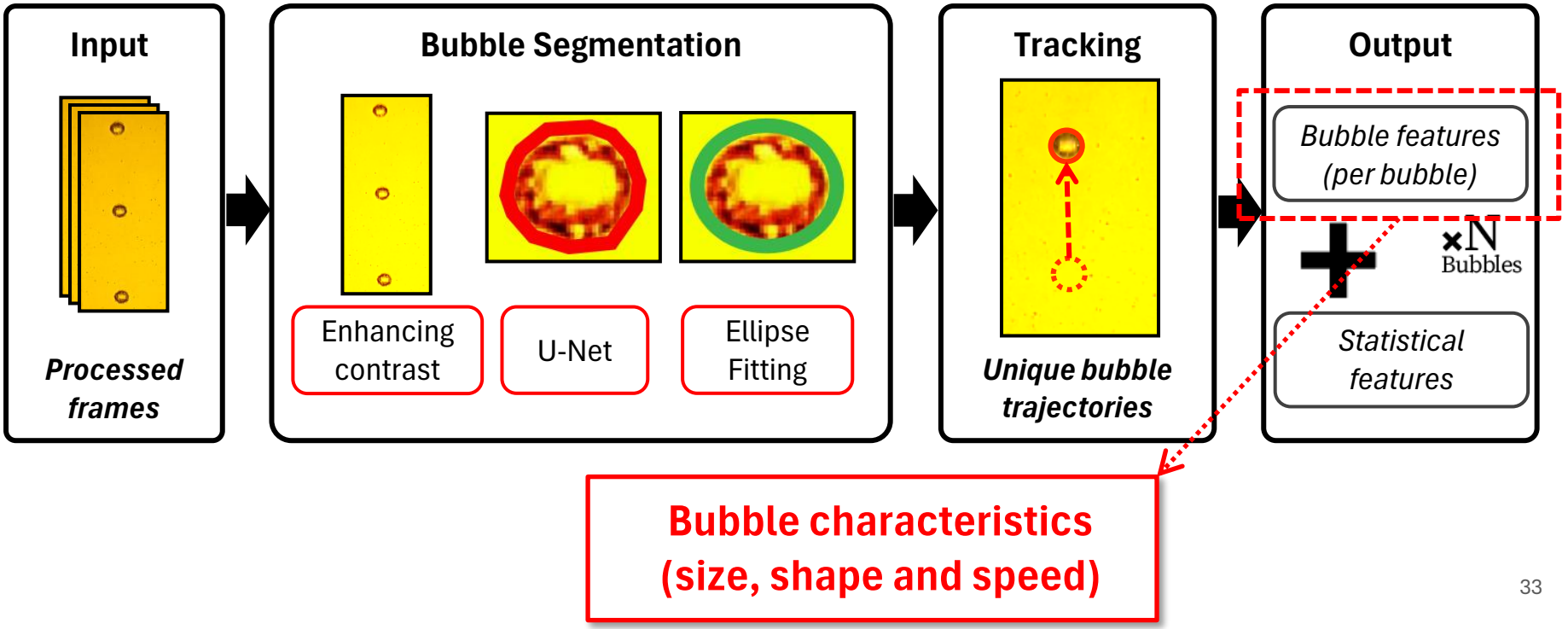
Goal: To select and process frames to **remove noise** from multiple sources



Bubble Feature Extraction

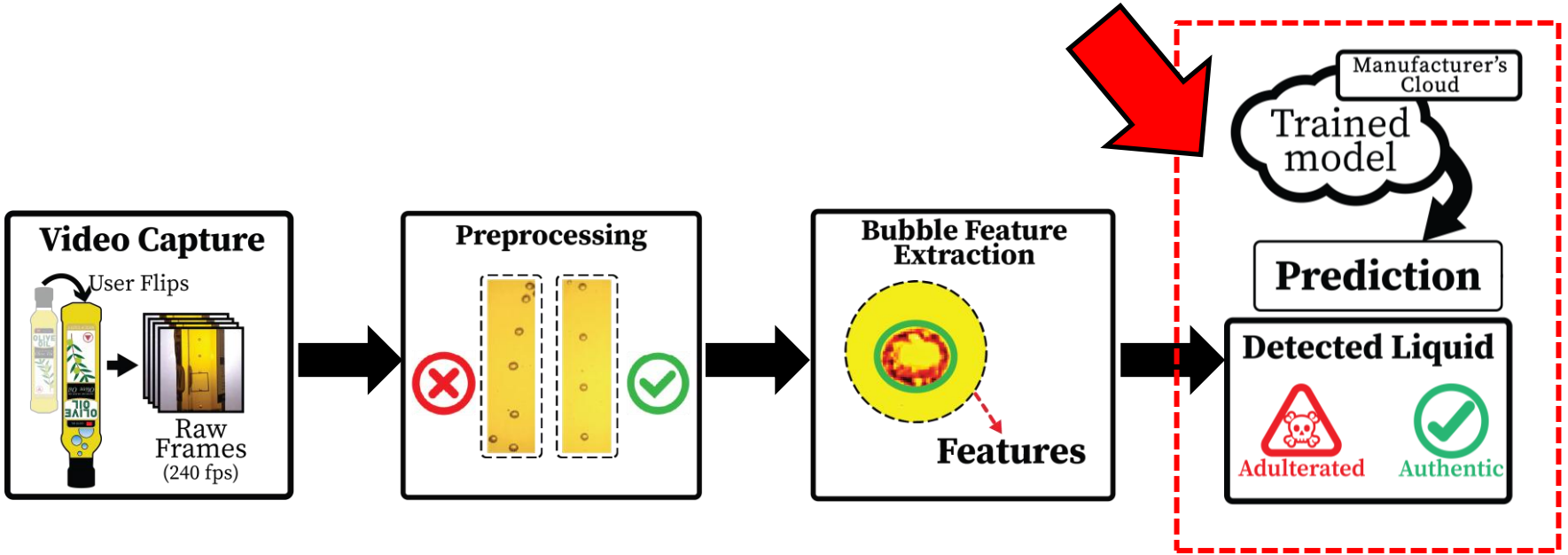


Goal: To extract **fine-grained** and **distinguishable** features



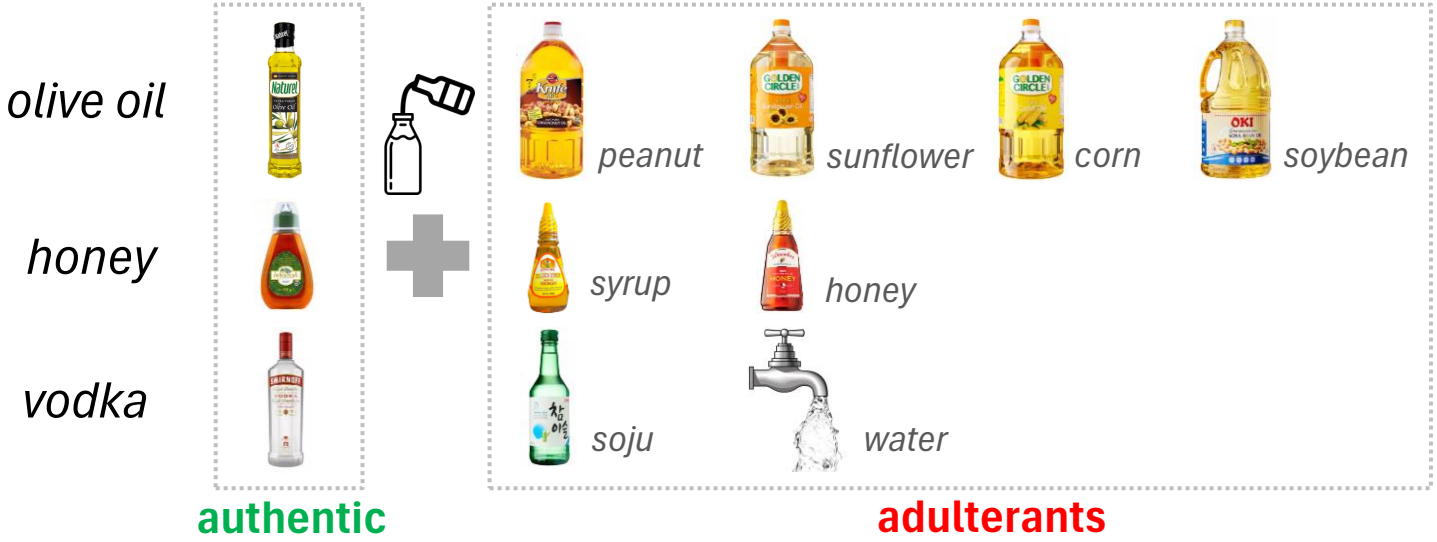
Prediction

Goal: To decide liquid authenticity leveraging extracted bubble features



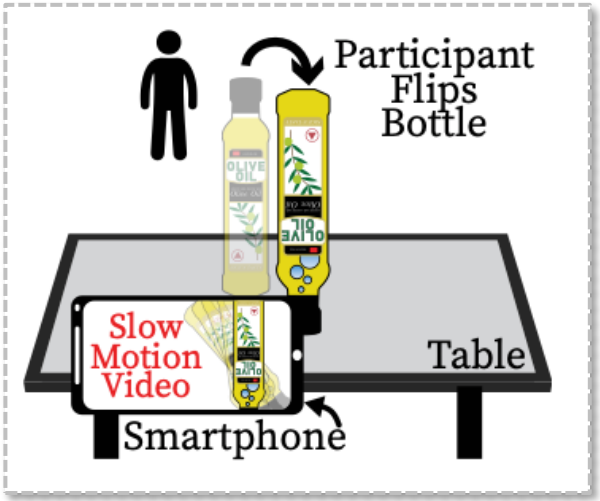
Evaluation setup

- We test *LiquidHash* with olive oil, honey and vodka
  - **3** instances of **authentic** liquid products
  - **8** instances of **adulterated** liquid products



Evaluation setup

- For each instance, we test **two** detection methods



vs

LiquidHash

70 tests x **5** Participants
Leave-one-out approach

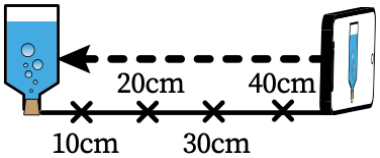
Baseline: No Assistance

Participants can **interact freely** with liquid products **except opening** the bottles

