



# Building Widely Usable Provenance Systems for Physical and Digital Artifacts

**Bangjie Sun**

PhD Candidate | Research Assistant | National University of Singapore

# The story of Salvator Mundi ...

## Origin

By Leonardo da Vinci

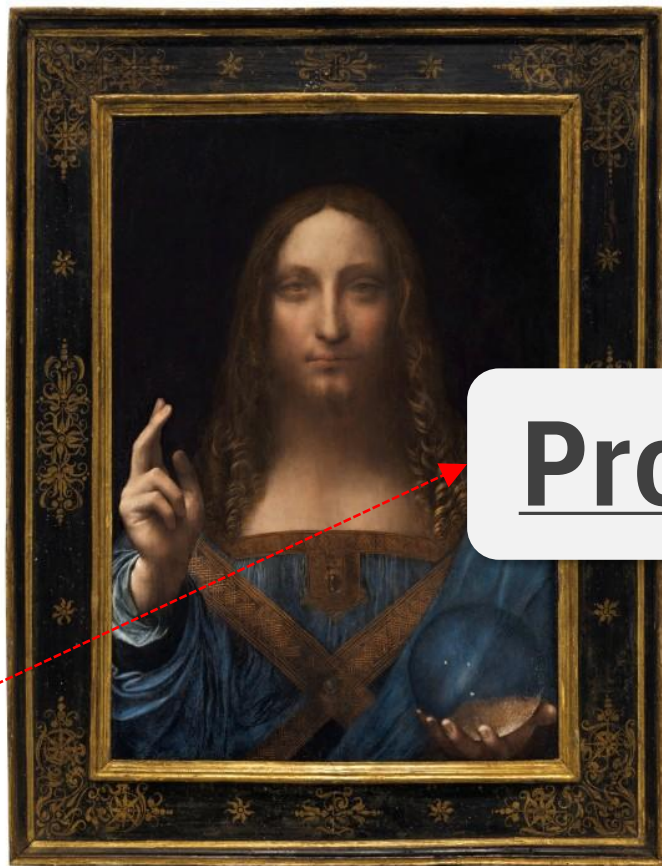
1958

Suspect of **counterfeit**

Sold for only £45

2017

Sold for \$450M



## Provenance

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

# Importance of provenance in modern society

- Problems arise without evidence of origin, authenticity and ownership

Provenance evidence

CNA Insider

### Are you buying fake skincare products online? The problem is more common than you think

Lab tests on ski authorised retail risks

**BBC** Register

### Fake alcohol deaths highlight SE Asia's methanol problem

22 November 2024

Frances Mao  
BBC News



The price difference may no retail shops and the same it finds out.



## FAKE LUXURY FRAGRANCES SEIZED!



Counterfeit consumer goods

**Origin:**

*Where do ingredients come from?*

**Authenticity:**

*Is it genuine and from an authorized seller or brand?*

**Ownership:**

*Has it ever been sold, returned, resold, or repackaged?*



Manufacturers, retailers, consumers

# Importance of provenance in modern society

- Problems arise without evidence of origin, authenticity and ownership

2.5 billion online images stolen every day in 2018

**Billions of fake images, videos generated by AI rewrite human memory**

Prolonged social media in face of e  
**'Mass theft': Thousands of artists call for AI art auction to be cancelled**

Letter says many of works being sold by Christie's are made by AI models trained on pieces by human artists, without a licence



**Fake & stolen digital content**



## Origin:

*Who created this image/video?  
What is the original source?*

## Authenticity:

*Is it edited after creation? Is it generated by AI?*

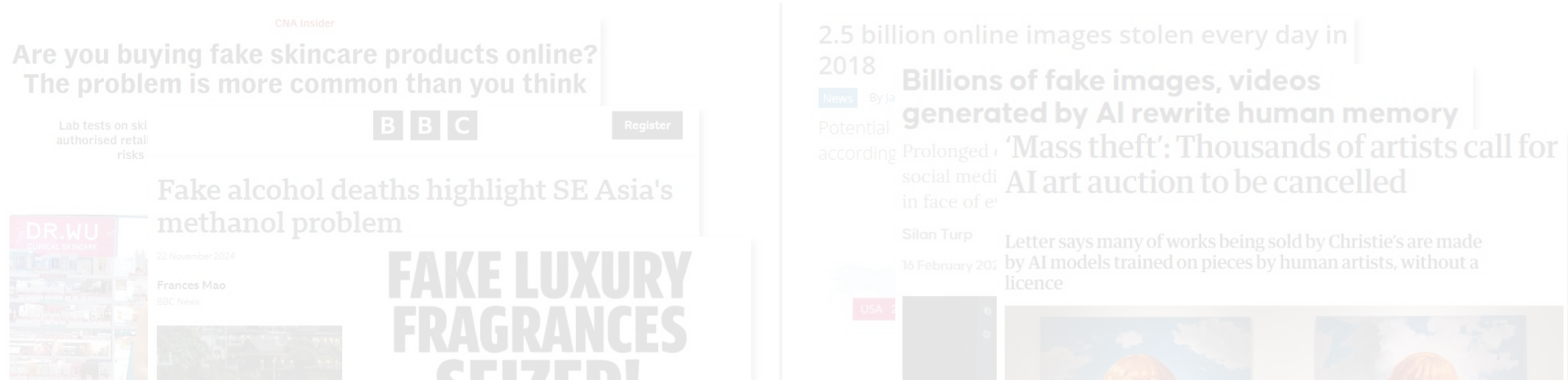
## Ownership:

*Who owns the copyright?*

**Content creators, platforms**

# Importance of provenance in modern society

- Problems arise without evidence of origin, authenticity and ownership



Verify the origin, authenticity and ownership of physical and digital artifacts.

# We recover provenance evidences, but ...

- Existing solutions rely on **extrinsic** evidences
- Extrinsic provenance: from **“name card”** attached **outside** the artifact itself



Differentiation often relies on **labels & packaging**



Examples of extrinsic evidences

# Problems with extrinsic provenance

- Easily modified, duplicated, removed, or forged
- More severely, **detached** from the artifact itself



Physical content



Second-hand empty perfume bottles

Linked to packaging only



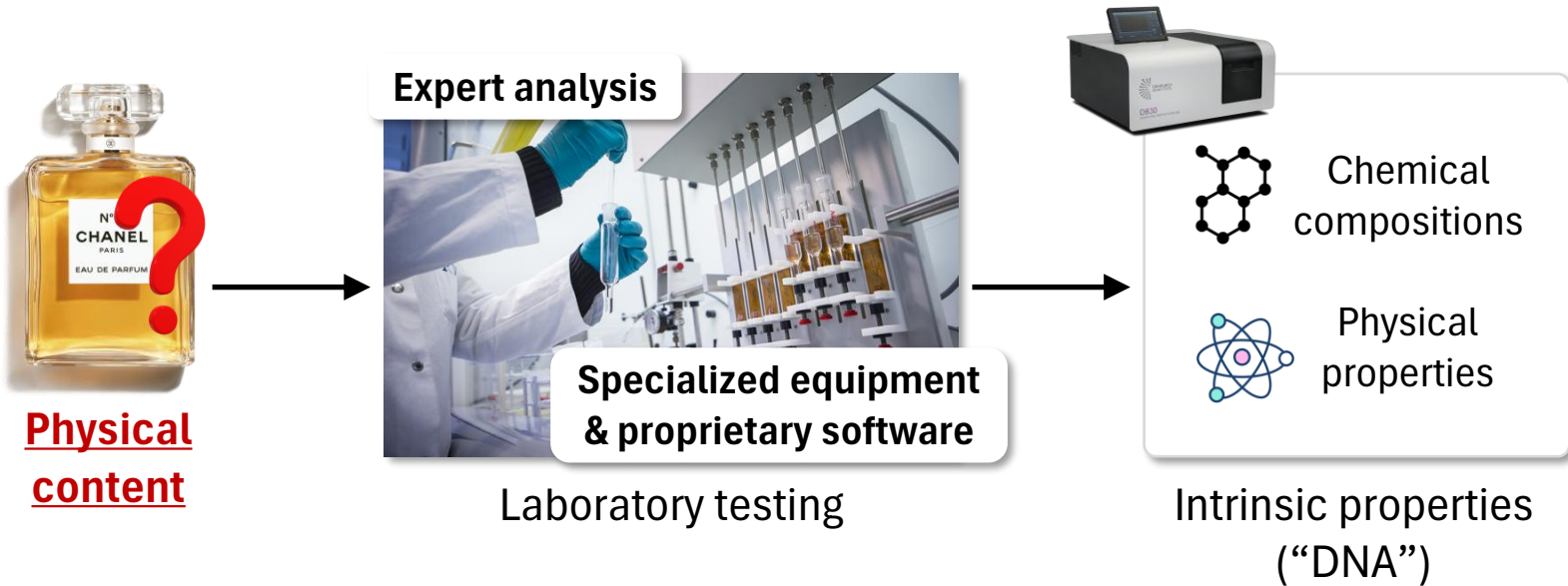
**It does not tie to the artifact itself**

RFID tags

Examples of extrinsic evidences

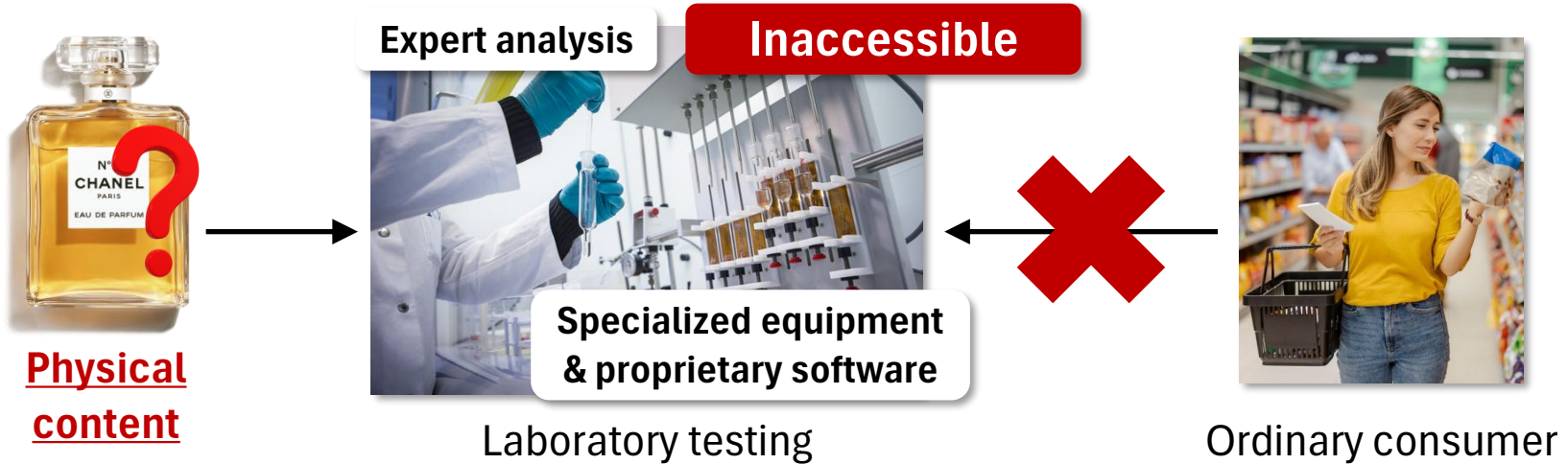
# Intrinsic provenance is the right way

- Intrinsic provenance: from evidence recovered from **intrinsic properties** (“DNA”) inherent to the artifact itself



# Intrinsic provenance is the right way, but ...

- Intrinsic provenance: from evidence recovered from **intrinsic properties** (“DNA”) inherent to the artifact itself



# It applies to digital content as well

- Ubiquitous intrinsic provenance also benefits digital content
- Wide deployment without proprietary software/expertise



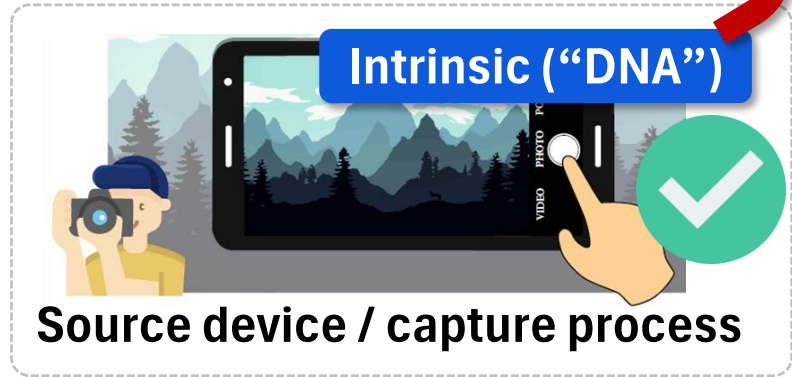
Photography



Copied/Edited



Metadata



Source device / capture process

**My research aims to**

**Build widely usable intrinsic provenance systems to address societal issues in physical and digital domains.**

# Research landscape

## Physical Domain

e.g., liquids & medicines

Tackle counterfeit, substandard physical products using commodity cameras only



Liquid form  
[MobiSys'22]



Fabric form  
[SenSys'23]



Powdered form  
[MobiSys'24]

*Note: different physical forms require distinct scientific insights and technological innovations*

## Digital Domain

e.g., images & videos

Tackle stolen or fake digital content using capture or creation process

*For stolen content:*



Photography  
[MobiSys'25]



Digital Art  
(Ongoing...)

Robust Image Retrieval  
[ArtSec'26 co-located with Oakland'26]

*For fake content:*



Fake Image  
[Oakland'26]



Fake Audio  
[Security'24]

## 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-quality masks, medicines and sanitisers during the pandemic.

## Fake honey scandal widens to Australian-sourced brands

### The Real Reason Your Olive Oil Is Probably Fake



BY MICHAEL SOMMERS / UPI

There are healthy for authentic **extra virgin** seemingly unlimited case.

Investigative journal which blew the lid of shocked America who **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

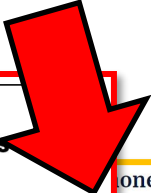


In 2008, melamine was added to milk and infant formula to increase its protein content. This led to the hospitalisation of around 54,000 infants, 6 deaths from kidney stones and, ultimately, a number of criminal prosecutions, resulting in 2 executions.

