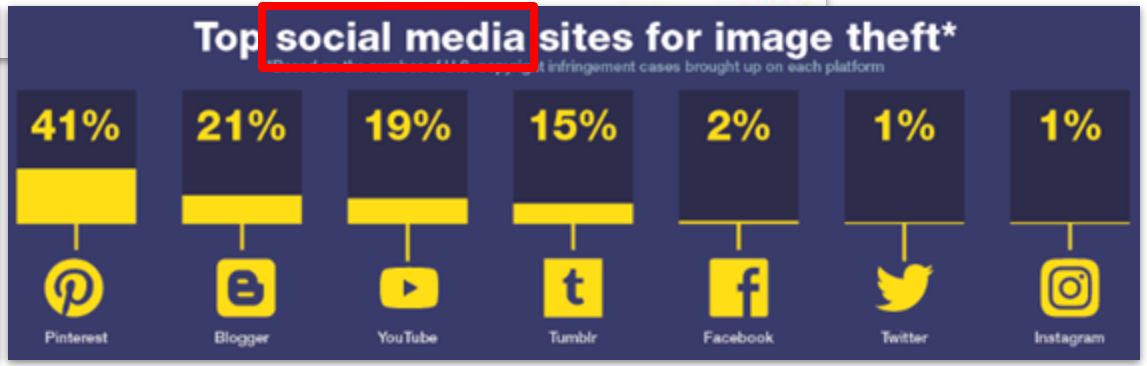
CAMPrints: Leveraging the "Fingerprints" of Digital Cameras to Combat Image Theft

Bangjie Sun, Mun Choon Chan, and Jun Han*

National University of Singapore *KAIST

A Surge in Online Image Theft

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



Scenario: Combat Image Theft

Shared

Charlie's iPhone Photo Album

Charlie

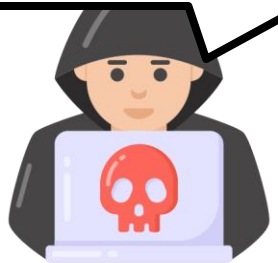
Mallory

Post on Mallory's social media

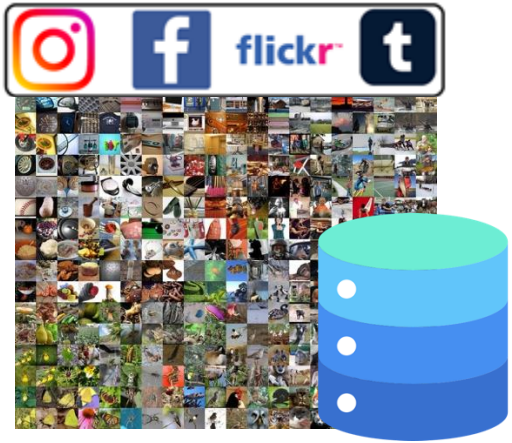
Ps

Image Editing

Steal images after **image editing**



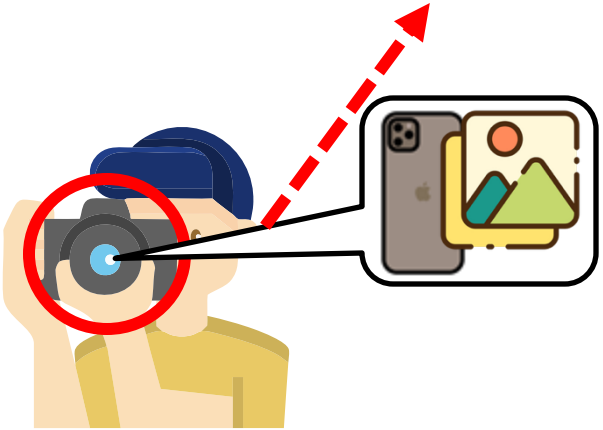
Scenario: Combat Image Theft



Search from image database

"Physical Token"