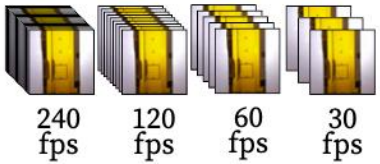
Summary of evaluation results

- Demonstrates **overall detection accuracy up to 95%**

- Robust against **camera-to-bottle distances**



- Robust against **video framerates**

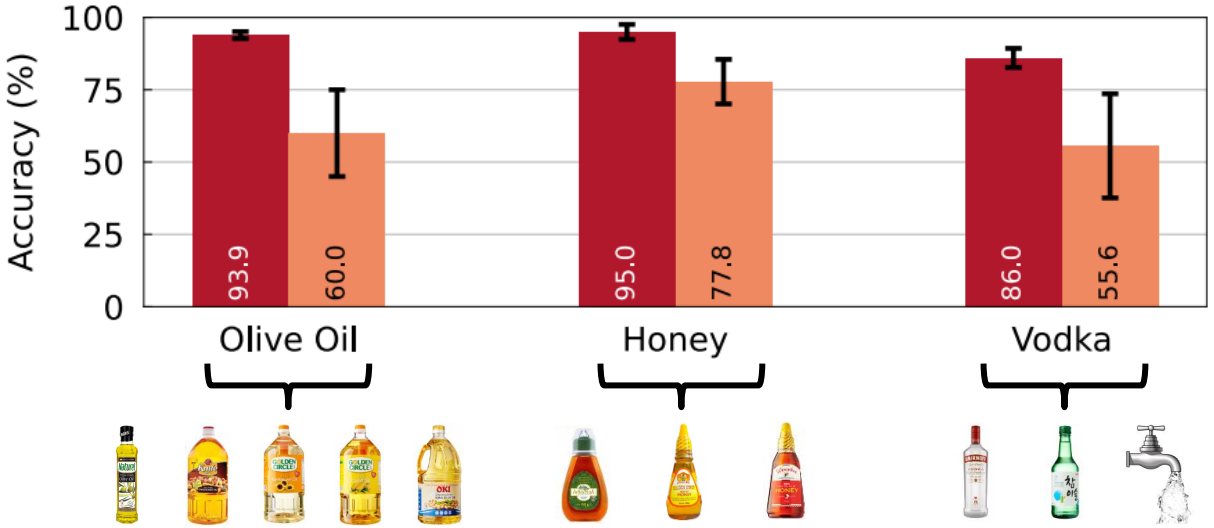


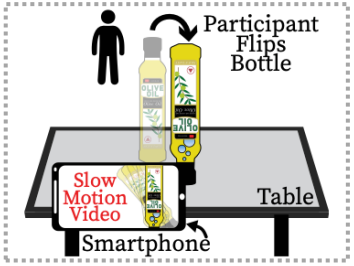
- Generalizes across **adulterant concentrations**

- Generalizes across **bottle dimensions**

Main results

- ***LiquidHash*** outperforms ***No Assistance*** baseline in all use cases of olive oil, honey and vodka





LiquidHash

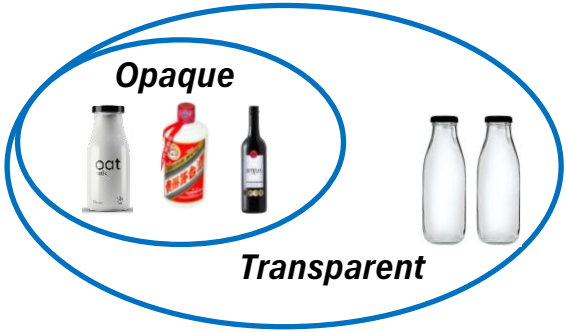
No Assistance

Discussion

① Accessible intrinsic provenance

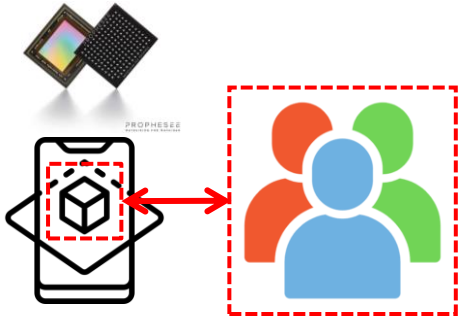
- Attack is extremely costly as evidences are difficult to fake
- Consumer empowerment serves as a deterrent

② Opaque materials



- Increasing usage of transparent bottles
- Utilize other modalities (e.g., IR sensing)

③ Future opportunities



- Low-cost, high-speed sensors (e.g., EVS)
- Sensor fusion and crowd sourcing

Focus of this talk

Extrinsic Provenance

External Labels & Metadata

Blockchain Technology

Database & Logs

Existing Approaches

Intrinsic Provenance

Physical Domain ↔ Digital Domain ↔ Latent Domain

e.g., liquids & medicines

RGB cameras only

Liquid form [MobiSys'22]

Fabric form [SenSys'23]

Powdered form [MobiSys'24]

Low-cost, high-speed sensors; sensor fusion ...

e.g., images & videos

Content capture/creation

Photography [MobiSys'25]

Digital Art *(Ongoing...)*

Content itself

Watermarks [S&P'26]

Perceptual Hashing [ArtSec'26] + *more...*

e.g., embeddings & weights

Inference behavior

Embeddings [MobiSys'26]

Model-as-service

more...

Human-AI collaboration

more...

Our Research Focuses

A Surge in Online Image Theft

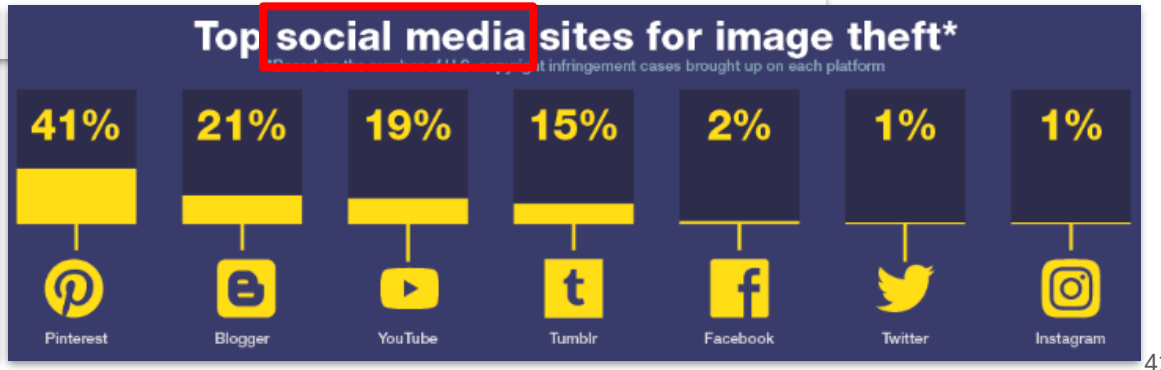
- **Unauthorized use** of copyrighted photos and images

Home » "A lot of photographers find out about image theft when the culprits tag them in social media'

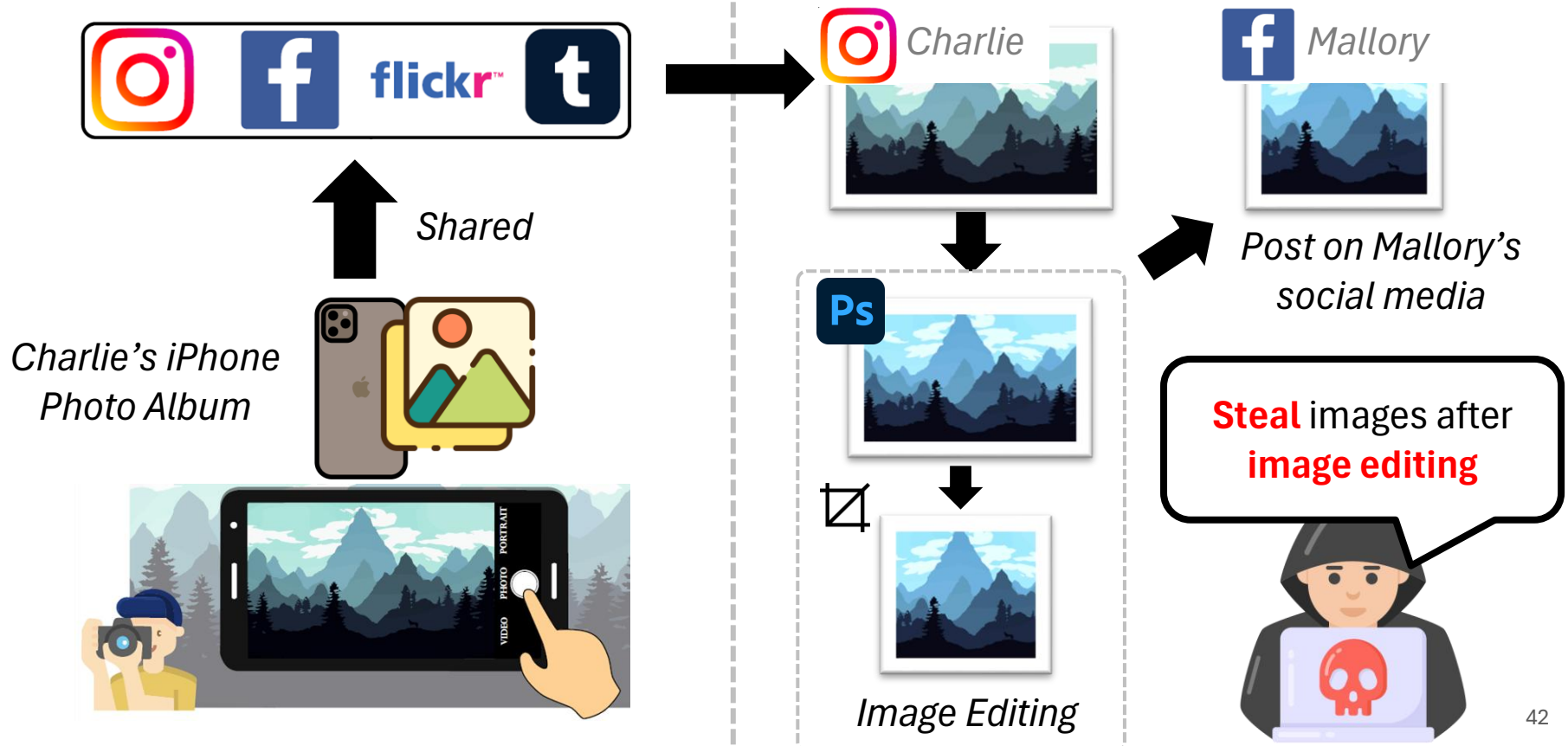
"A lot of photographers find out about image theft when the culprits tag them in social media"

Geoff Harris
9 November 2020 / 14:46 GMT

OVER 2.5 BILLION ONLINE IMAGES ARE STOLEN EVERY DAY, COPYTRACK REPORTS



Scenario: Combat Image Theft

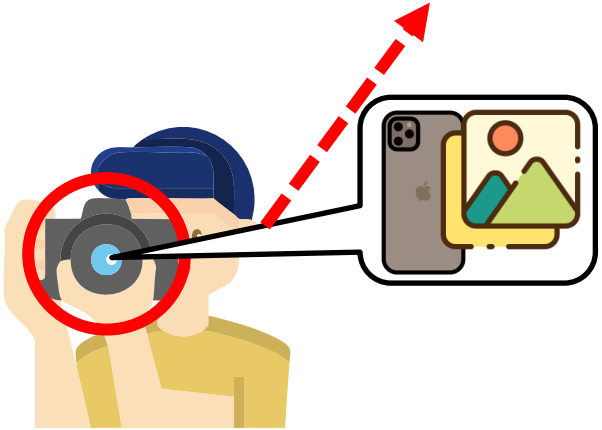


Scenario: Combat Image Theft

Search from image database

"Physical Token"

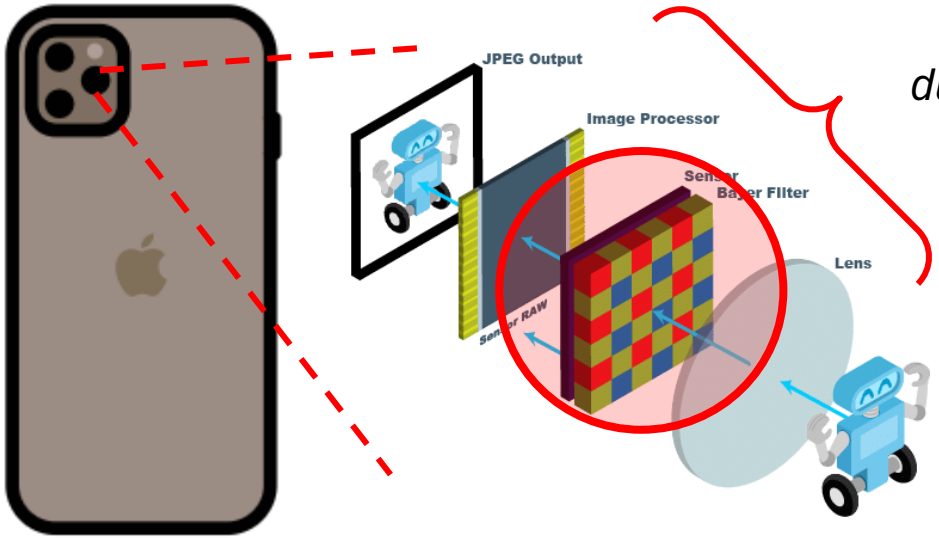
Physical Proof of Ownership



How to help Charlie combat image theft?