153 View all comments

# Counterfeit liquid food products

- Detrimental health effects to consumers



**MUNCHIES**  
FOOD NEWS

## 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 Miss Pardi

16 August 2017, 3:00am

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.

## 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.

## Money scandal widens to Australian-sourced

## Reason Your Olive

...site awful and unhealthy foods that taste like... or as intimates refer it: EVOO – which benefits – if, indeed, it's authentic. Unfort...

...eller is author of the whistleblowing c... 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




**MUNCHIES**  
FOODSERVICE

## 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 Head

16 August 2017, 3:00am



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.

## 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.

Money scandal widens to Australian-sourced

The Real Reason Y

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

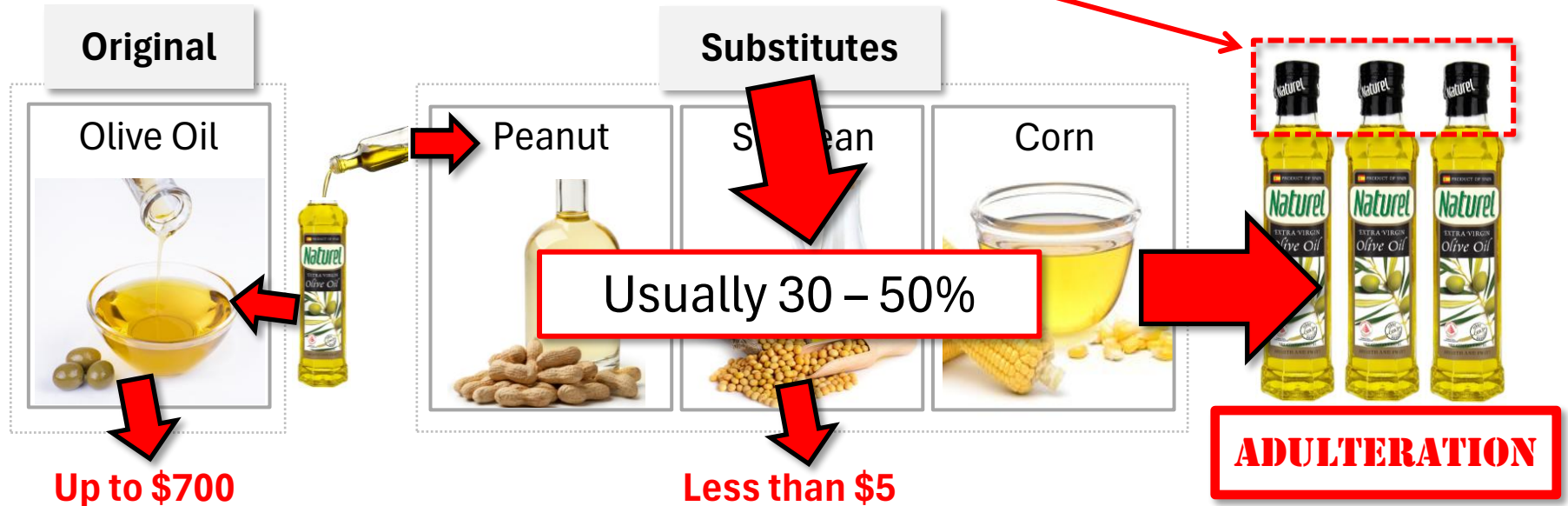
By Chris Cattini on 04-Apr-2016 10:00:00



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.

# Threat model: counterfeiters adulterate liquid content

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



# Threat model

- **Counterfeiter's goal:**
  - Adulterate the liquid content to strive for economic gain
  - Preserve product appearance and packaging to deceive consumers
- **Counterfeiter's capabilities:**
  - Use cheap substitutes to replace a substantial portion of original content
  - Repackage liquid content in authentic bottles



# Use case: verify authenticity of olive oil

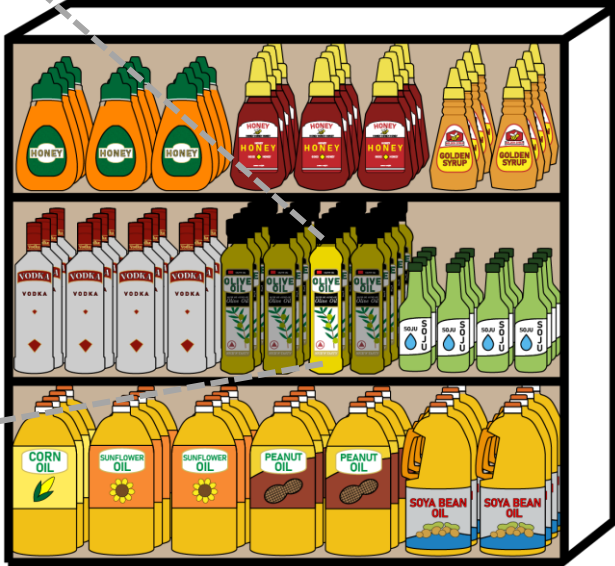


# Use case: verify authenticity of olive oil



✓ Authentic

SUPERMARKET



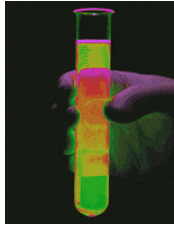
*How can you tell which one is authentic?*

# 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



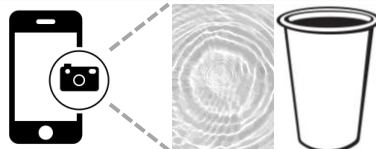
- Academic proposals

## Wireless signals



[Ha, NSDI'20]

## Smartphone vibration



[Yue, MobiSys'19]



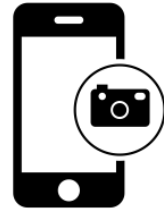
[Huang, MobiCom'21]

### *Disadvantage:*

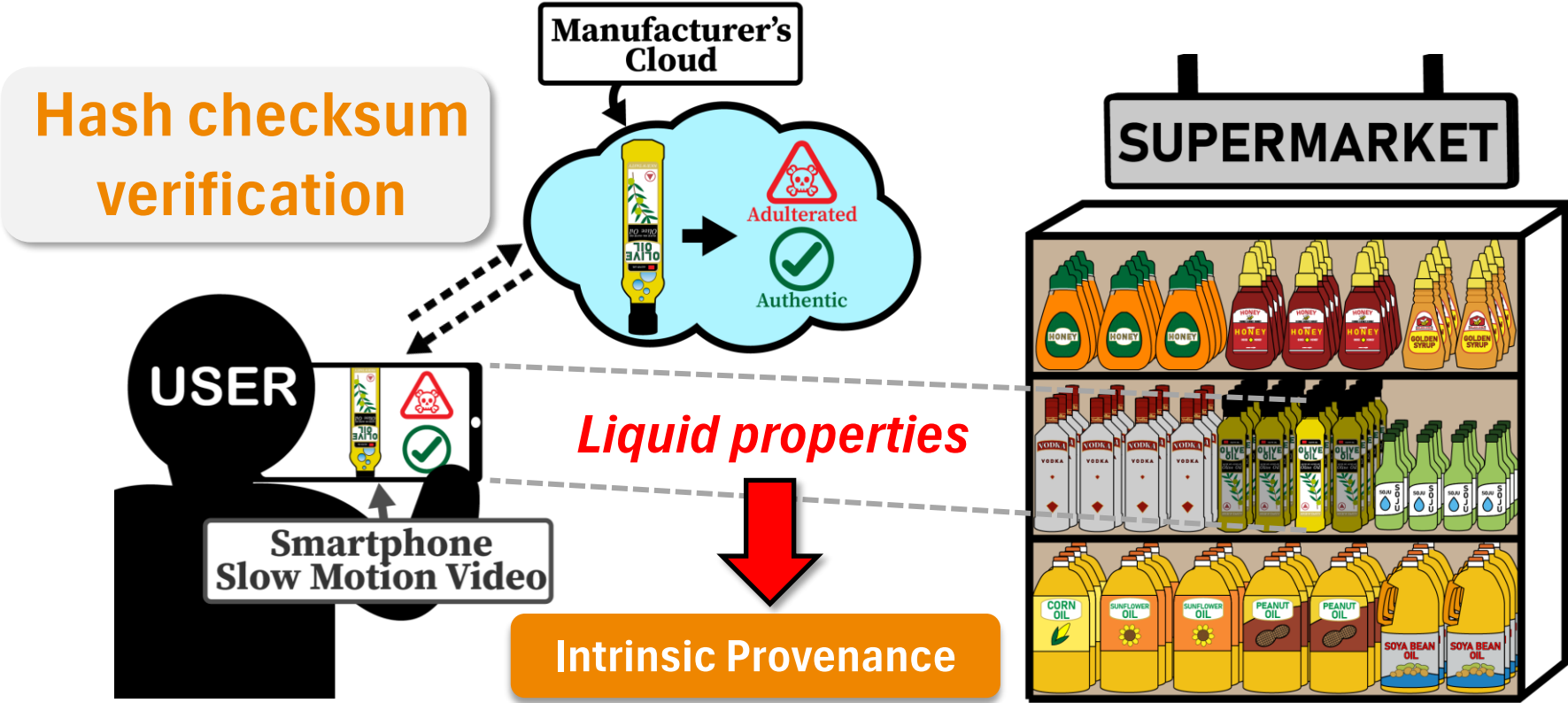
- Require **additional** and **specialized** equipment
- Require **opening** of the bottle and **controlled** settings



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



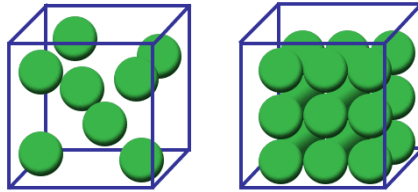
# Our Work: *LiquidHash*



# Liquid properties

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

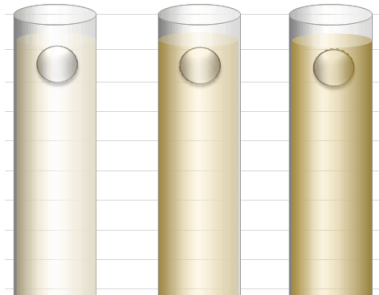
Density



Surface tension

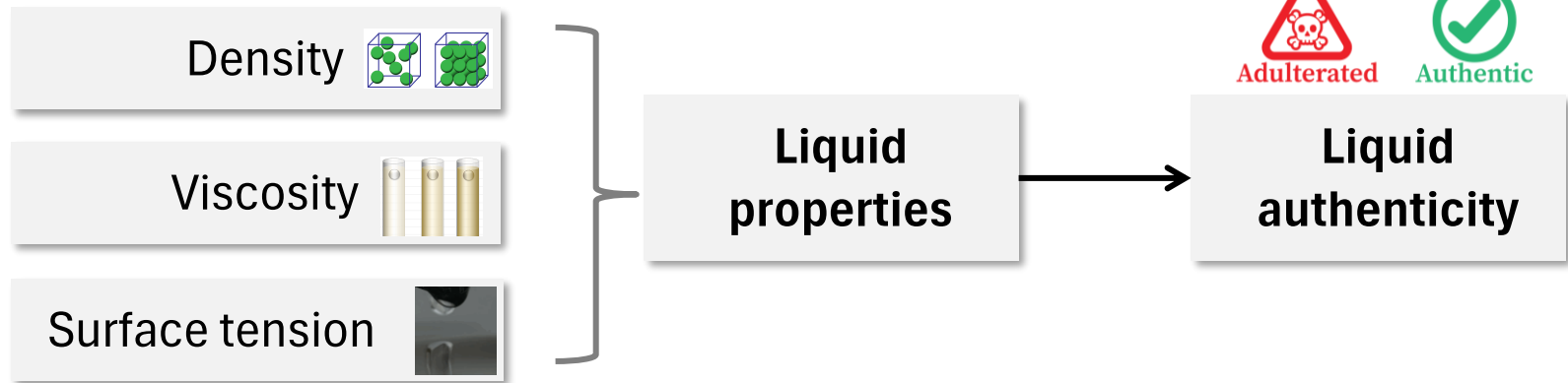


Viscosity



# 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

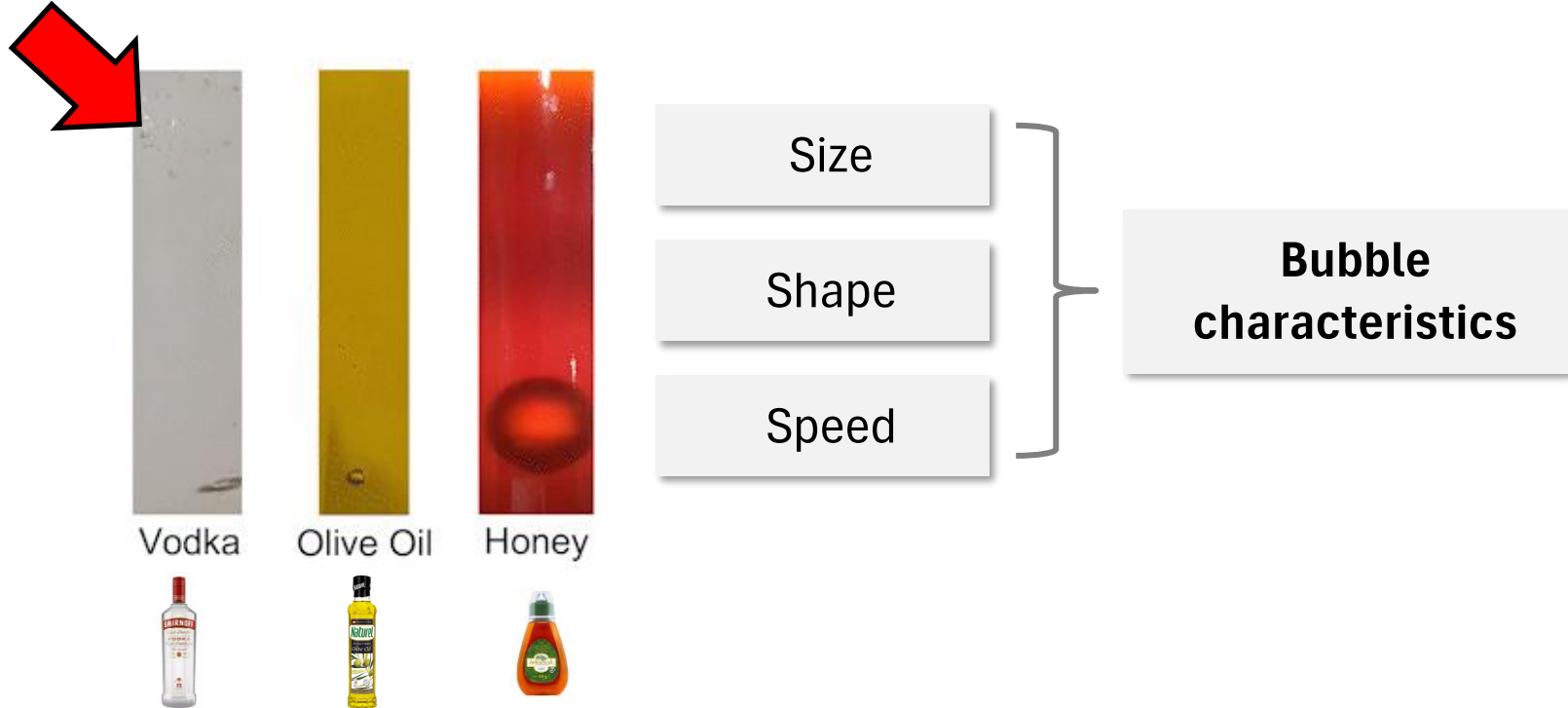


***What do we do with this setup?***

This constrained setup  
has limited granularity of  
information!