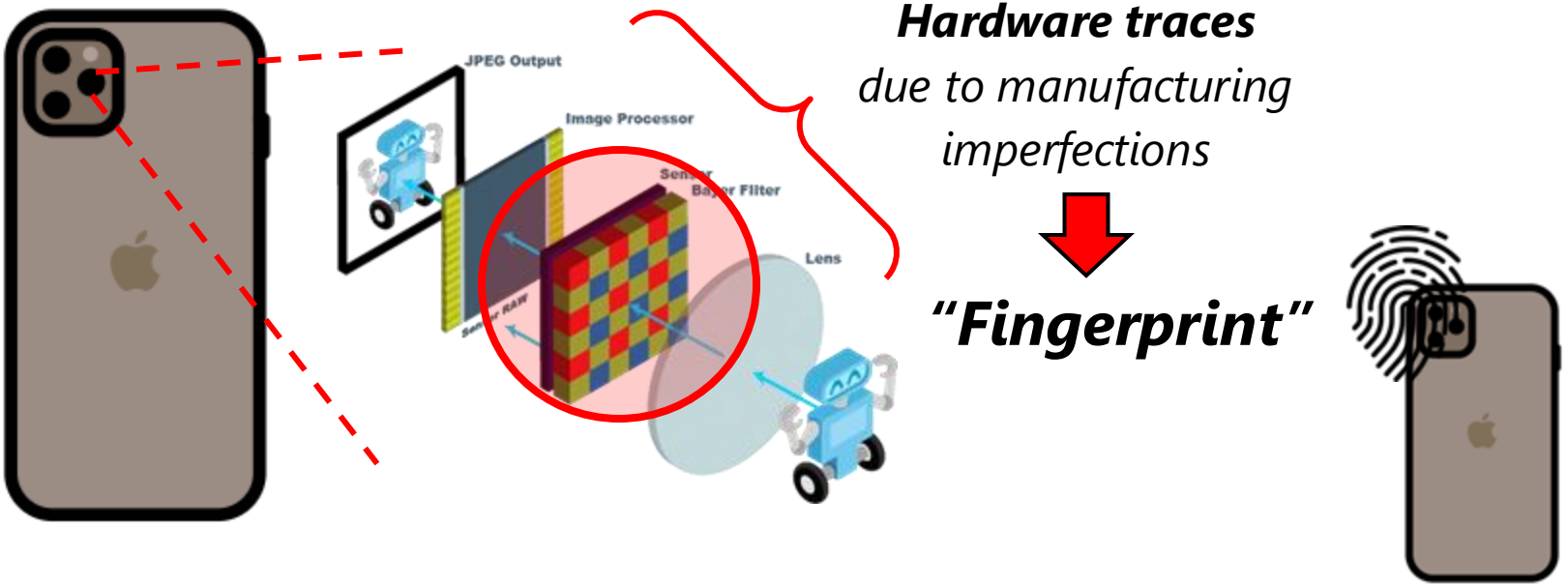
Physical Proof of Ownership



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



PRNU: The Most Distinctive Hardware Trace

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

Uniform white light

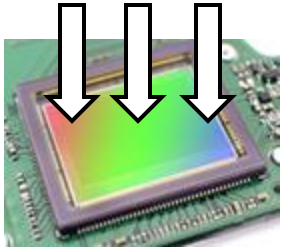
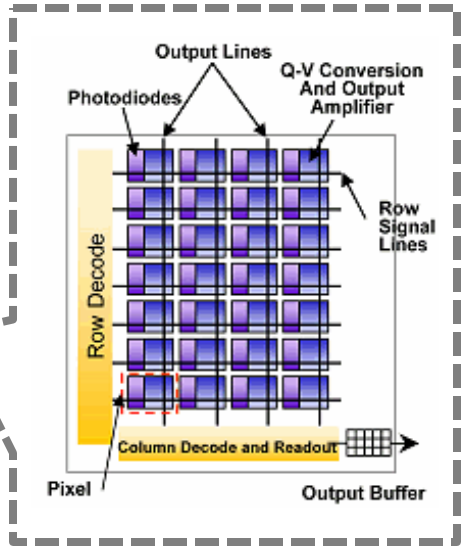
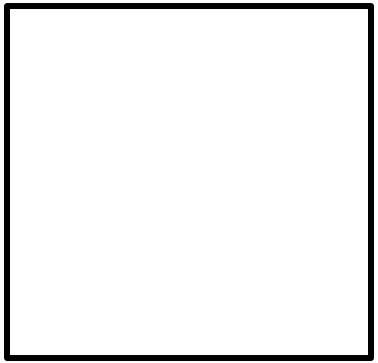