Utilize Camera “Fingerprints”

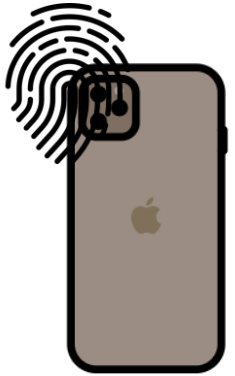
- Unique **hardware traces** due to manufacturing imperfections
- Identify the **specific camera** that took a particular photo



Hardware traces

due to manufacturing imperfections

“Fingerprint”



PRNU: The Most Distinctive Hardware Trace

- **Photo Response Non-Uniformity (PRNU)** captures differences in **electrical conductivities** of photodiodes in image sensor

Uniform white light

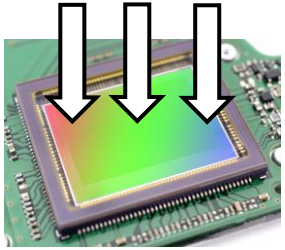
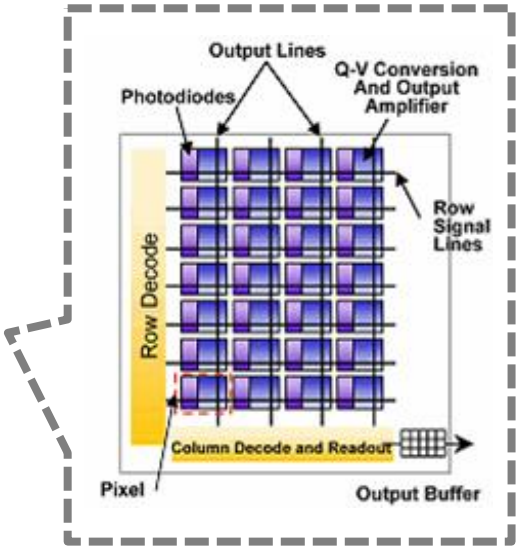
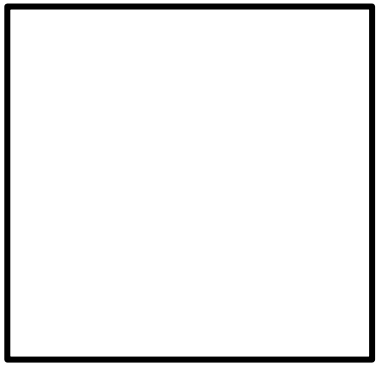


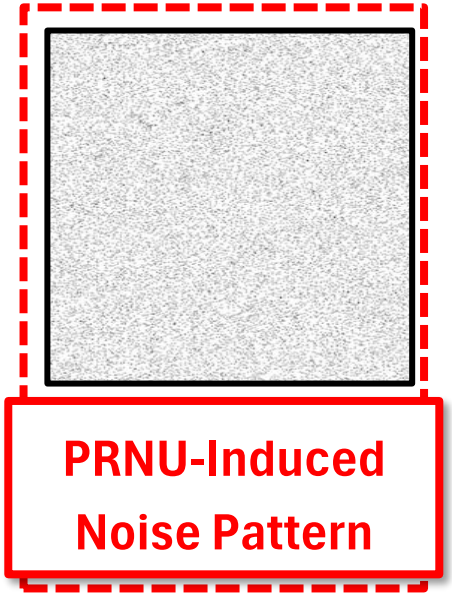
Image Sensor





Perfect

Same value across all pixels



PRNU-Induced Noise Pattern

PRNU: The Most Distinctive Hardware Trace

- PRNU is a **noise pattern** residing in images
- Same sensor produces **similar patterns regardless of image editing**

Uniform white light

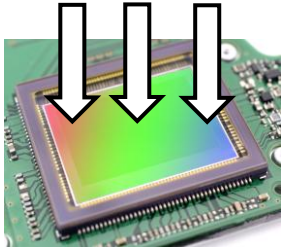
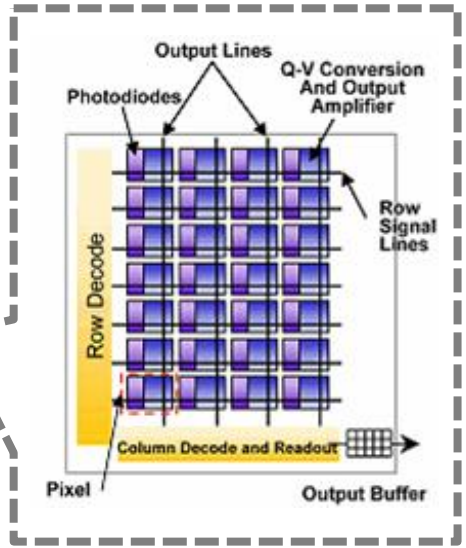
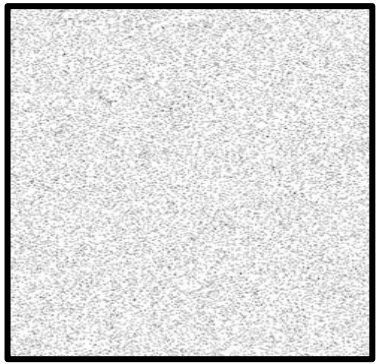


Image Sensor





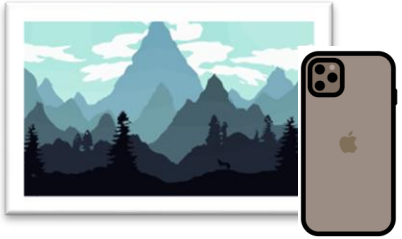
PRNU-Induced Noise Pattern

Original Image

Edited Image

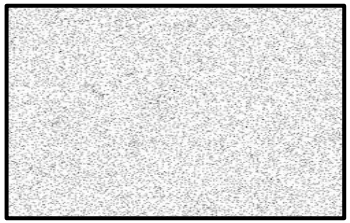
Related Work: General Pipeline of Using PRNU

- Related work focuses on **extracting** and **matching** noise patterns

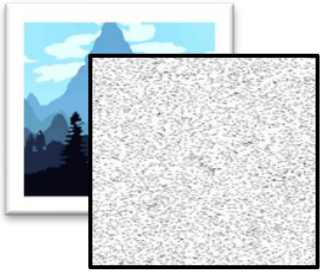


An Image Taken by Charlie's iPhone

PRNU Extraction

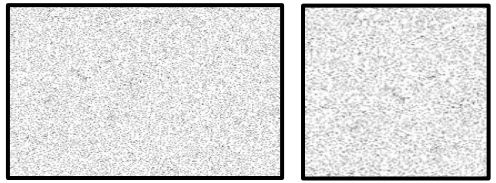


Reference Noise Pattern, ***Ref***



Test Noise Pattern, ***Test*** (*From A Suspicious Image*)

PRNU Matching



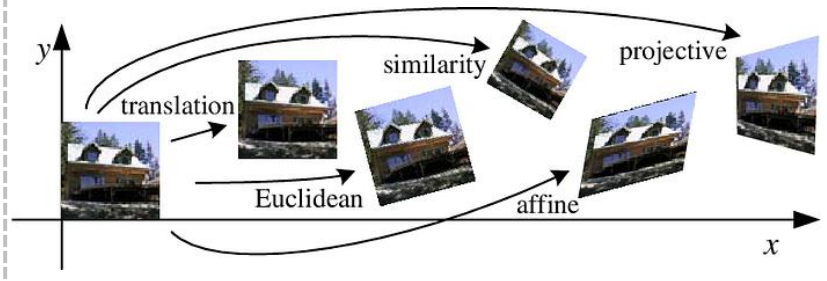
Compare similarity

Sim. > Threshold ?

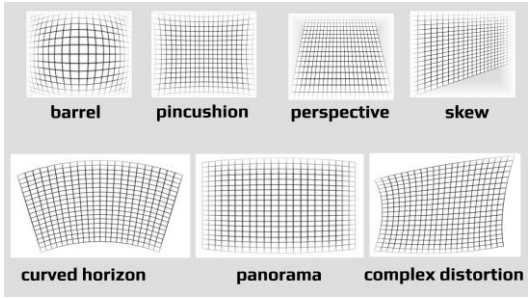
Related Work: Limitations

- Extremely sensitive to **geometric transformations** and **distortions**

PRNU Matching



Examples of Transformations



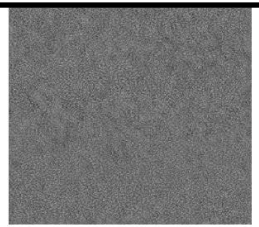
Examples of Distortions

Transformation functions f_1 ... f_n

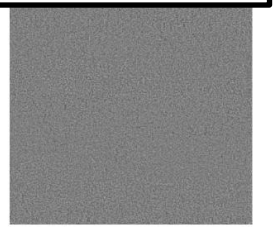
Related Work: Limitations

- Extremely sensitive to **geometric transformations** and **distortions**

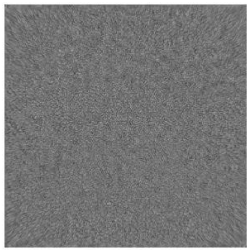
Examples of noise patterns



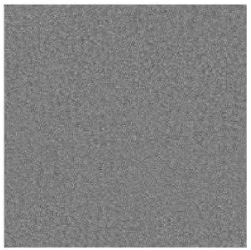
Ref
(original)



Test A
(f_1: color effects)