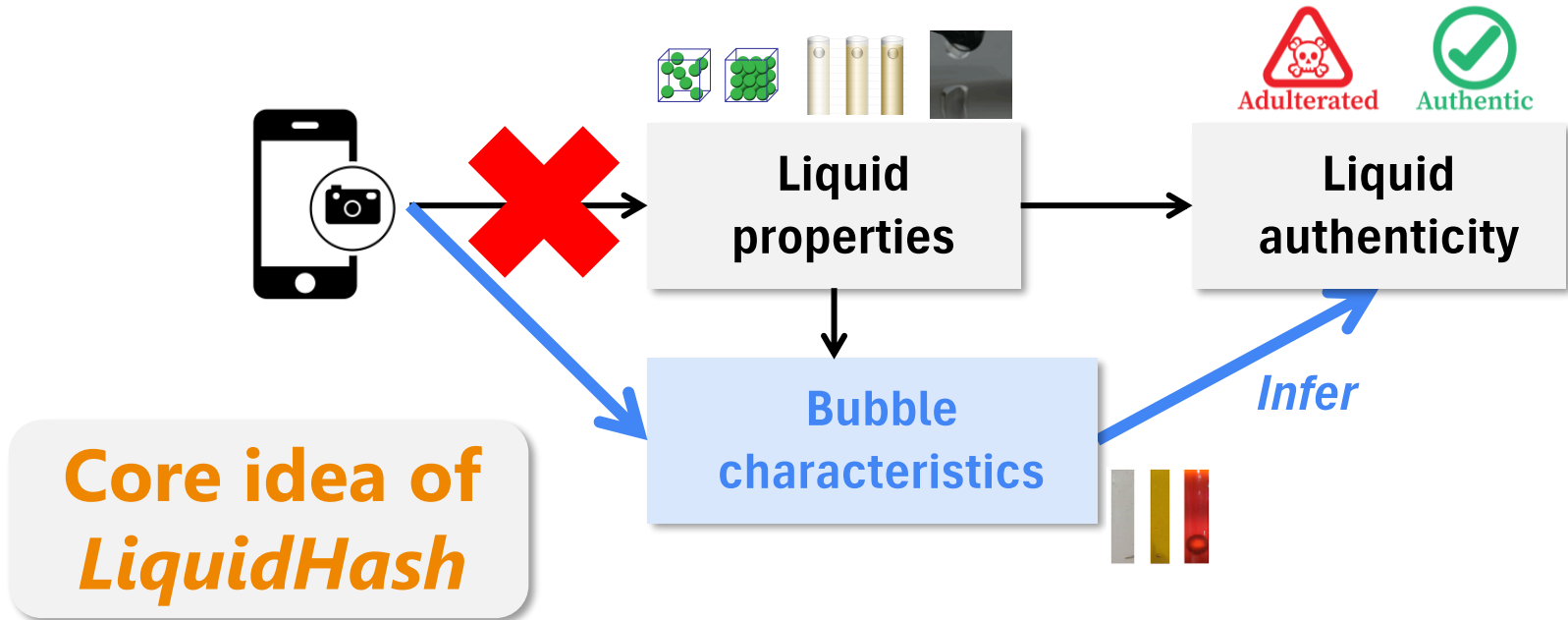
# Bubble characteristics

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



# Bubble characteristics

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

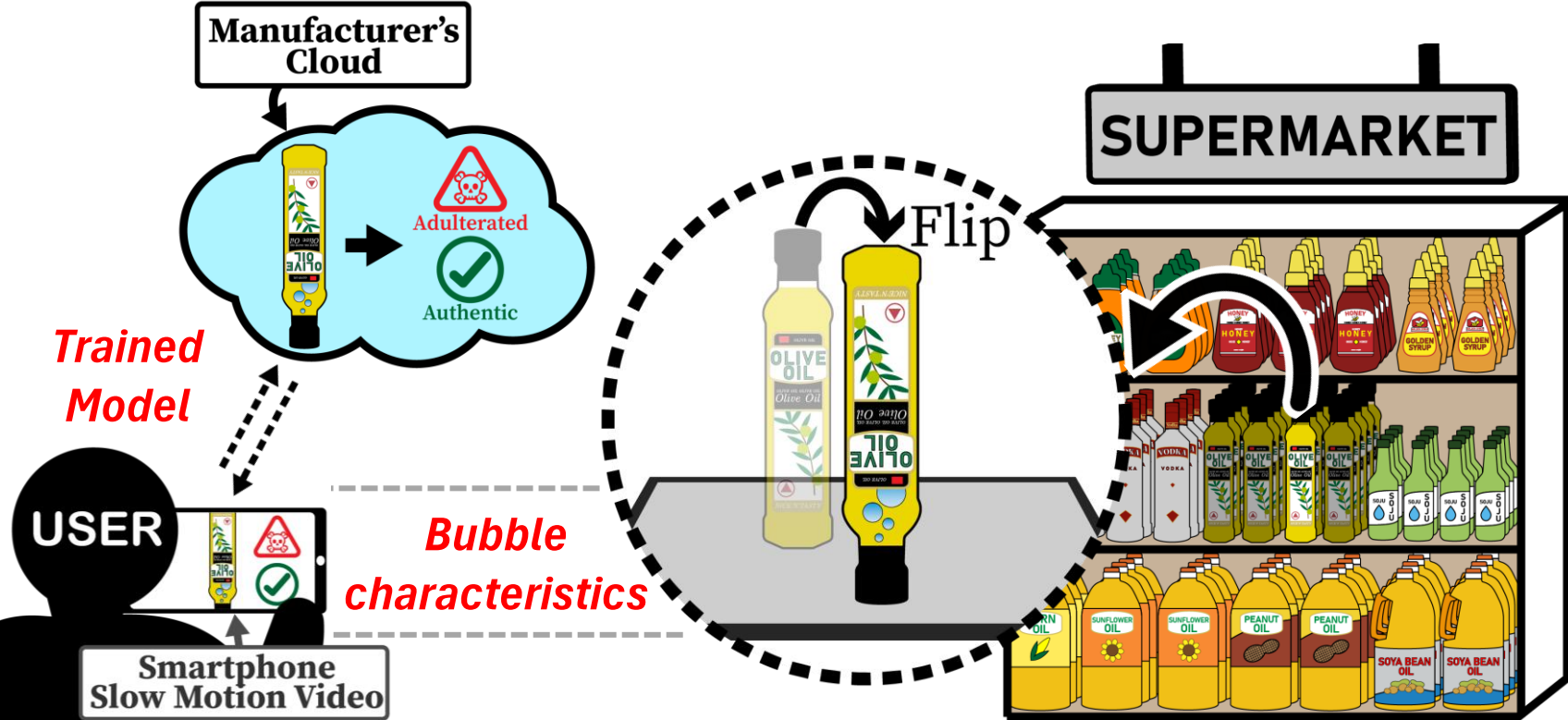


# Our Work: *LiquidHash*

Human interaction:  
*Flip once!*

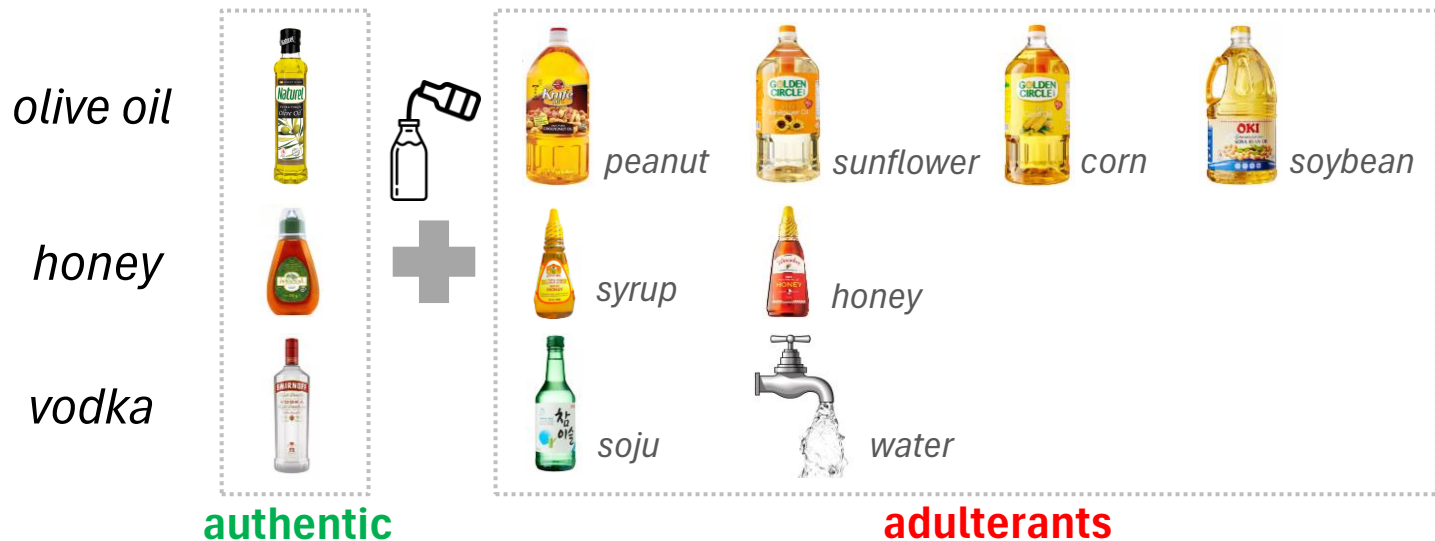


# Our Work: *LiquidHash*



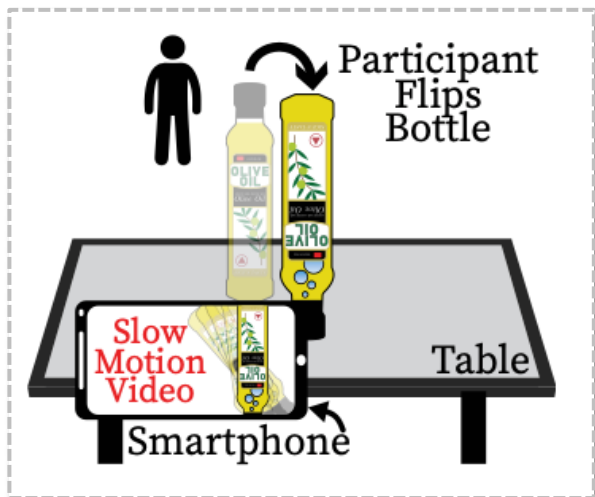
# Evaluation setup

- 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



## *LiquidHash*

70 tests x 5 Participants  
Leave-one-out approach

VS



## *Baseline: No Assistance*

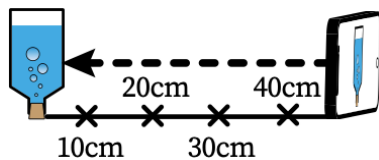
Participants can **interact freely** with liquid products **except opening** the bottles

# Summary of evaluation results

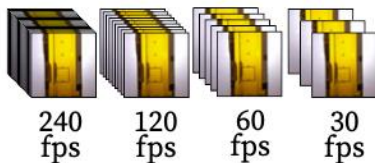
- Demonstrates **overall detection accuracy up to 95%**



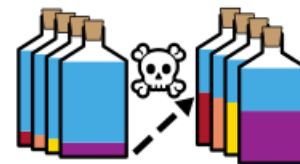
- Robust against **camera-to-bottle distances**