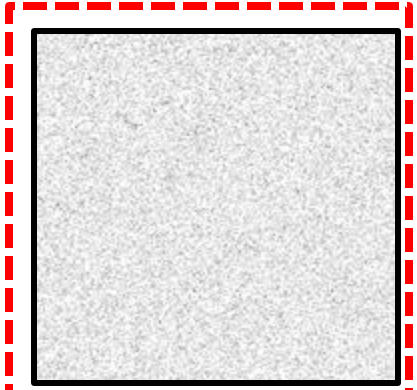
Image Sensor





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

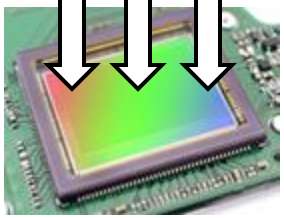
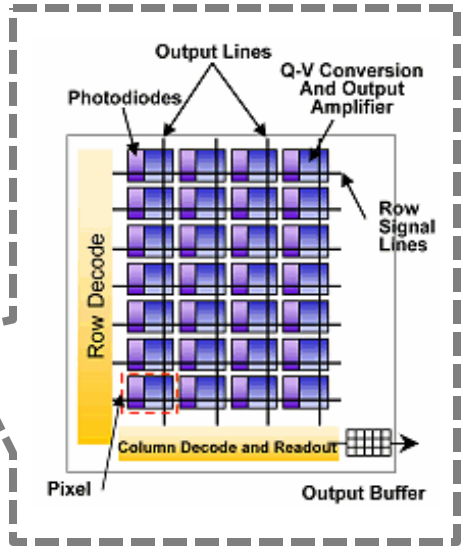


Image Sensor



PRNU-Induced Noise Pattern

Original Image

Edited Image

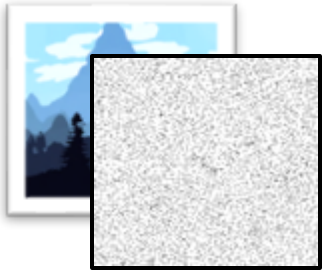
Related Work: General Pipeline of Using PRNU

- 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

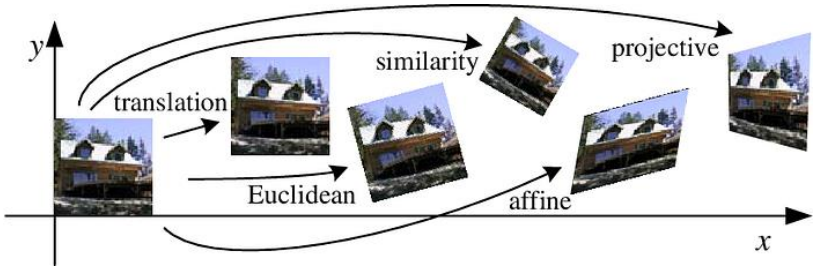
Compare similarity

Sim. > Threshold ?