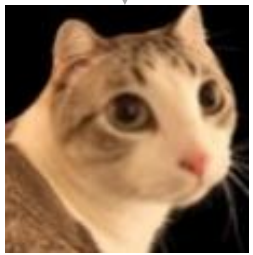


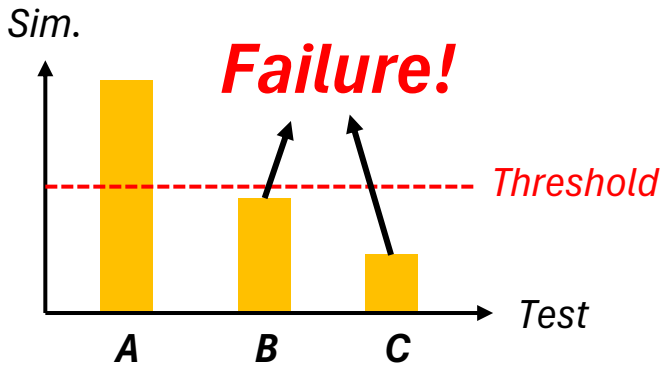
Test B
(f_2: distortion)



Test C
(f_3: crop+resize)

For illustration purpose





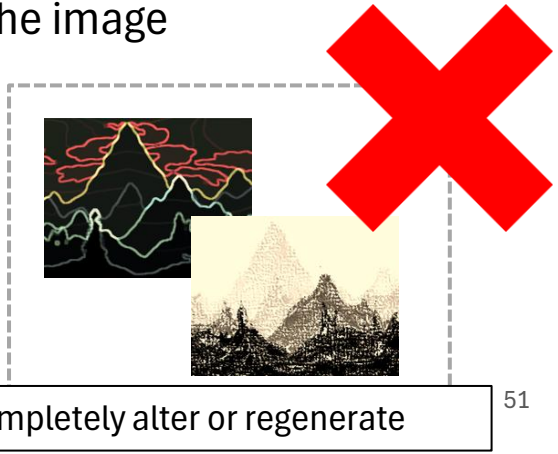
We need a robust solution when Ref and Test are not spatially aligned

Can we detect image theft even when attackers could freely edit images?

Threat Model

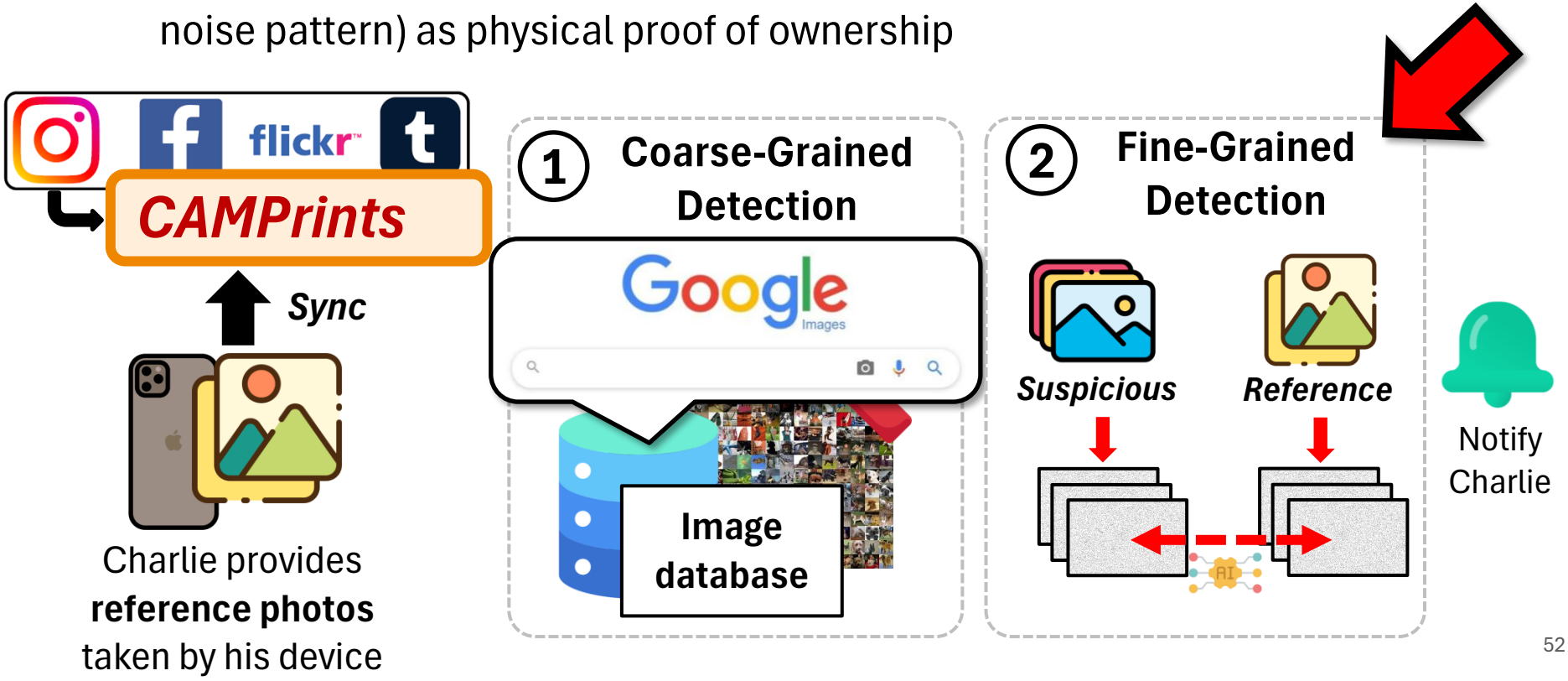
- **Attacker's goal:**
  - Alter the image to avoid detection of image theft
  - Preserve image content and quality for economic value

- **Attacker's capabilities:**
  - Use image editing software and test against detection methods
  - No transformations that completely alter or regenerate the image



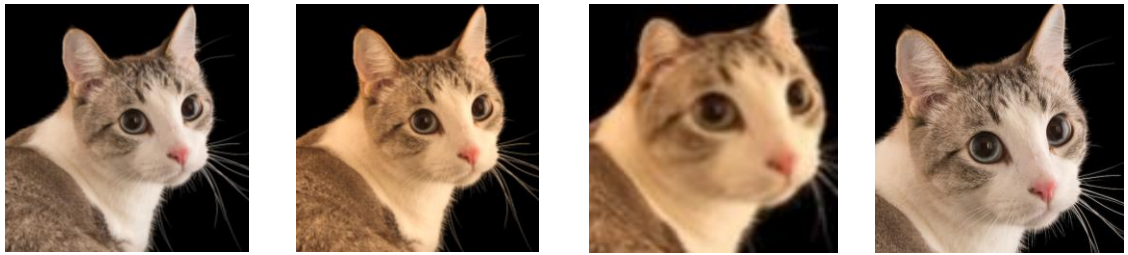
Our Work: *CAMPrints*

- Detect online image theft using camera “fingerprints” (i.e., PRNU-induced noise pattern) as physical proof of ownership



Core Idea of *CAMPrints*

- A noise pattern should be **recognizable** even after transformations

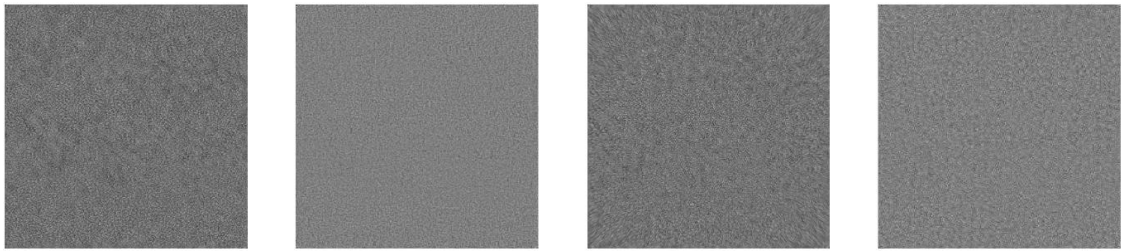


Ref
(original)

Test A
*(**f_1**: color effects)*

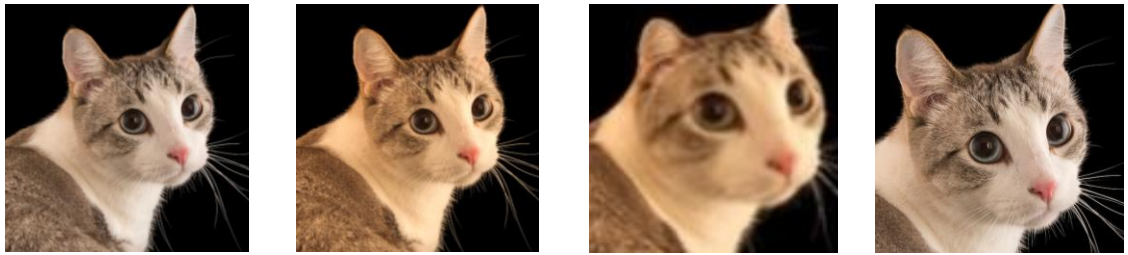
Test B
*(**f_2**: distortion)*

Test C
*(**f_3**: crop+resize)*



Core Idea of *CAMPrints*

- A noise pattern should be **recognizable** even after transformations

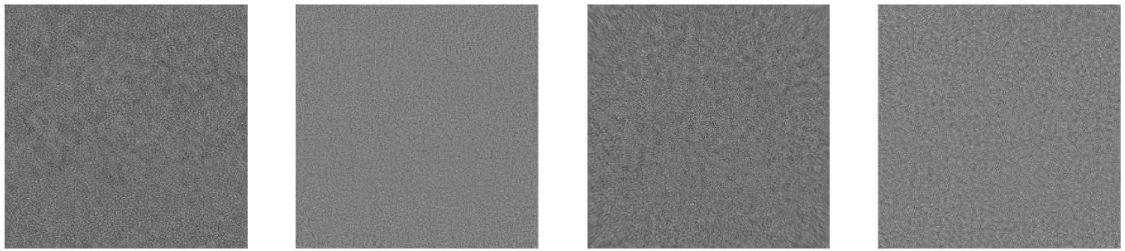


Ref *(original)*

Test A *(f_1: color effects)*

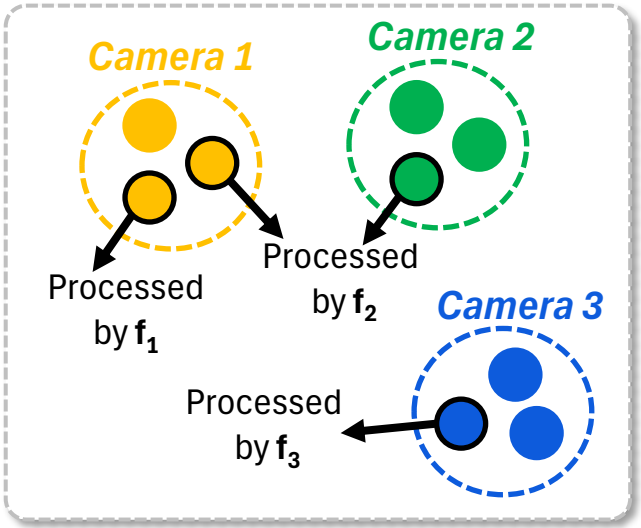
Test B *(f_2: distortion)*

Test C *(f_3: crop+resize)*



Representation Learning

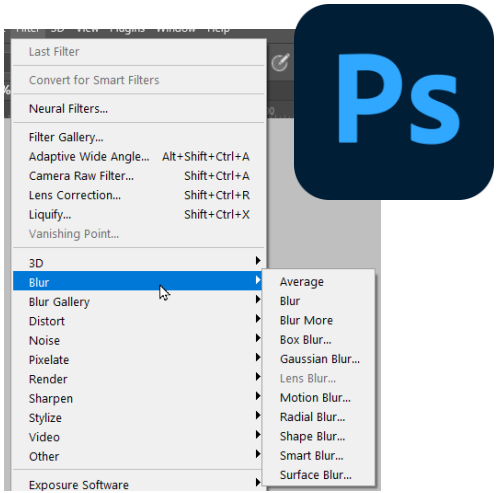
form tight clusters regardless of transformations (f_n)