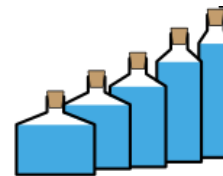
- Robust against **video framerates**



- Generalizes across **adulterant concentrations**

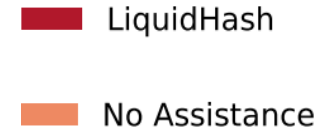
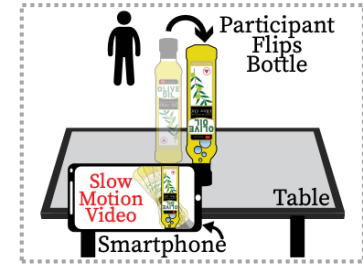
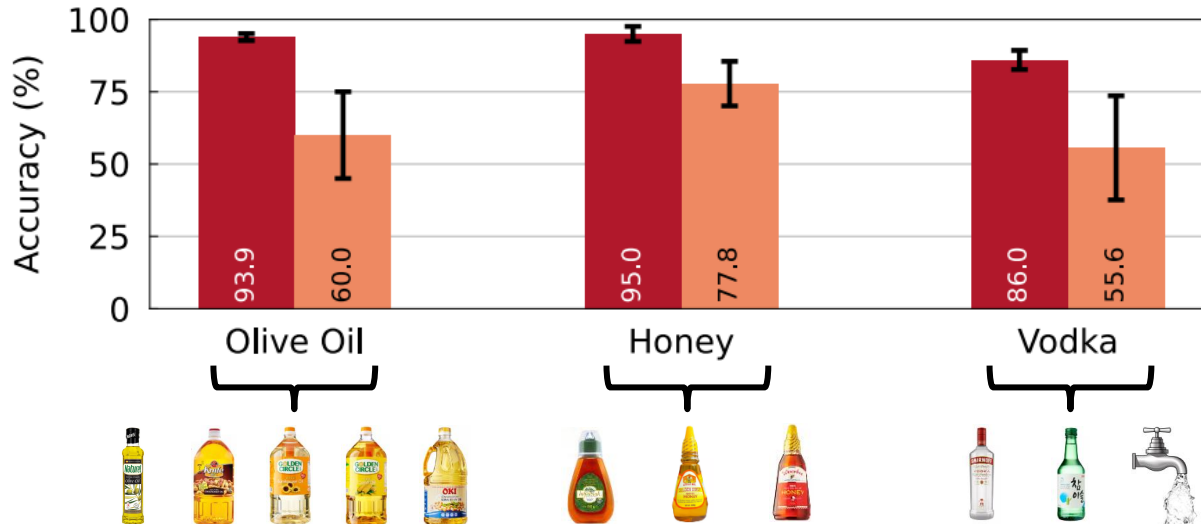


- Generalizes across **bottle dimensions**



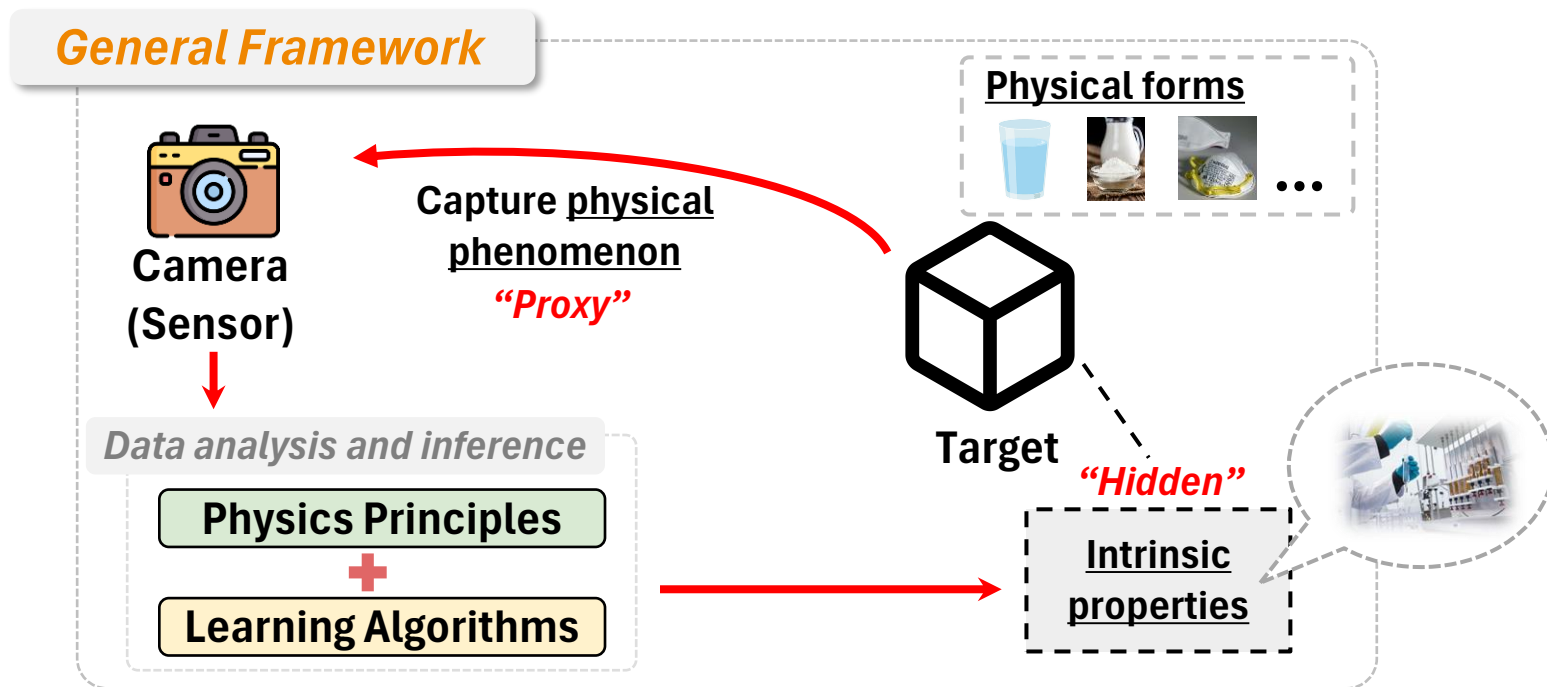
# Main results

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



# Methodological Generalization

- Commodity RGB cameras as the tool to extract intrinsic properties
- Utilize capturable physical phenomenon as **proxy**



# Research landscape

## Physical Domain

e.g., liquids & medicines



Liquid form  
[MobiSys'22]



Fabric form  
[SenSys'23]



Powdered form  
[MobiSys'24]

## Digital Domain

e.g., images & videos

### Problem 1: generalize to media modalities

*Similar to physical products, different forms of digital content require distinct innovations*

### Problem 2: identify intrinsic properties

*Unlike physical properties, intrinsic properties of digital content are not as straightforward*

### Problem 3: extract properties robustly

*Adversaries have more control over the digital content to “hide” intrinsic properties*

**Form**      **Intrinsic properties**      **Phenomenon**

Liquid      Density, viscosity, surface tension      Rising air bubbles

Fabric      Fiber diameter, volume fraction, thickness      Light scattering and absorption

Powder      Wettability, porosity      Droplet deformation

# Research landscape

## Physical Domain

e.g., liquids & medicines



Liquid form  
[MobiSys'22]



Fabric form  
[SenSys'23]



Powdered form  
[MobiSys'24]

Form	Intrinsic properties	Phenomenon
Liquid	Density, viscosity, surface tension	Rising air bubbles
Fabric	Fiber diameter, volume fraction, thickness	Light scattering and absorption
Powder	Wettability, porosity	Droplet deformation

## Digital Domain

e.g., images & videos

Tackle stolen or fake digital content using **capture or creation process**

*For stolen content:*



Photography  
[MobiSys'25]



Digital Art  
(Ongoing...)

Robust Image Retrieval  
[ArtSec'26 co-located with Oakland'26]

*For fake content:*



Fake Image  
[Oakland'26]



Fake Audio  
[Security'24]

# 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**

**72%**

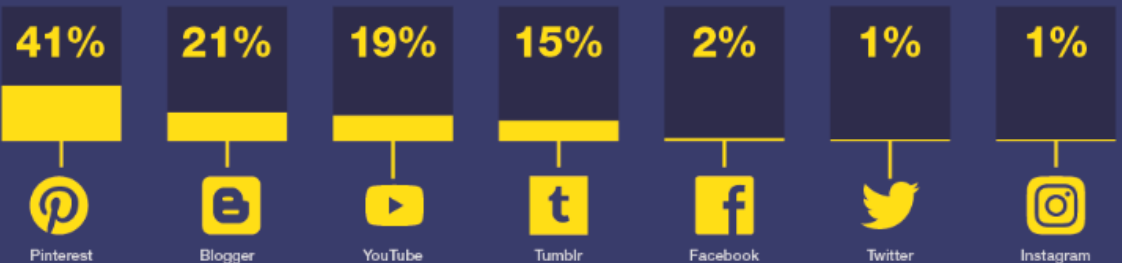
of images taken by businesses are **altered**

For every image used illegally, photographers and image agencies lose about \$446