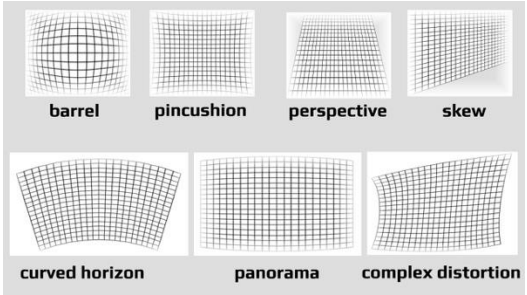
Related Work: Limitations

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

PRNU Matching



Examples of Transformations

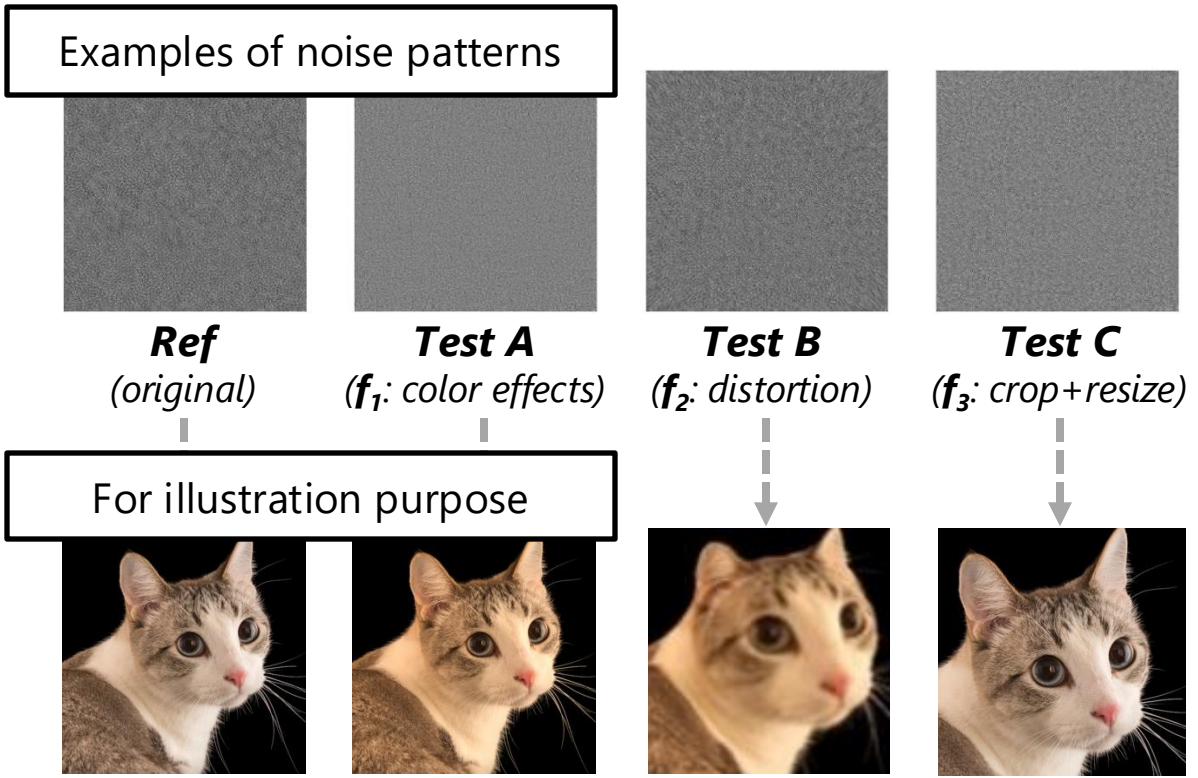


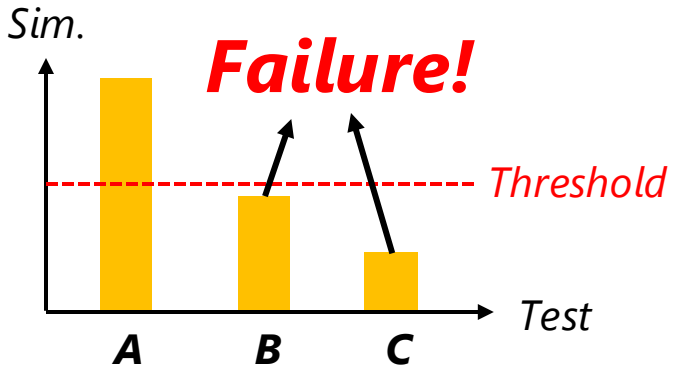
Examples of Distortions

Transformation functions $f_1 \quad \dots \quad f_n$

Related Work: Limitations

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





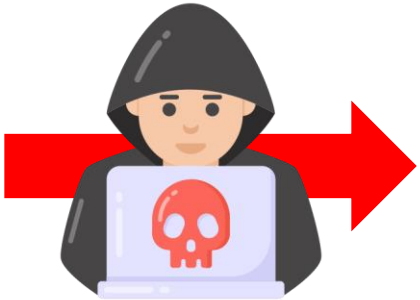