Challenge #1: Image Editing Operations

- **Freely edit images** as long as image content and quality is preserved (i.e., within a quality budget)
- A wide range of image editing **types** and **combinations**

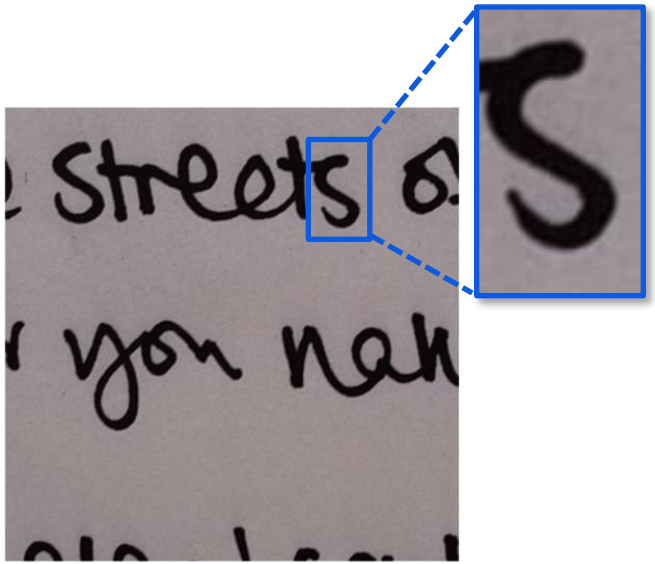
Examples of image editing operations on iOS



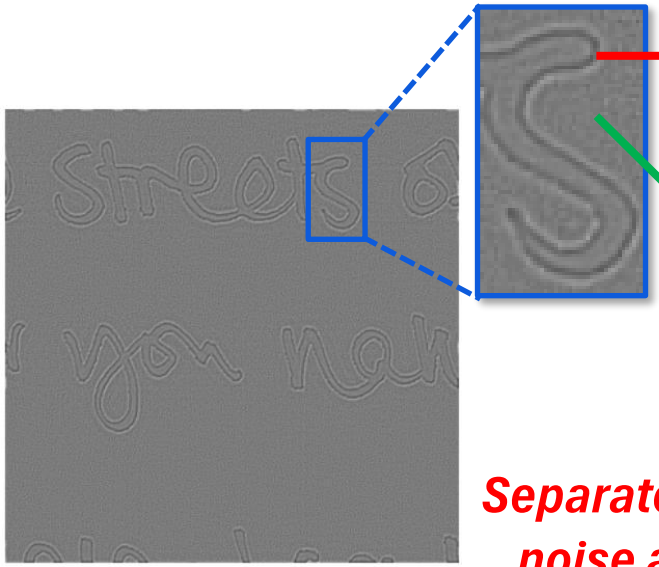
Examples of image editing operations on Photoshop

Challenge #2: Multiple Sources of Noises

- Extraction of noise pattern is imperfect
- Contains a **mixture** of content noises and sensor noises



Input Image



Extracted Noise Pattern

Content noises (e.g., edges, textures)

Sensor noises (our target)

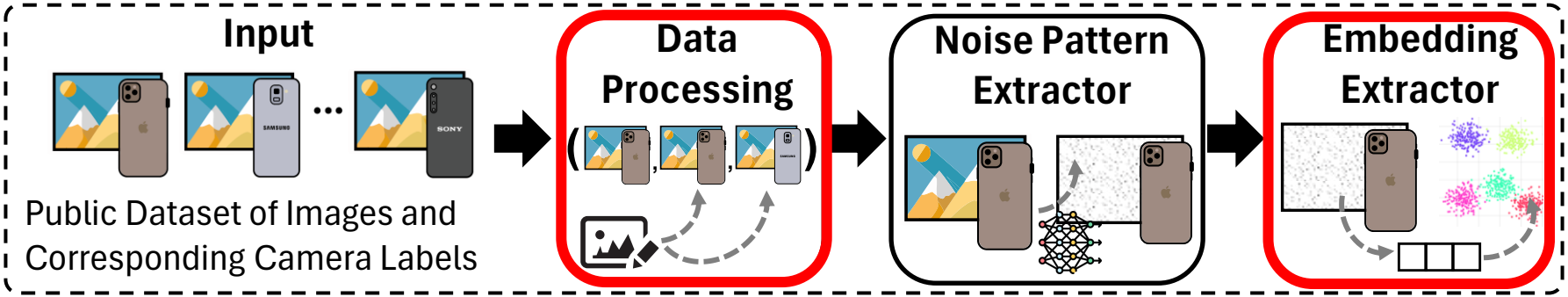
Separate content-induced noise and sensor noise

Design of *CAMPrints*

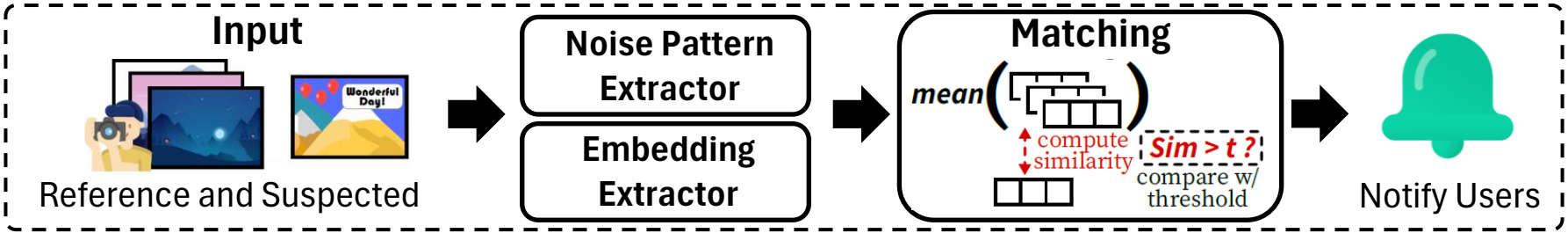
For Challenge #1
Image Editing Operations

For Challenge #2
Multiple Sources of Noises

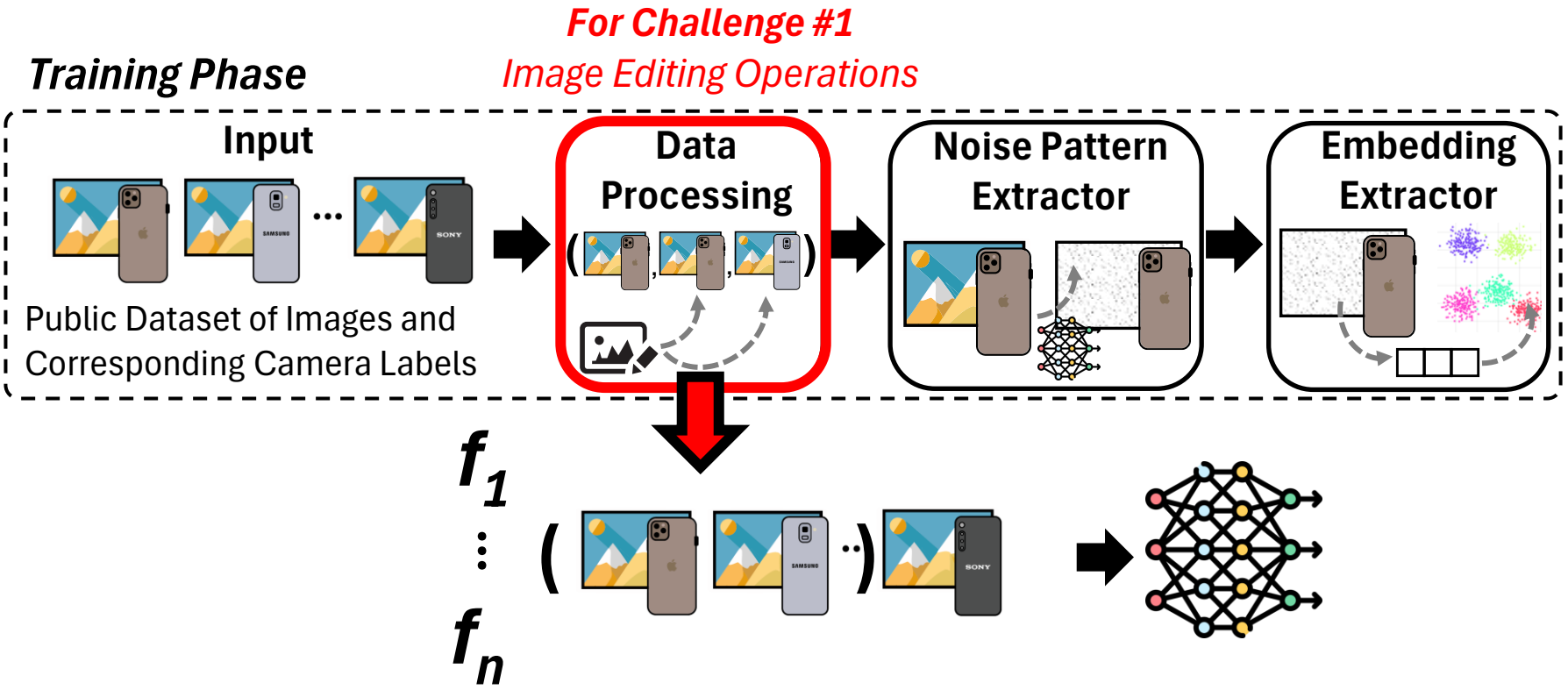
Training Phase



Verification Phase



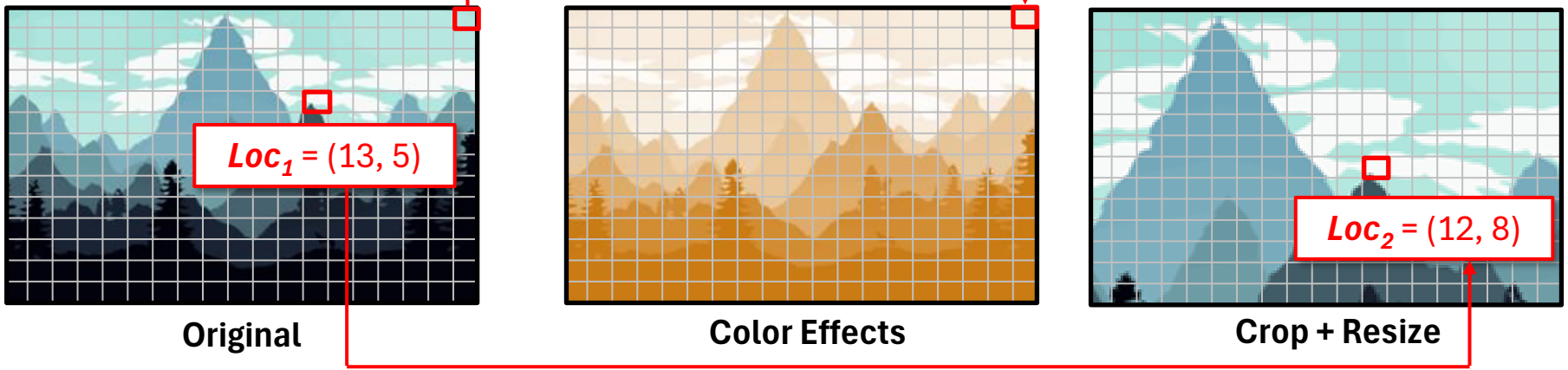
Design of *CAMPrints*



Data Processing: Representative Image Editing

- We select a ***small yet representative set*** of image editing
- Categorize the effects of image editing