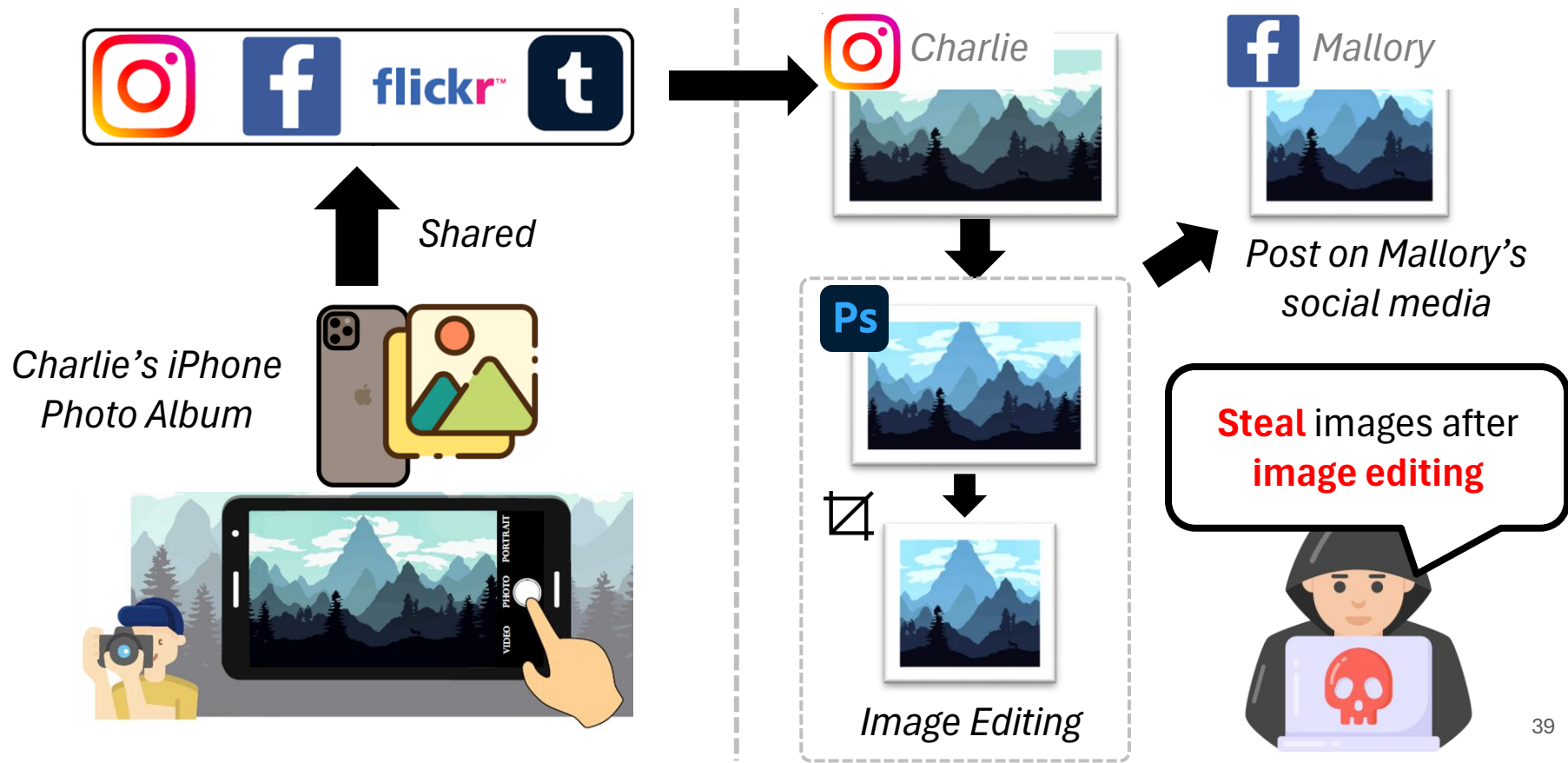


Top **social media** sites for image theft\*

\*Percentage of infringement cases brought up on each platform

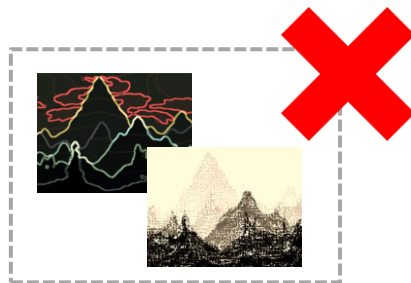


# Threat model: adversaries steal online photos

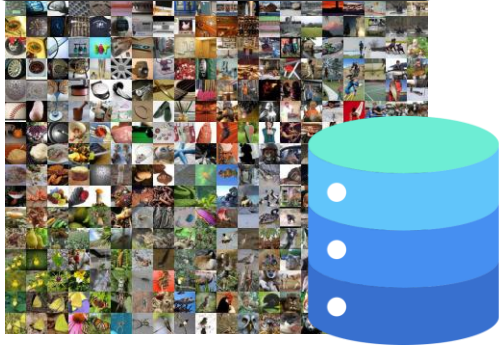


# Threat model

- **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



# How can social media combat image theft?



Search from image database

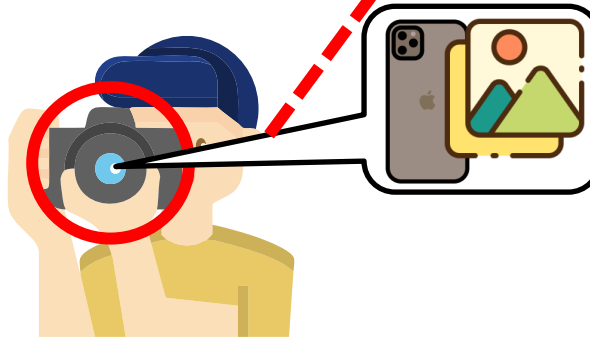


*"Physical Token"*

*Physical Proof of Ownership*

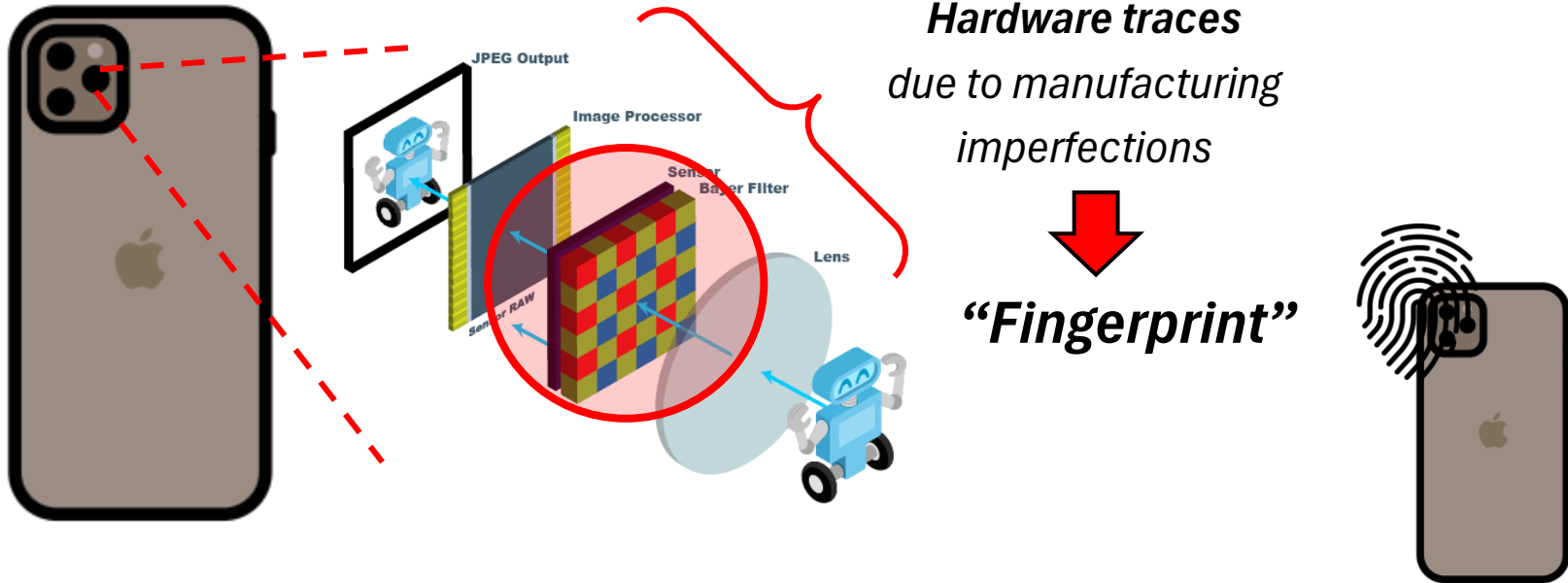


**How to help Charlie combat image theft?**



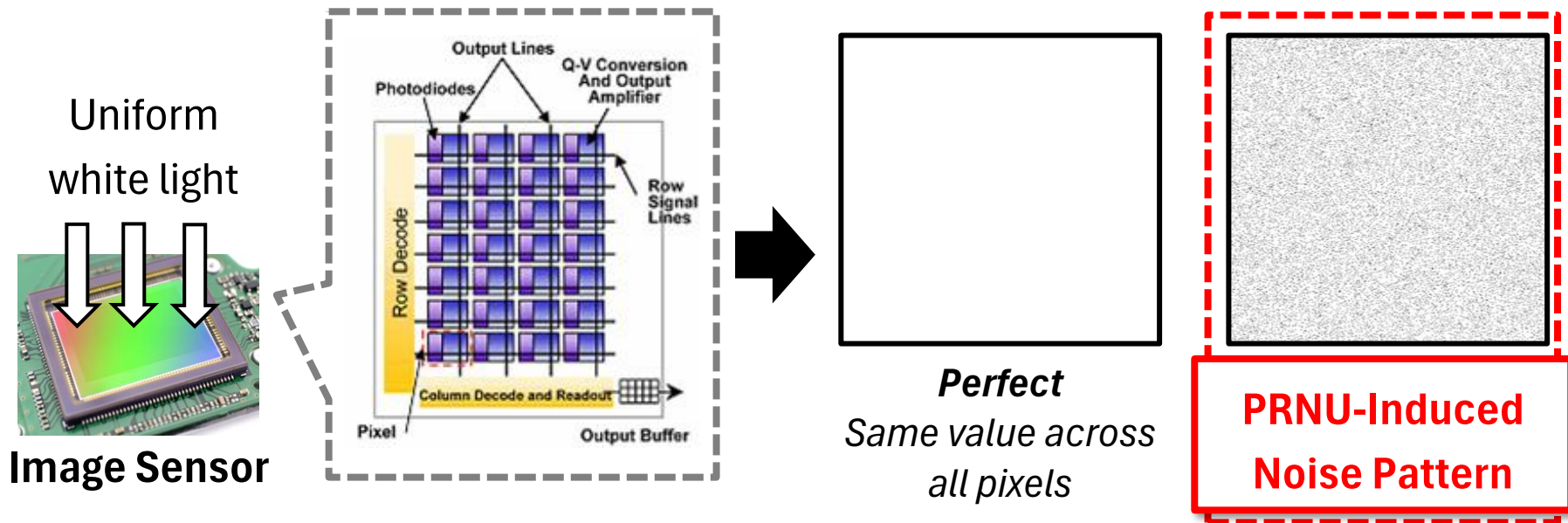
# Utilize camera “fingerprints”

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



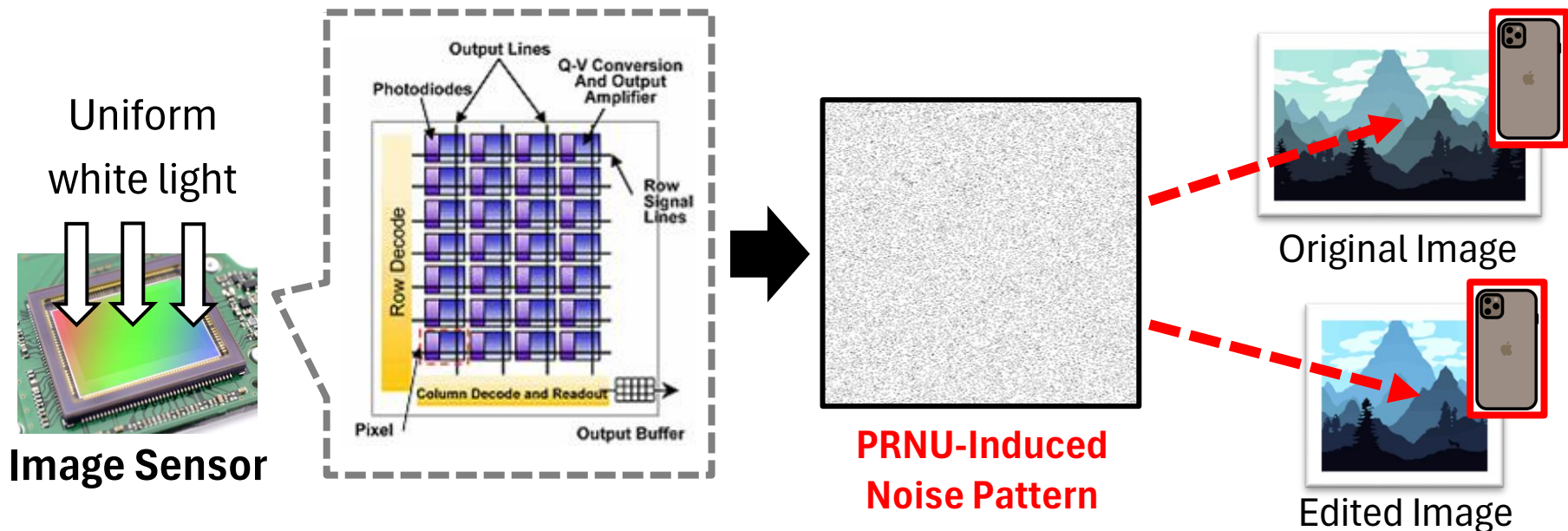
# PRNU: the most distinctive hardware trace

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



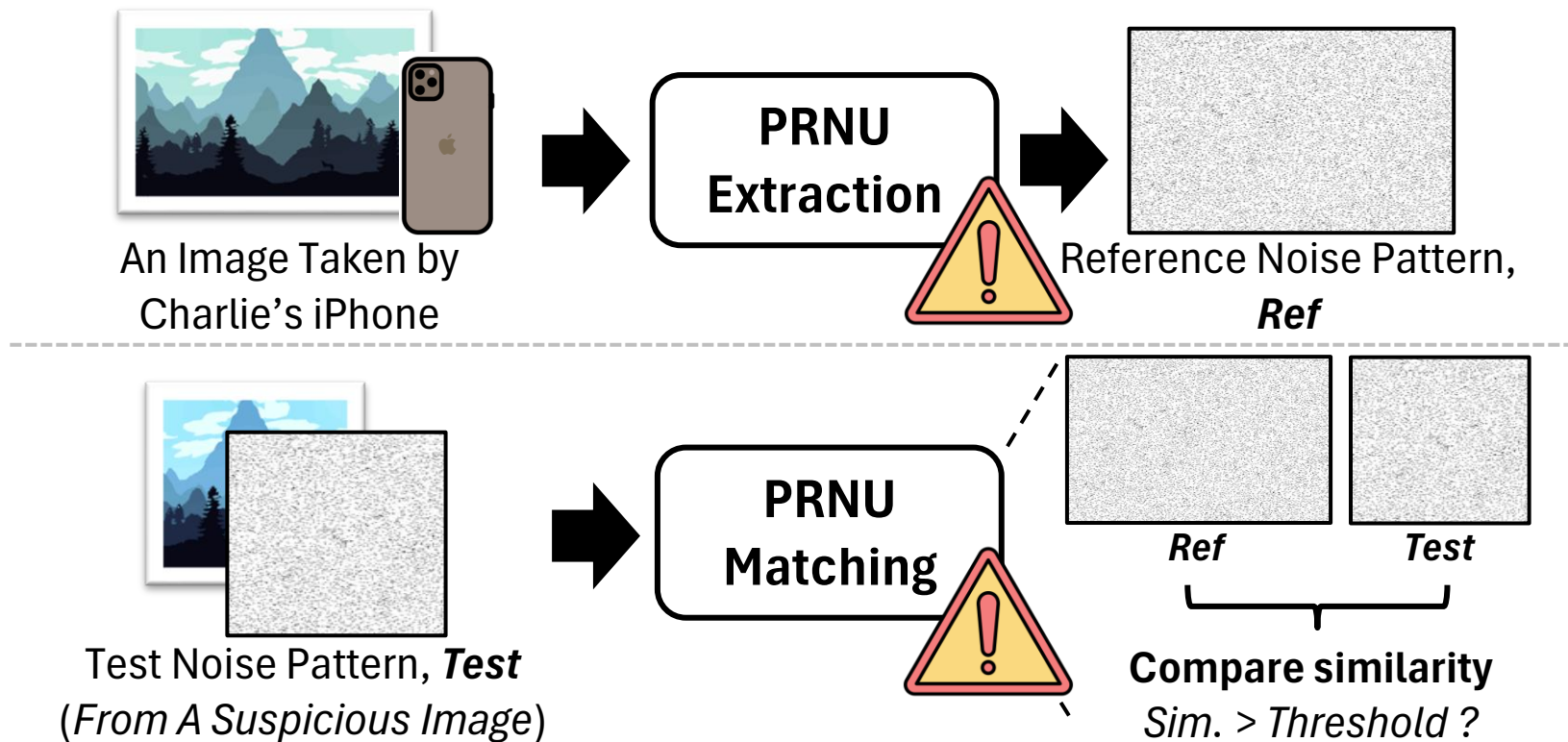
# PRNU: the most distinctive hardware trace

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



# Related work: general pipeline of using PRNU

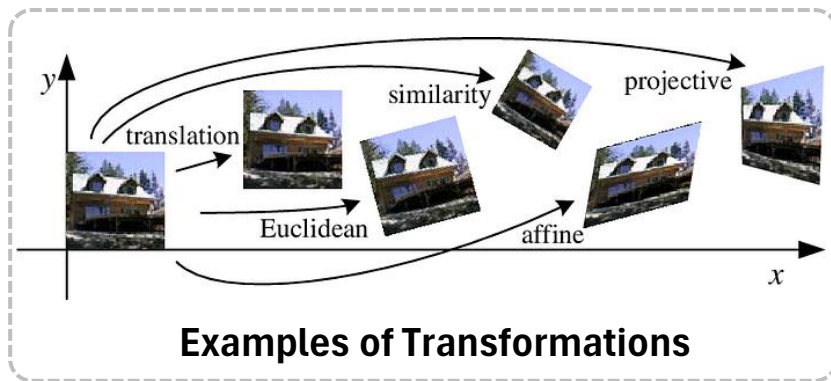
- Related work focuses on **extracting** and **matching** noise patterns



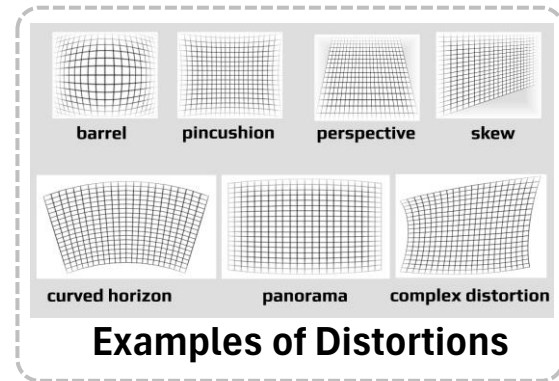
# Related work: limitations

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

PRNU  
Matching



Examples of Transformations



Examples of Distortions

*Transformation functions*

$f_1$

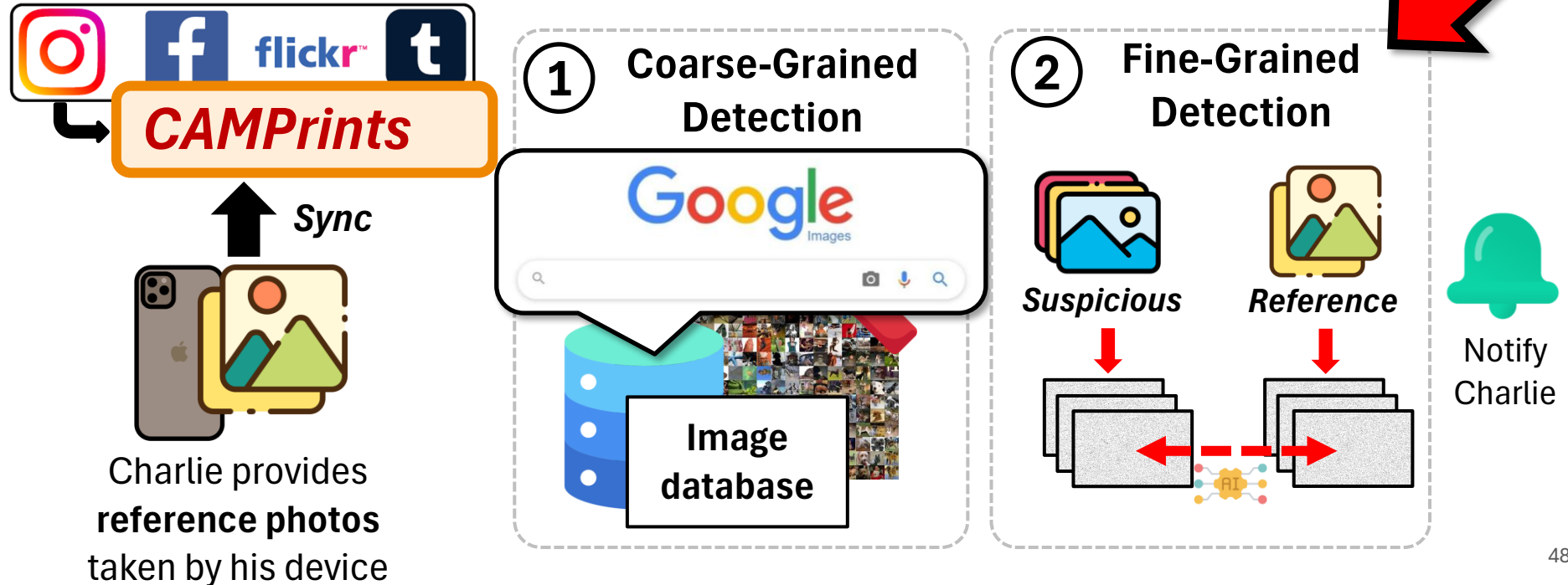
...