We need a robust solution when Ref and Test are not spatially aligned

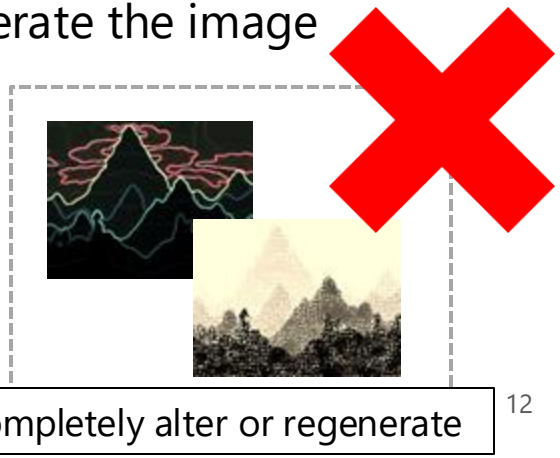
Can we detect image theft even when attackers could freely edit images?

Threat Model

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

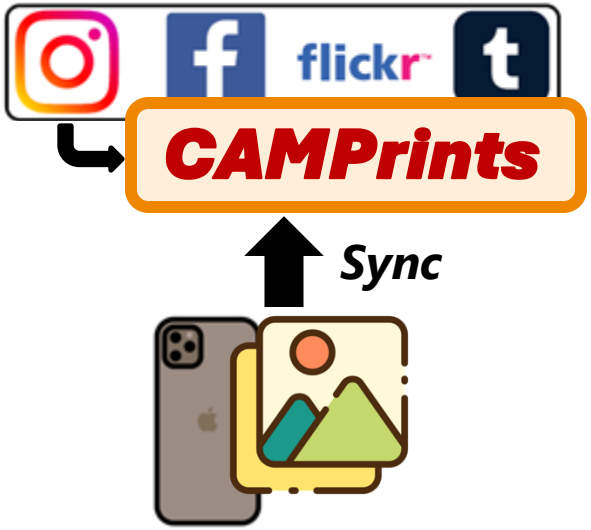
- **Attacker's capabilities:**
  - Use image editing software and test against detection methods
  - No transformations that completely alter or regenerate the image