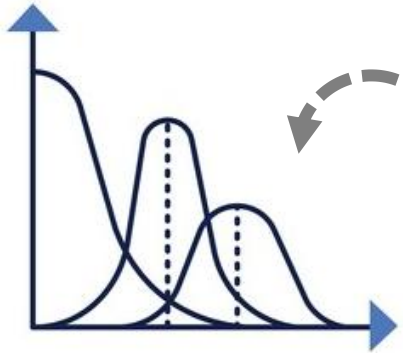
Effect (1) Pixel value changes from $Color_1$ to $Color_2$



Effect (2) Pixel location shifts from Loc_1 to Loc_2

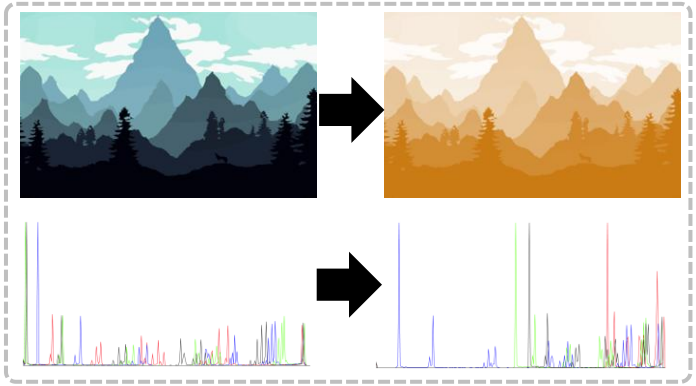
Data Processing: Representative Image Editing

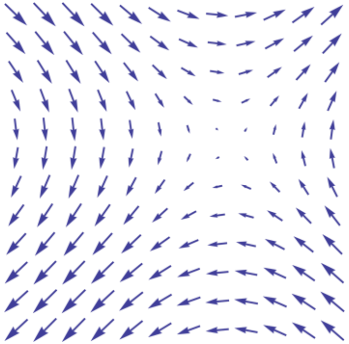
- Quantify pixel value changes using histograms
- Quantify pixel location shifts using motion vectors



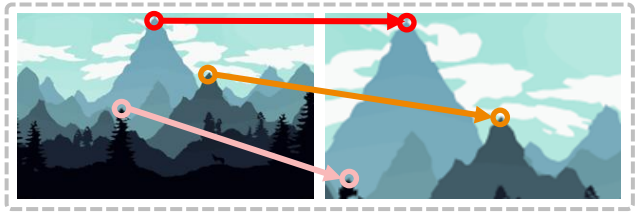
Color Histogram Difference

Effect (1)





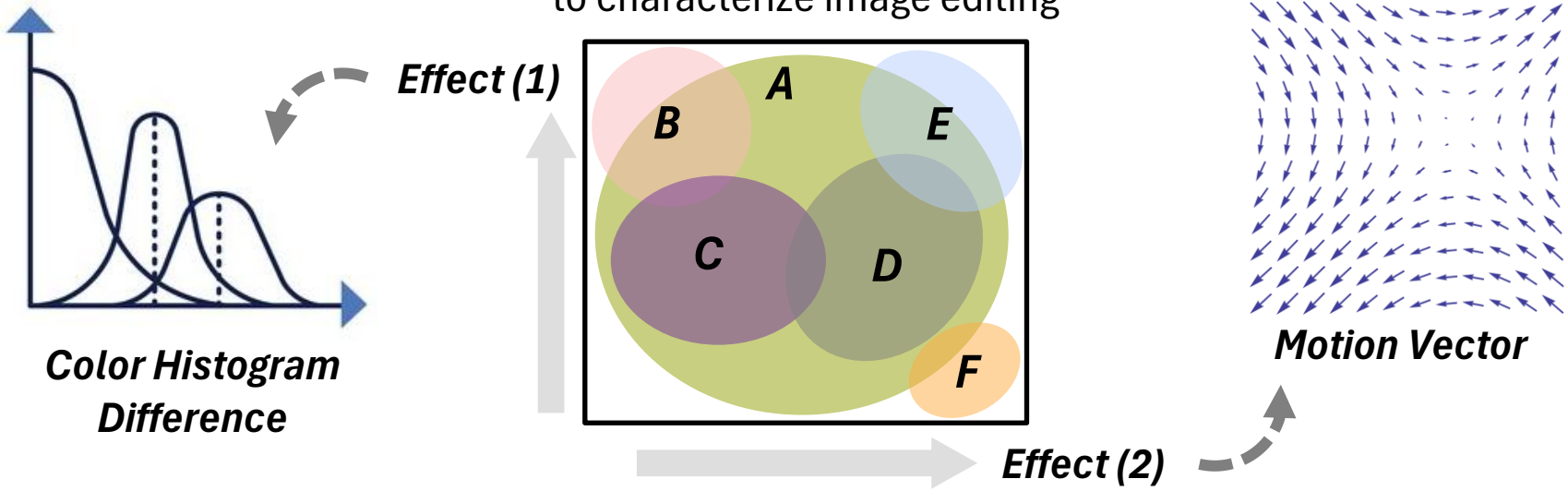
Motion Vector



Effect (2)

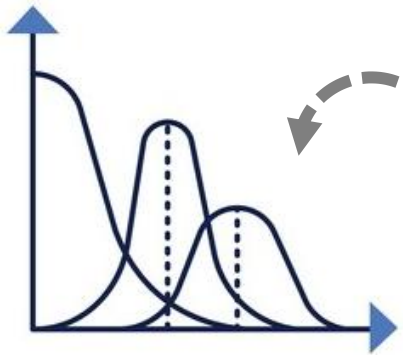
Data Processing: Representative Image Editing

- **2D feature space** simulating both effect (1) pixel value changes and (2) pixel location shifts



Data Processing: Representative Image Editing

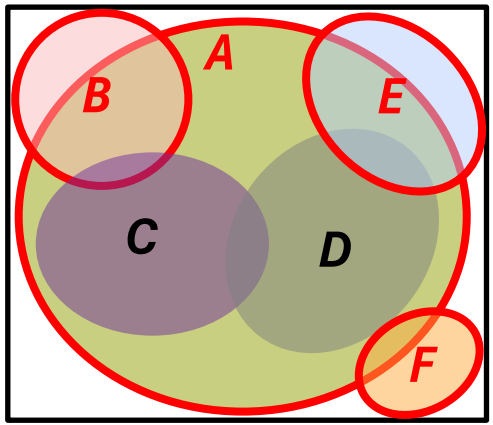
- Select largest spanning circle as the representative operation
- Continue selecting to fill up the uncovered regions



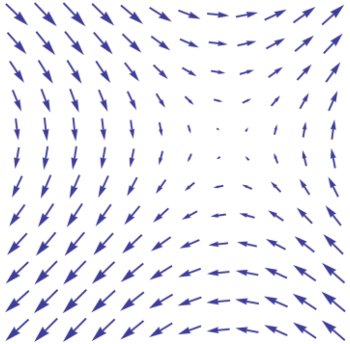
Color Histogram Difference

Effect (1)

Set (A, B, E, F) is one of the representative set

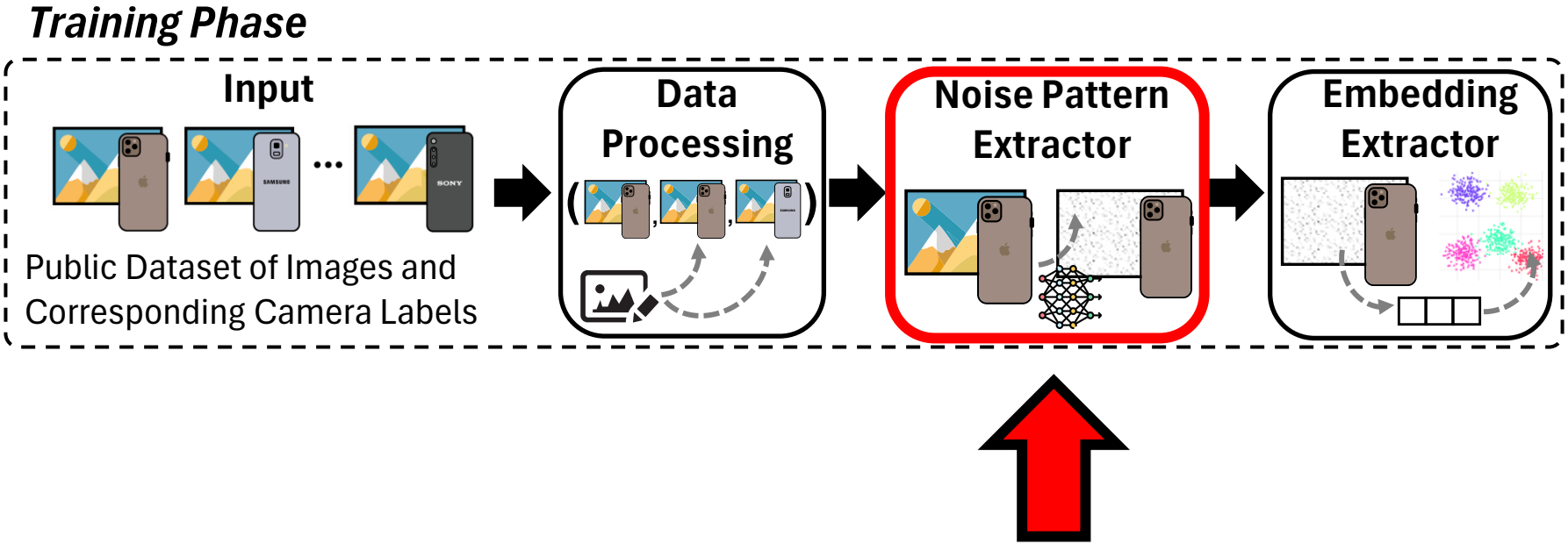


Effect (2)