$f_n$

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

# Our work: *CAMPrints*

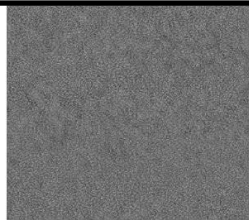
- Detect online image theft using camera “fingerprints” (i.e., PRNU-induced noise pattern) as physical proof of ownership



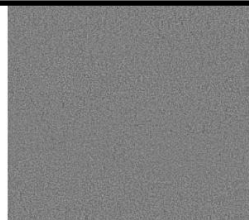
# Challenge #1: noise patterns do not match directly

- Direct matching of noise pattern often fails

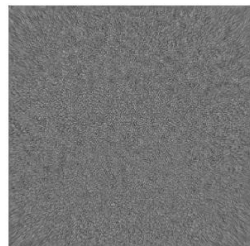
Examples of noise patterns



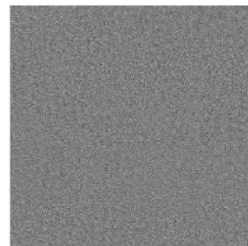
**Ref**  
(original)



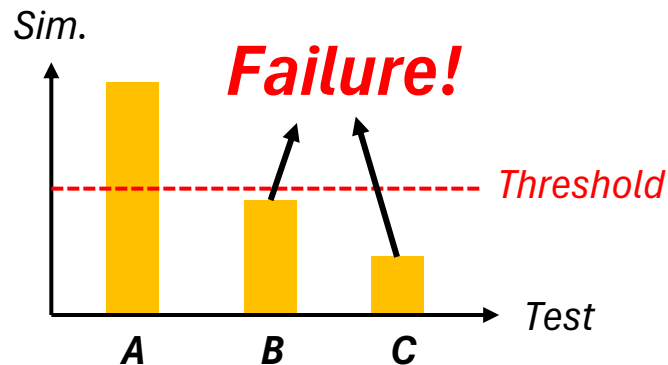
**Test A**  
( $f_1$ : color effects)



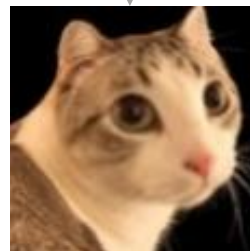
**Test B**  
( $f_2$ : distortion)



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



For illustration purpose



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

# Core idea #1: representation learning

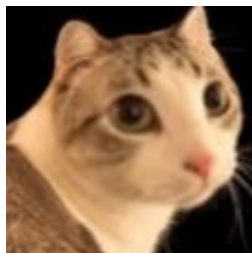
- A noise pattern should be **recognizable** even after transformations



**Ref**  
(original)



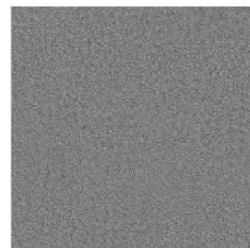
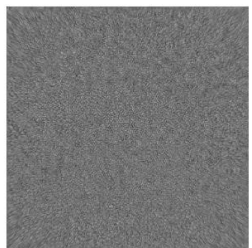
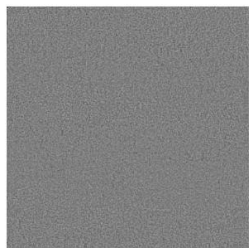
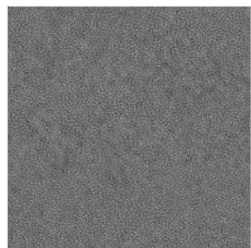
**Test A**  
( $f_1$ : color effects)



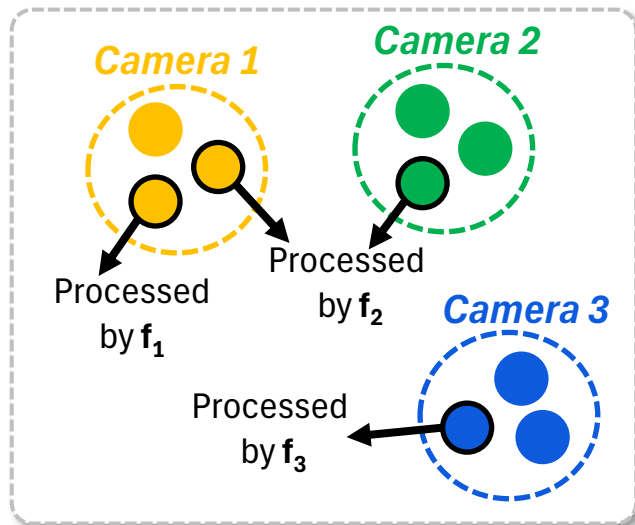
**Test B**  
( $f_2$ : distortion)



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



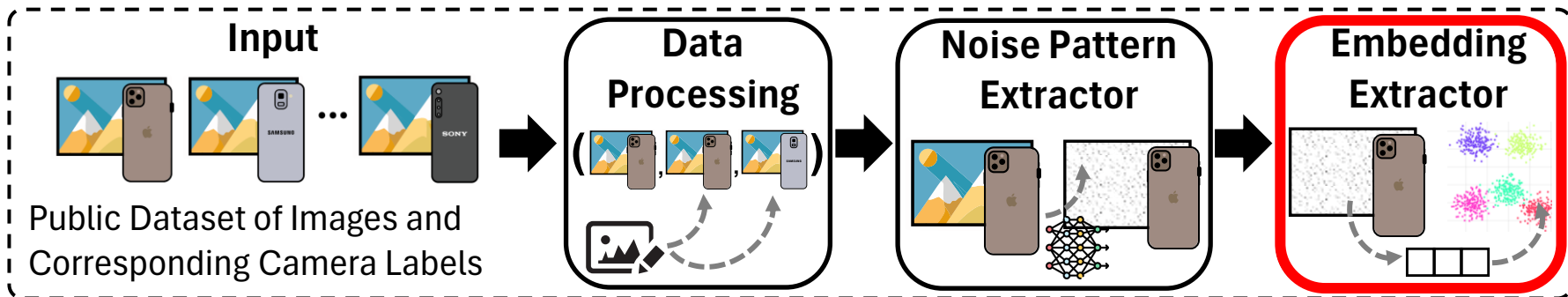
**Representation Learning**  
form tight clusters regardless of  
transformations ( $f_n$ )



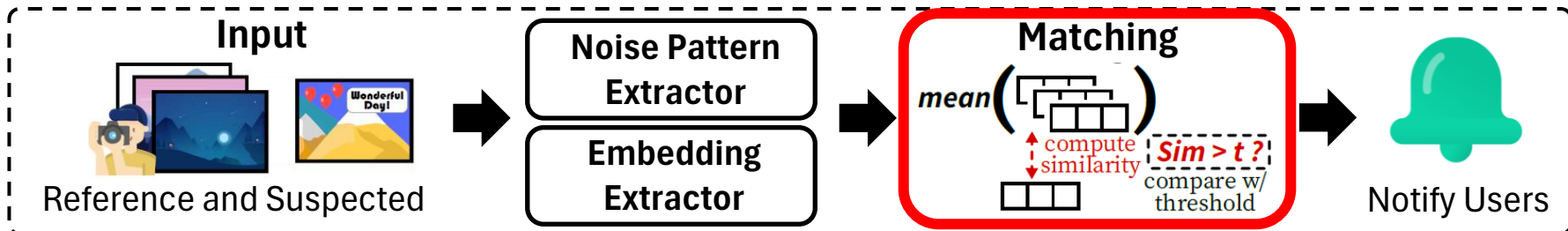
# Design of CAMPrints

- Instead of matching noise patterns, we match the embeddings of them

## Training Phase



## Verification Phase

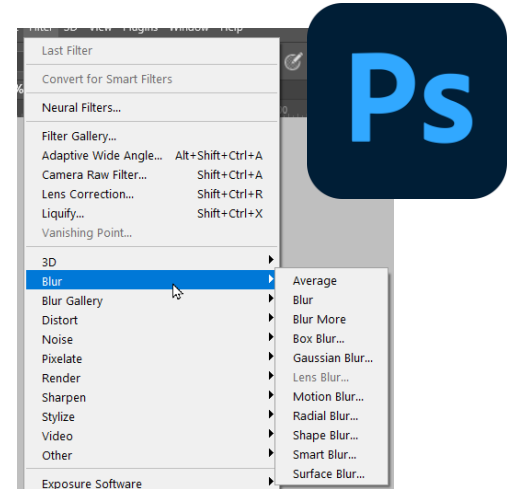


# Challenge #2: image editing operations

- **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

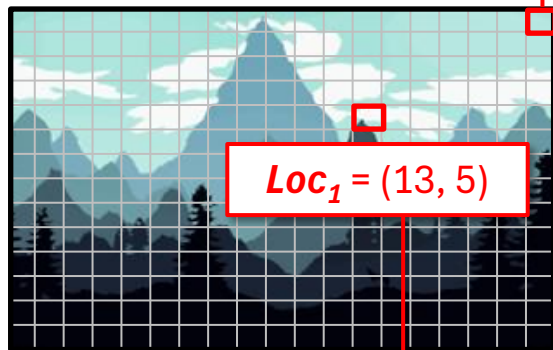


Examples of image editing operations on Photoshop

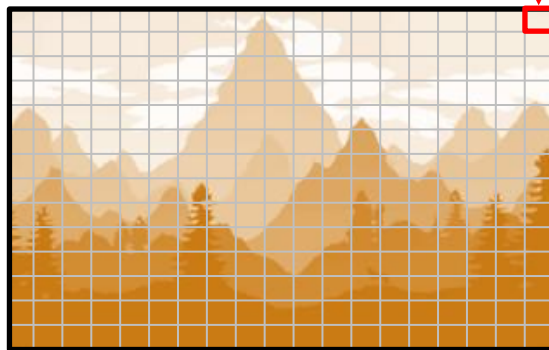
## Core idea #2: representative image editing

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

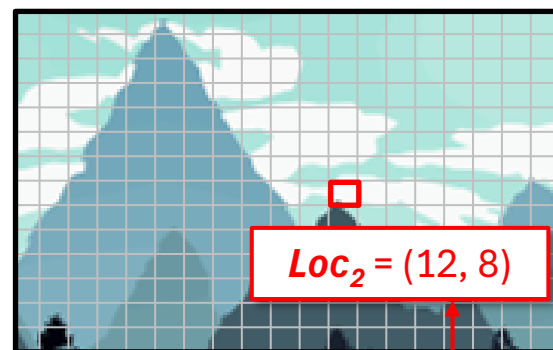
*Effect (1) Pixel value changes* from  $Color_1$  to  $Color_2$



$Loc_1 = (13, 5)$



Color Effects

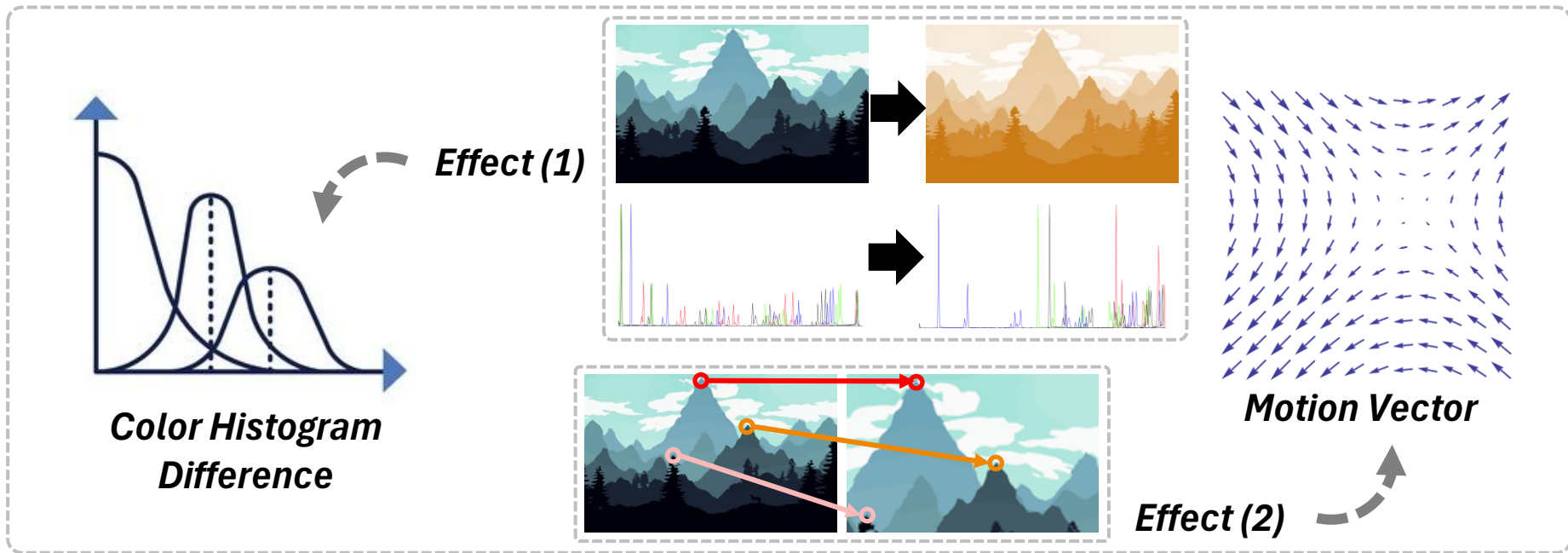


$Loc_2 = (12, 8)$

*Effect (2) Pixel location shifts* from  $Loc_1$  to  $Loc_2$

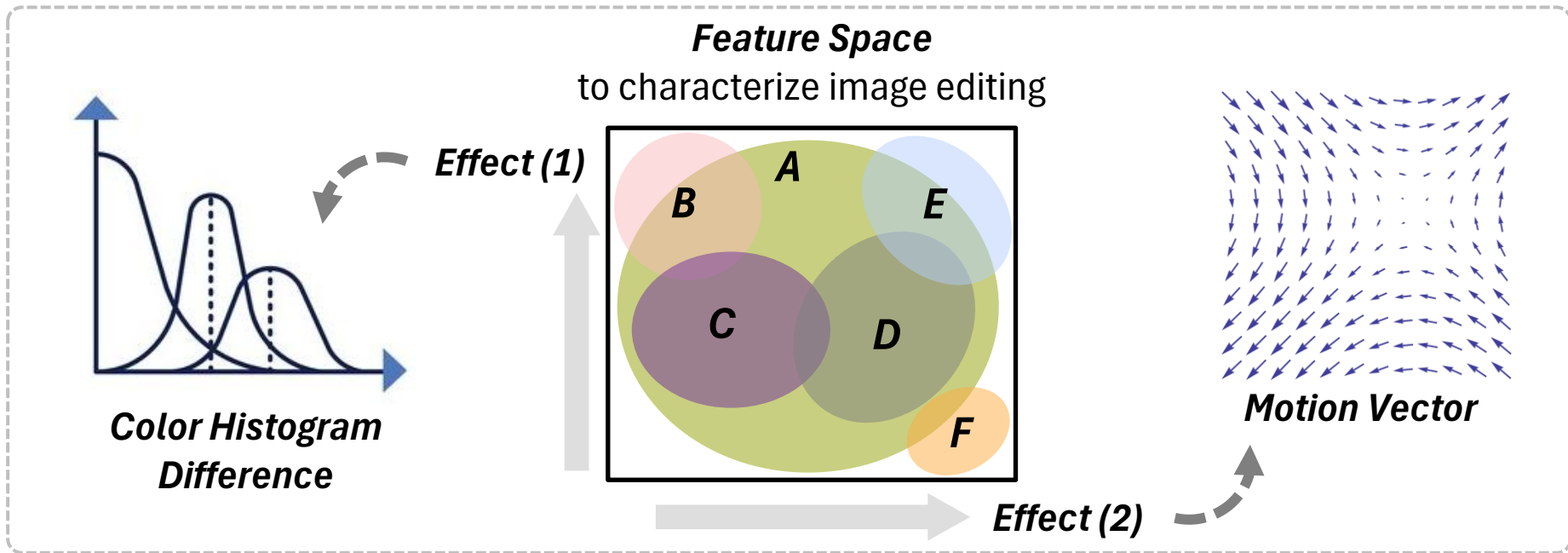
# Core idea #2: representative image editing

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



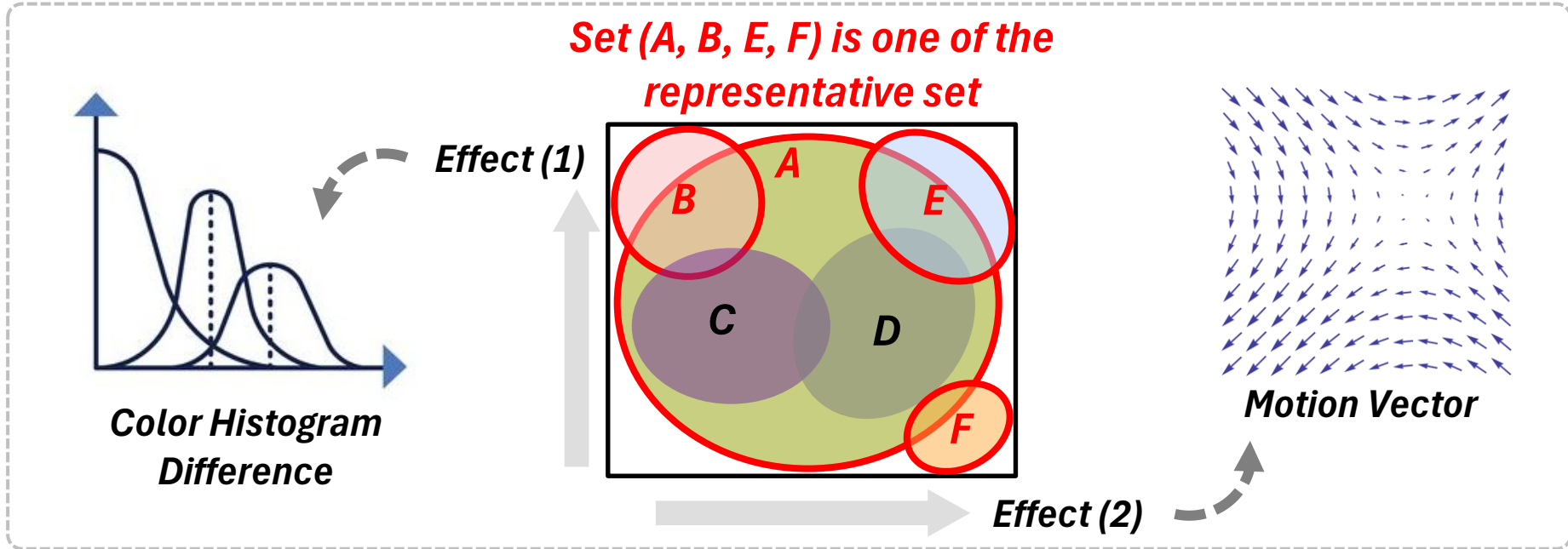
## Core idea #2: representative image editing

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



## Core idea #2: representative image editing

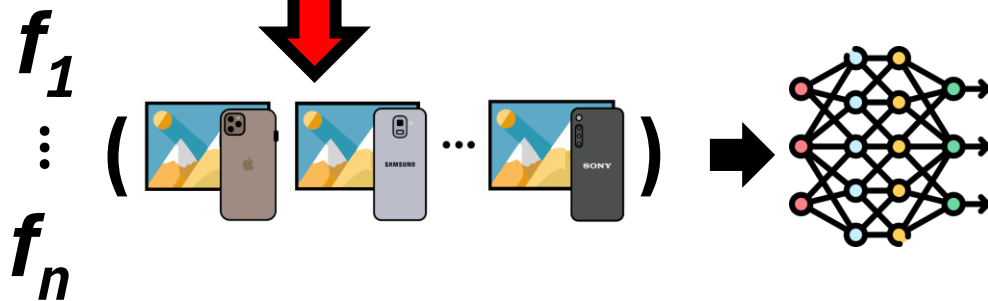
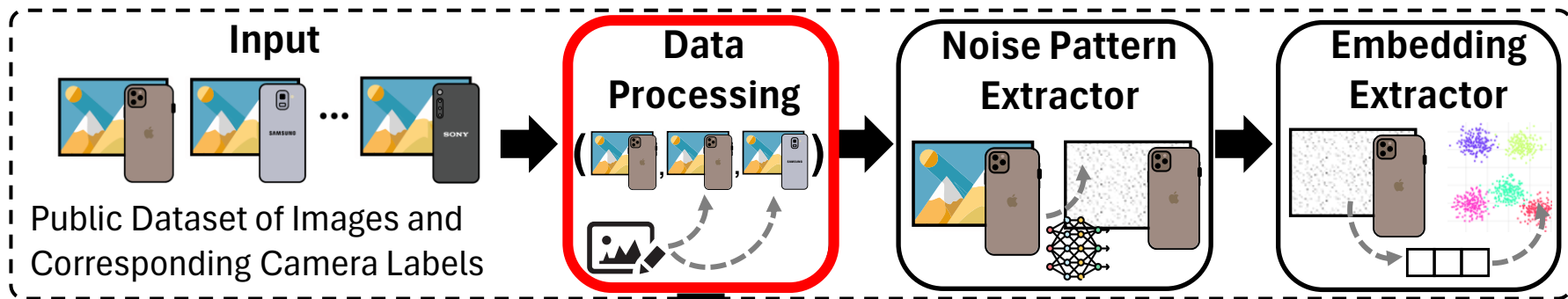
- Select largest spanning circle as the representative operation
- Continue selecting to fill up the uncovered regions



# Design of *CAMPrints*

- Instead of 40+ image editing operations, we use **only 4 representative** ones

## Training Phase

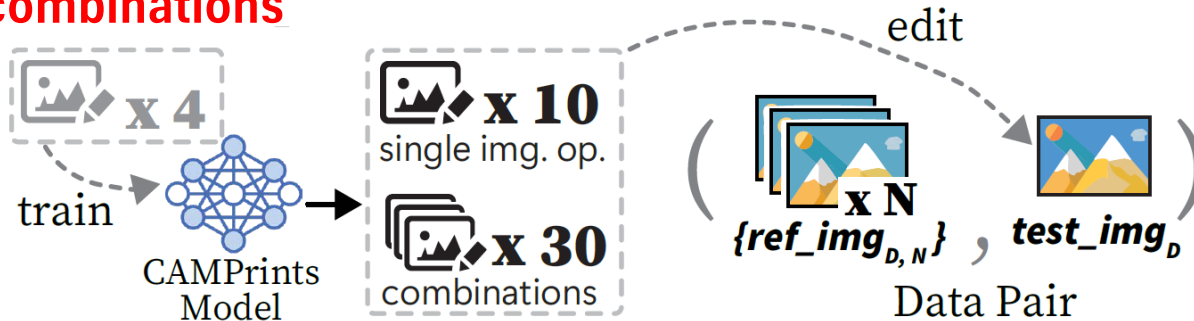


# Experiment setup

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



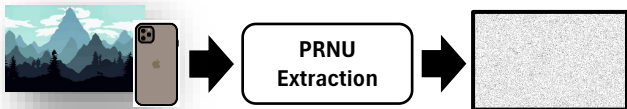
- We train the model with **only four** operations and test on **40 other operations and combinations**



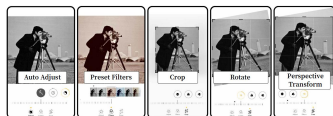
# Summary of evaluation results

- Demonstrates **overall average ROC-AUC of 0.92**, outperform baseline methods by **1.8x**

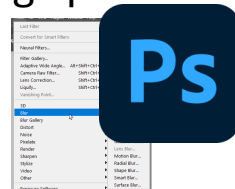
- Remains **compatible** to existing PRNU extraction methods



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



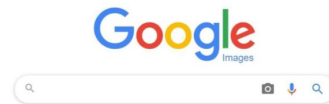
- Generalizes to **unseen** image processing operations



- Generalizes across **commercial software**

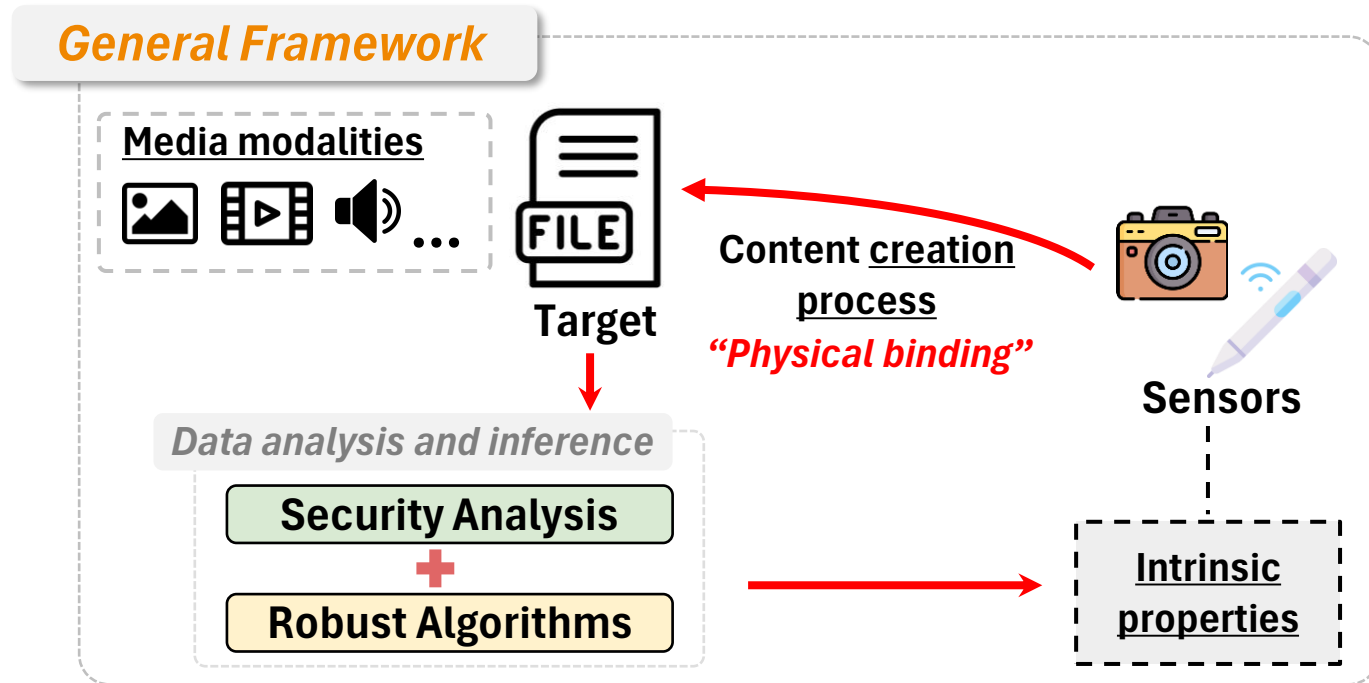


- Yields **80% less false positives** compared to Reverse Image Search



# Methodological Generalization

- Physical bindings to content creation process
- Security analysis and robust algorithms for usable defences

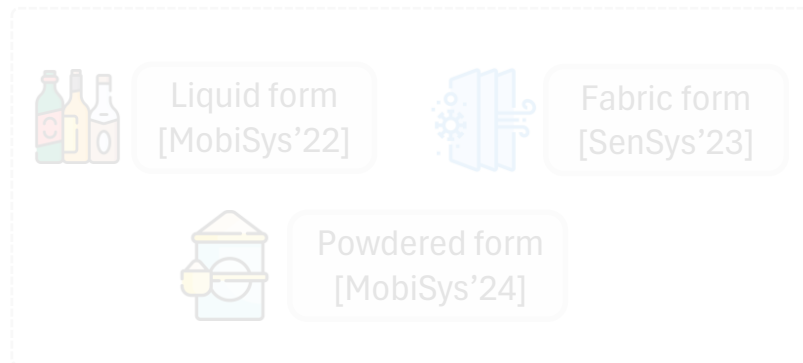


# Research landscape

## Physical Domain

e.g., liquids & medicines

Tackle counterfeit, substandard physical products using commodity cameras only



*Note: different physical forms require distinct scientific insights and technological innovations*

## Digital Domain

e.g., images & videos

Tackle stolen or fake digital content using capture or creation process

*For stolen content:*



Photography  
[MobiSys'25]



Digital Art  
(Ongoing...)