Motion Vector

Design of *CAMPrints*

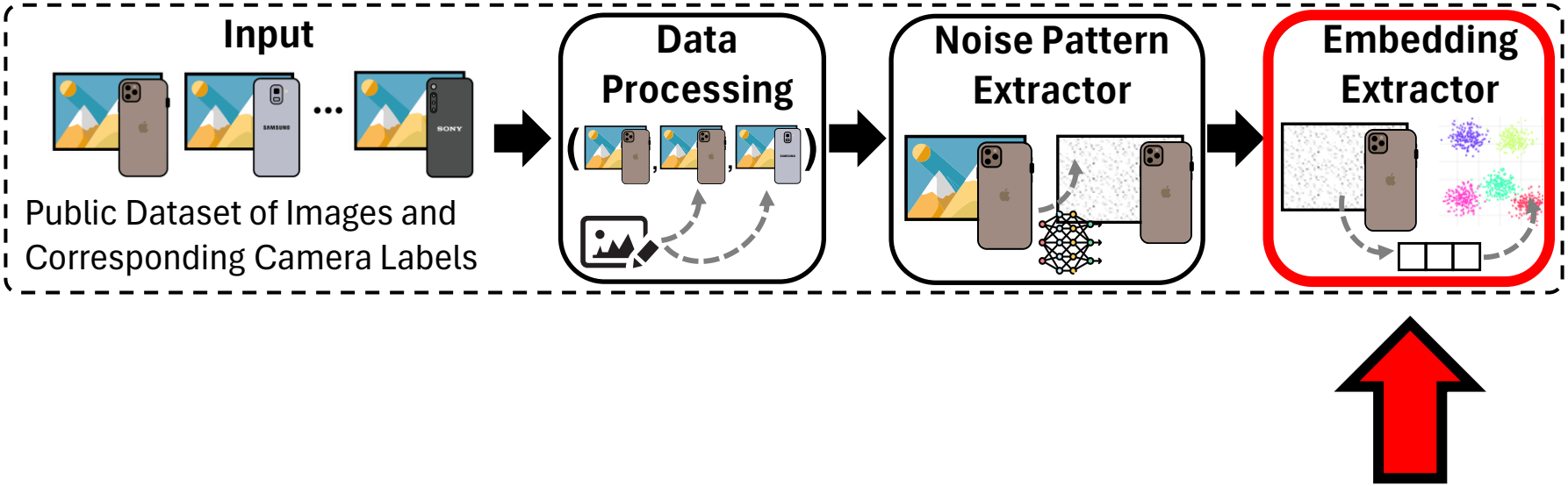


Design of *CAMPrints*

For Challenge #2

Multiple Sources of Noises

Training Phase



Embedding Extractor

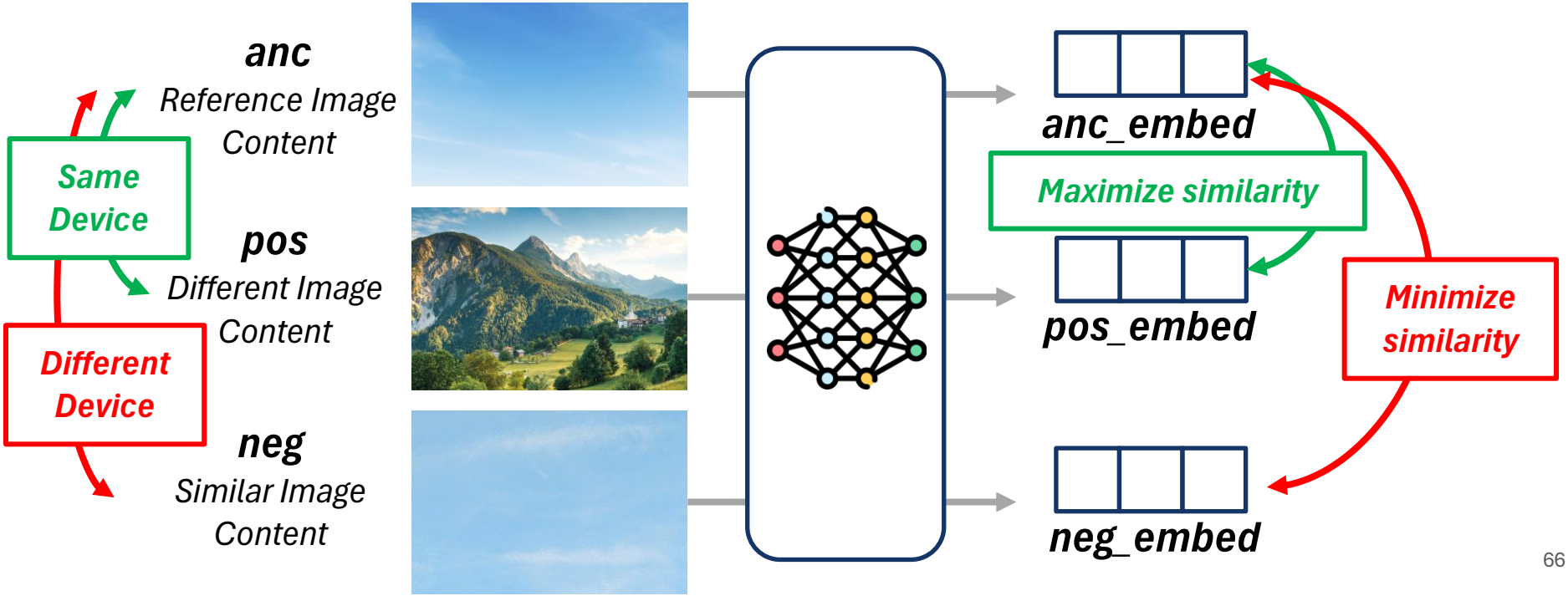
Goal: Encode noise pattern into latent representation to

1. Filter out **content-induced noises**
2. **Maximize similarity between features** from the **same device**

Embedding Extractor

Goal: Encode noise pattern into latent representation to

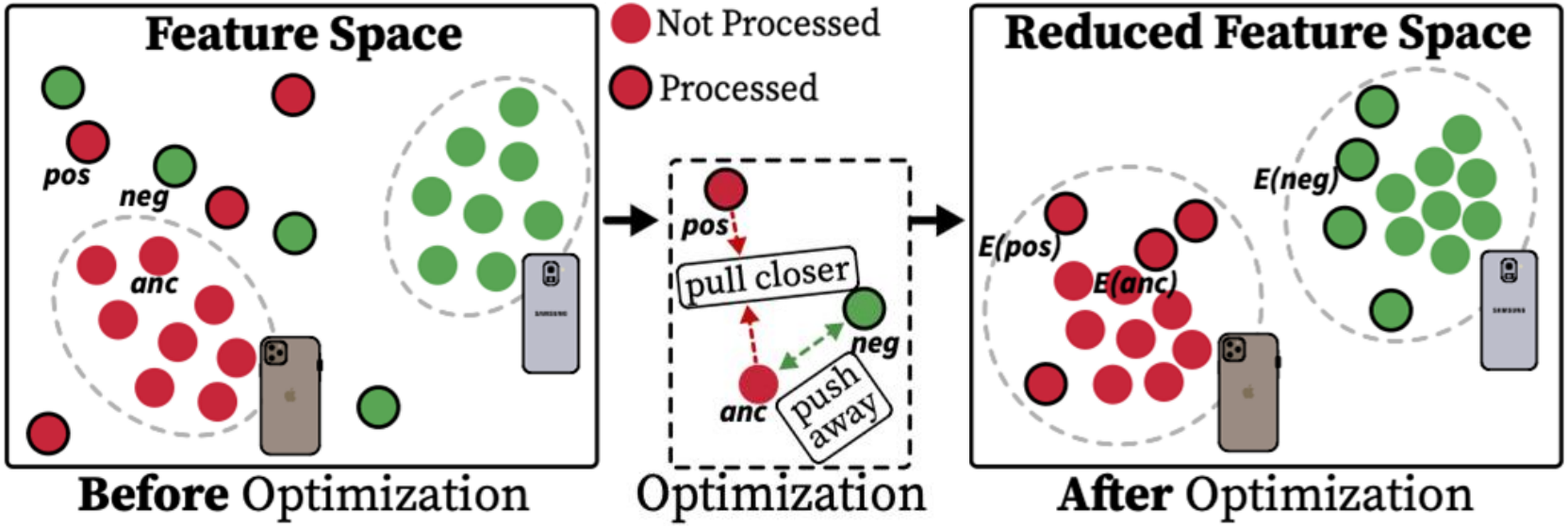
1. Filter out **content-induced noises**



Embedding Extractor

Goal: Encode noise pattern into latent representation to

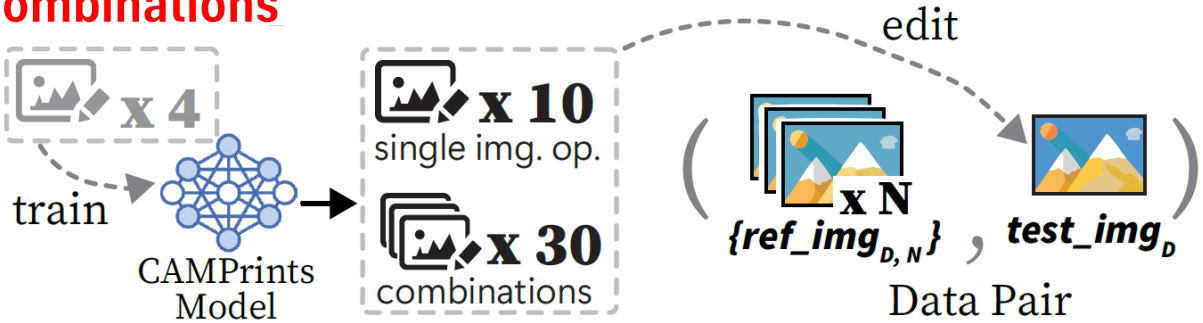
1. Filter out content-induced noises
2. **Maximize similarity between features** originating from same device despite image editing



Experiment setup

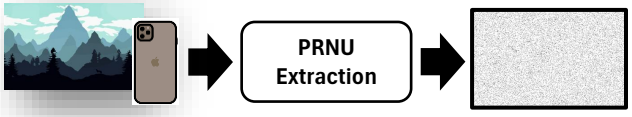
- We ensure **at least three different instances** per make-and-model to evaluate the **instance-level** accuracy

- We train the model with **only four** operations and test on **40 other operations and combinations**

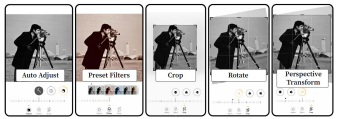


Summary of evaluation results

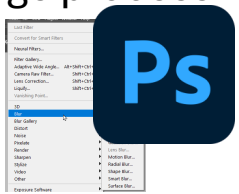
- Demonstrates **overall *average AUC* of 0.92**, outperform baseline methods by **1.8x**
- Remains **compatible** to existing PRNU extraction methods