Robust Image Retrieval  
[ArtSec'26 co-located with Oakland'26]

*For fake content:*



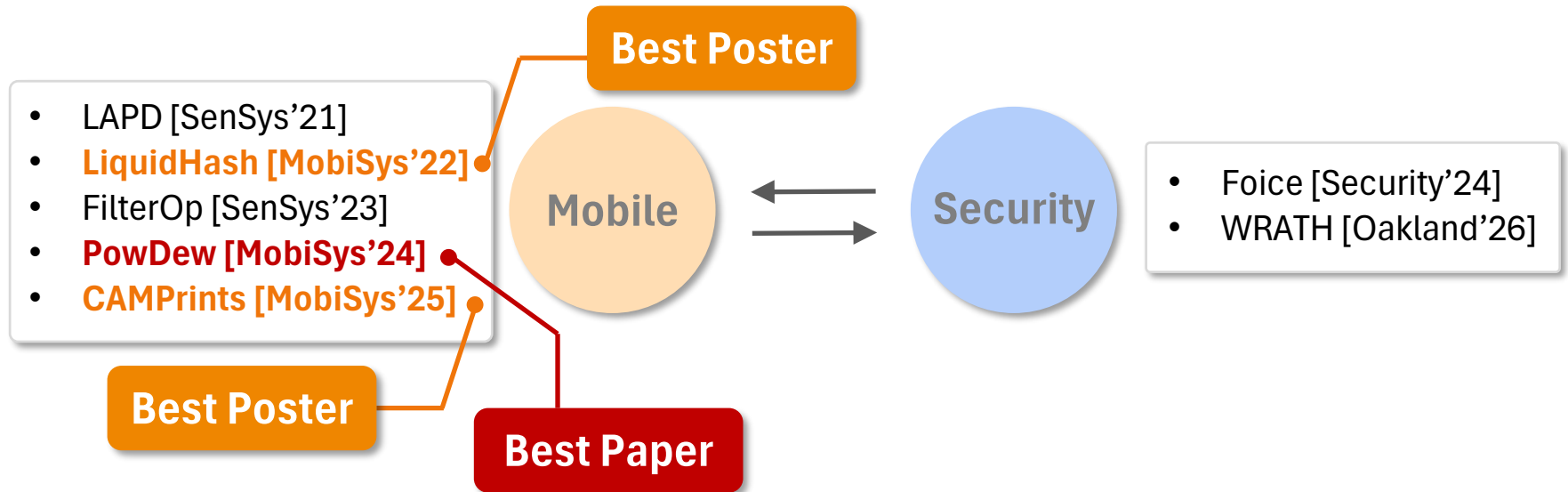
Fake Image  
[Oakland'26]



Fake Audio  
[Security'24]

# My journey so far

- Publish in top-tier mobile and security conferences
- Multiple awards from the mobile community for recognizing our contribution in building ubiquitous intrinsic provenance systems



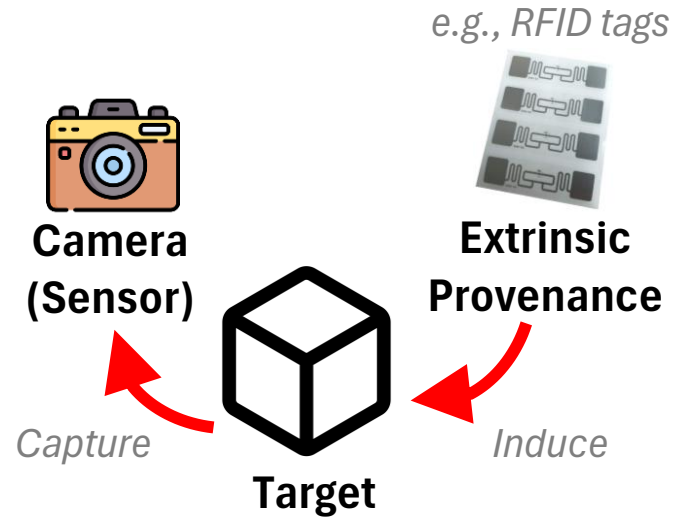
# Future research

- Direction #1: improve **usability** of provenance systems

*Example:*



*Insight: co-design of packaging (hardware) and extraction of intrinsic properties of physical content (software)*

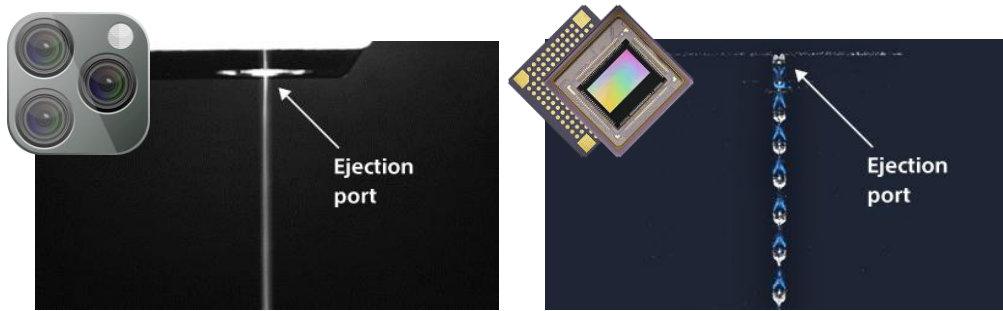


**Build widely usable provenance systems.**

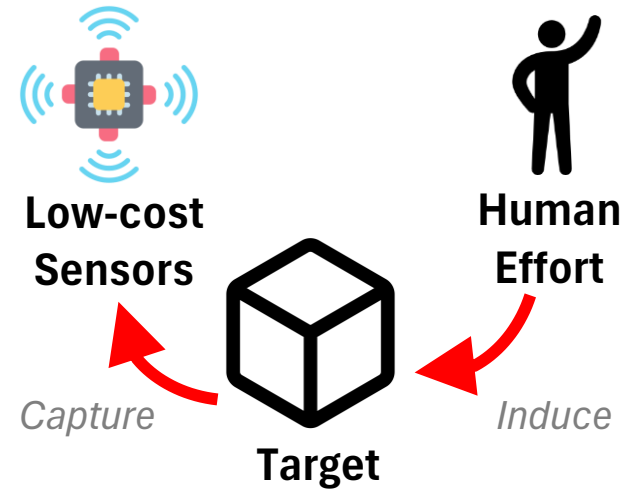
# Future research

- Direction #1: improve **usability** of provenance systems

*Example:*



*Insight: low-cost, high-resolution, high-speed sensors (e.g., event cameras) could reduce human effort*

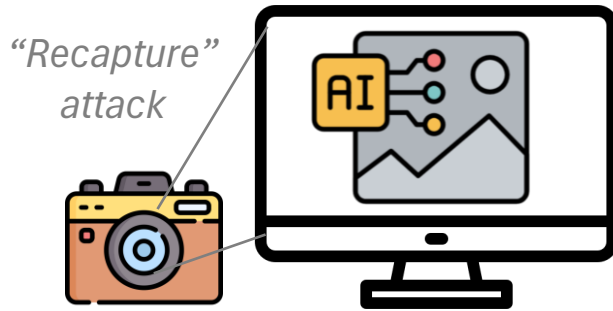


**Build widely usable provenance systems.**

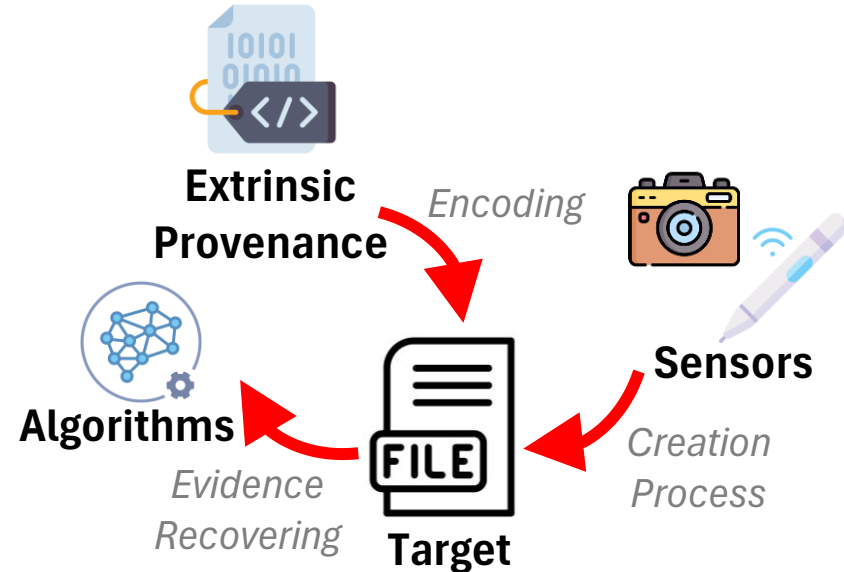
# Future research

- Direction #2: improve **robustness** of provenance systems

*Example:*



*Insight: robust against a wide range of attacks (e.g., physical attacks, adaptive attacks, generative attacks)*

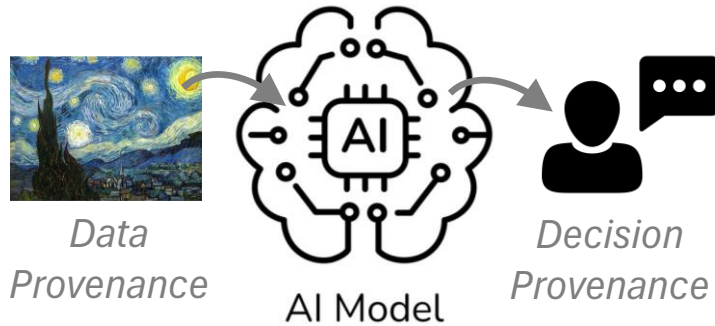


**Build widely usable provenance systems.**

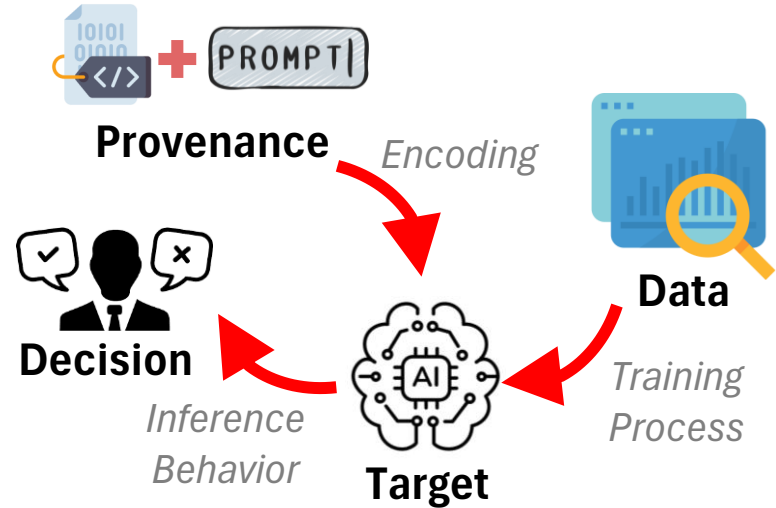
# Future research

- Direction #3: improve **coverage** of provenance systems

*Example:*

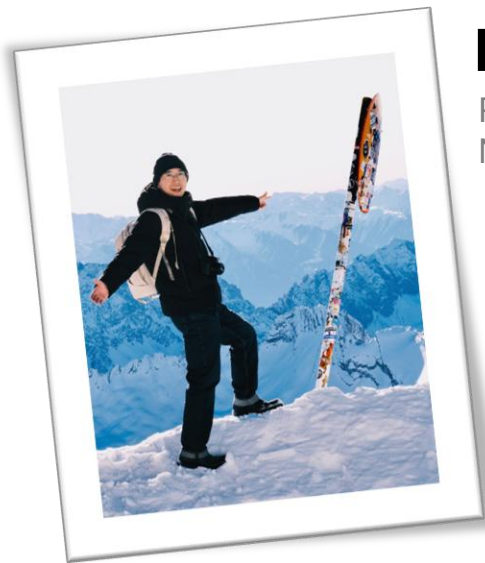


*Insight: increasing use of AI models in daily lives requires broader coverage of provenance systems*



**Build widely usable provenance systems.**

# 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**