- Remains robust against **number and order** of image operations



- Generalizes to **unseen** image processing operations

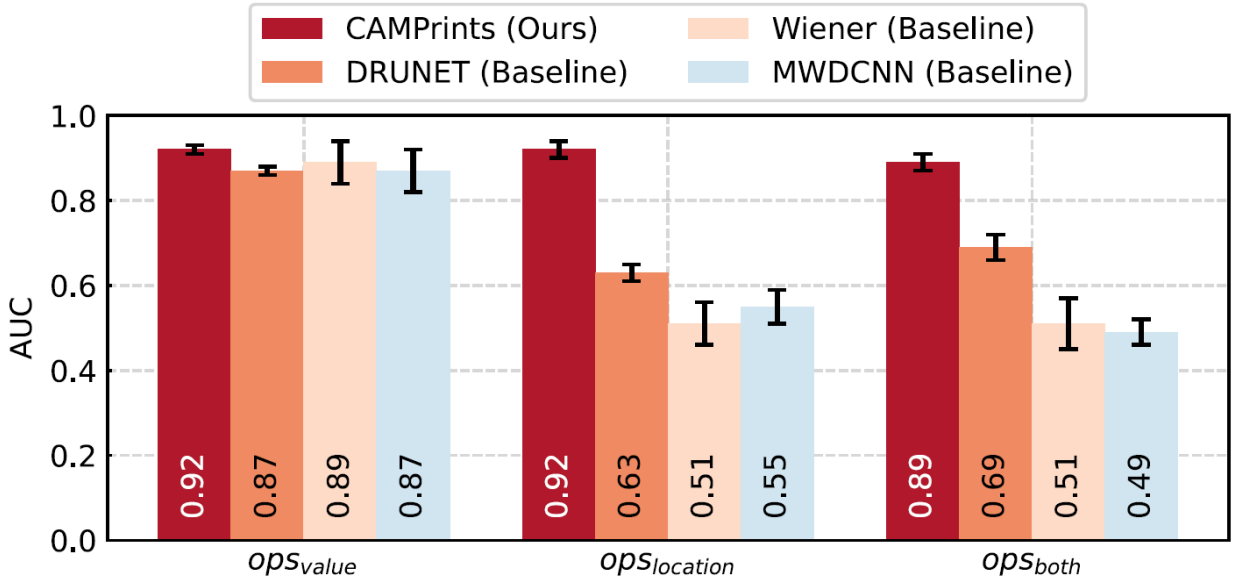


- Generalizes across **commercial software**

- Yields **80% less false positives** compared to Reverse Image Search

Overall performance

- *CAMPrints* significantly outperforms baselines by up to 1.8x in terms of AUC, especially for geometric transformations

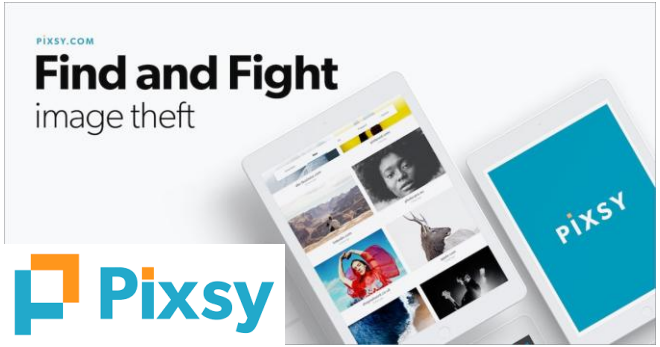


Discussion

① Real-world impact

Potential integration into

- Social media and photo sharing platforms
- Copyright monitoring services



***Pixsy**, an example copyright monitoring service*

② Future opportunities

- Co-existence of physical and digital "tokens" (e.g., invisible watermarks)

CAMPrints + 

- Open standards for digital authenticity and provenance

Google Meta Microsoft
amazon OpenAI C2PA
Coalition for Content Provenance and Authenticity

- Online media forensics



Future research

Extrinsic Provenance

External Labels & Metadata

Blockchain Technology

Database & Logs

Existing Approaches

Intrinsic Provenance

Physical Domain ⟷ **Digital Domain** ⟷ **Latent Domain**

Physical Domain

e.g., liquids & medicines

RGB cameras only

- Liquid form [MobiSys'22]
- Fabric form [SenSys'23]
- Powdered form [MobiSys'24]

Low-cost, high-speed sensors; sensor fusion ...

Digital Domain

e.g., images & videos

Content capture/creation

- Photography [MobiSys'25]
- Digital Art *(Ongoing...)*

Content itself

- Watermarks [S&P'26]
- Perceptual Hashing [ArtSec'26] + *more...*

Latent Domain

e.g., embeddings & weights

Inference behavior

- Embeddings [MobiSys'26]

Model-as-service

more...

Human-AI collaboration

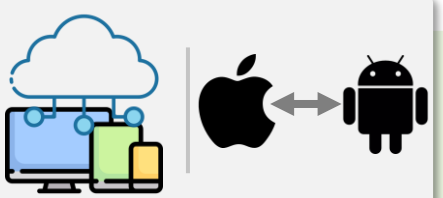
more...

Our Research Focuses

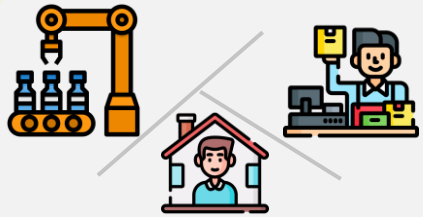
Future research

Multimodal
Fusion & Intelligence

Cryptographic Recording
of Intrinsic Properties



Cross-stack /
Platform integration



Multiple Deployment
Scenarios / Stakeholders

Hybrid Provenance

Extrinsic Provenance

Existing Approaches

Intrinsic Provenance

Physical Domain ⟷ Digital Domain ⟷ Latent Domain

Our Research Focuses

Broader research theme

Computing for Social Good

e.g.,

Spy Cam Detection [SenSys'21]

Trustworthy Mobile Sys. & Apps.

e.g.,

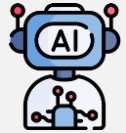
Voice Deepfake [SEC'24]

Accountable Human-AI Collab.

e.g.,

Sensor-augmented Generative AI

Auditable Physical AI

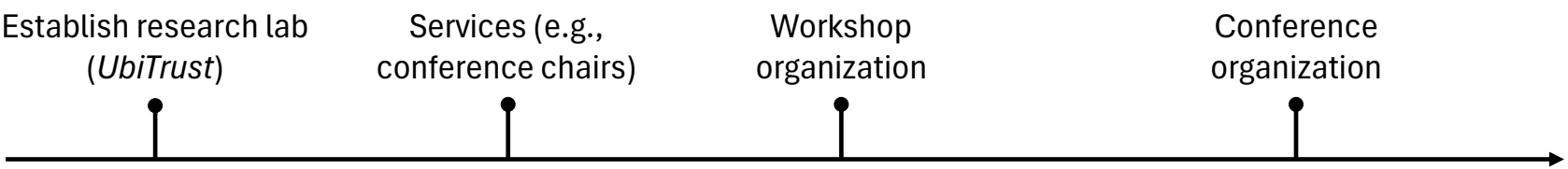


e.g.,

Provenance-augmented JEPA

Develop ubiquitous systems to build trust.

Research and industrial collaboration opportunities



Mobile Sensing *(Primary)*

Mobile venues
- ACM MobiSys
- ACM MobiCom
- ACM SenSys
- IMWUT UbiComp
- IEEE PerCom

Journals
- TMC / TOSN / IOTJ / PMC

Secure Computing *(Secondary)*

Security venues
- IEEE S&P
- USENIX Security
- ACM CCS

Vision / AI venues
- AAAI / IJCAI
- CVPR / ECCV / ICCV
- ICLR / ICML / NIPS

Industrial Collaboration

- **Brand protection**
  Ennventure RED POINTS
- **Logistics / supply chain**
  amazon 3M Science. Applied to Life.™
- **Monitoring services**
  Pixsy flickr TinEye
- **Open-source projects**

Teaching

Experience

Graduate Tutor
National University of Singapore
Aug 2020 - Aug 2025

- CS3203 Software Engineering Project
  - AY2020-2021 Semester 1 (Aug 20 - Dec 20)
  - AY2020-2021 Semester 2 (Jan 21 - May 21)
  - AY2021-2022 Semester 2 (Jan 22 - May 22)
- CS1101S Programming Methodology
  - AY2022-2023 Semester 1 (Aug 22 - Dec 2)
  - AY2023-2024 Semester 1 (Aug 23 - Dec 3)
  - AY2024-2025 Semester 1 (Aug 19 - Dec 3)
- CS2102 Database Systems
  - AY2022-2023 Semester 2 (Jan 23 - May 23)
  - AY2023-2024 Semester 2 (Jan 24 - May 24)

Teaching Assistant
National University of Singapore
Aug 2019 - May 2020

- CS4247 Graphics Rendering Techniques
  - AY2019-2020 Semester 2 (Jan 20 - May 20)
- CS3241 Computer Graphics
  - AY2019-2020 Semester 1 (Aug 19 - Dec 19)

Project advisor for Orbital Best Advisor Award
National University of Singapore
AY2019-2020 Summer (May 20 - Aug 20)

I like to design and teach project-based courses

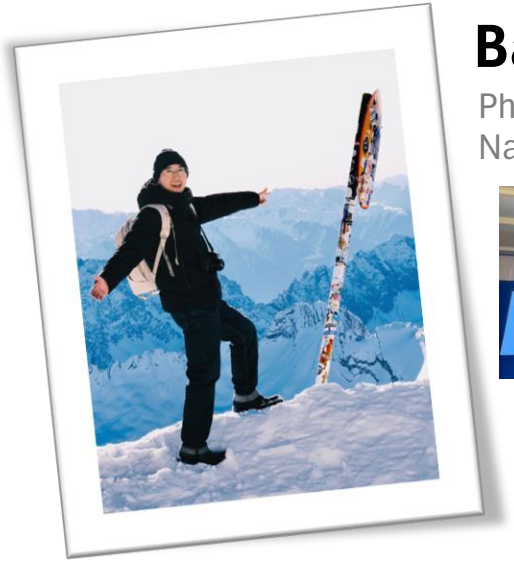
Introductory-level courses

- Programming foundation and methodology
- Software engineering practices and projects
- Database systems and information retrieval
- Computer graphics and rendering

Graduate-level courses

- Multimedia systems, security and provenance
- AIoT systems, mobile sensing and distributed AI
- Computer vision
- Human-computer interaction and human-AI collaboration
- Knowledge-driven and explainable AI

Thank you!



Bangjie Sun

PhD Candidate | Research Assistant
National University of Singapore




Research Interests

A central premise of my research is that no single provenance signal is sufficient on its own. Beyond cryptographic records and other forms of extrinsic provenance, I study how visible physical signals, sensor fingerprints, and computational forensics provide complementary **intrinsic provenance** for building trustworthy systems that remain robust under adversarial manipulation. I also aim to make provenance recovery and verification **practical on commodity everyday devices** rather than confined to specialized laboratories or proprietary platforms. Ultimately, I seek to advance **hybrid provenance** systems that integrate these signals not only to verify the origin, authenticity, and transformation history of physical and digital artifacts, but also to enable **accountable human-AI workflows** in which transformations, interventions, and responsibility can be meaningfully audited.

Mobile & Sensing Systems PRIMARY

Security & Privacy SECONDARY