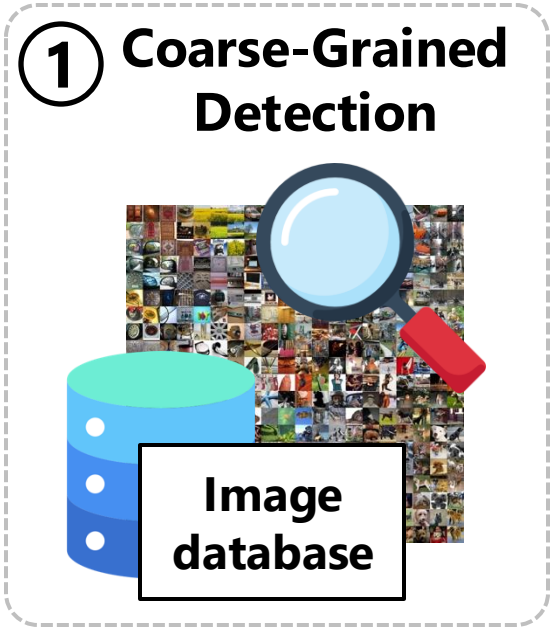


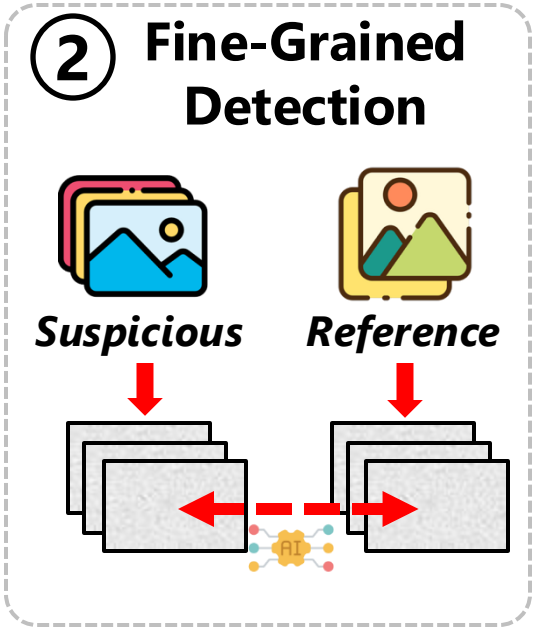
Our Work: *CAMPrints*

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



Charlie provides **reference photos** taken by his device

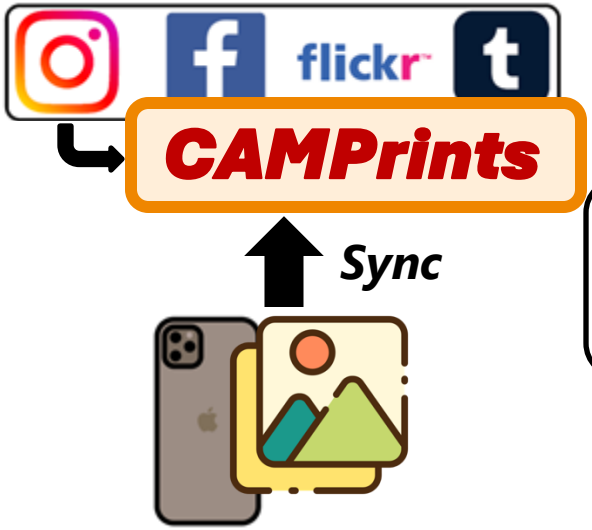




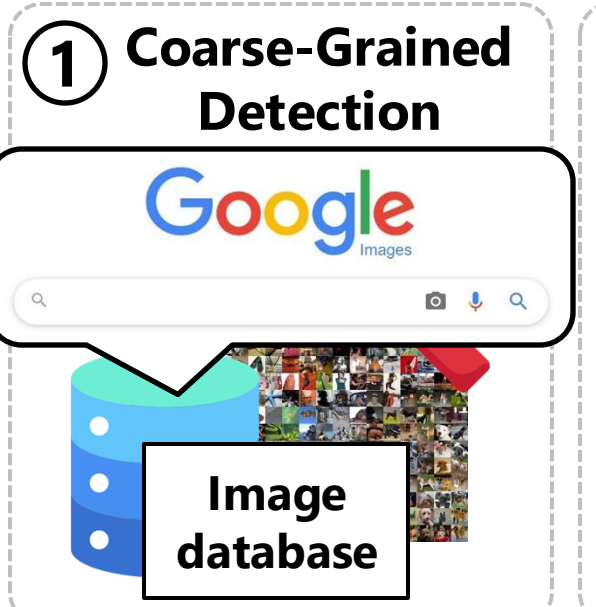
Notify Charlie

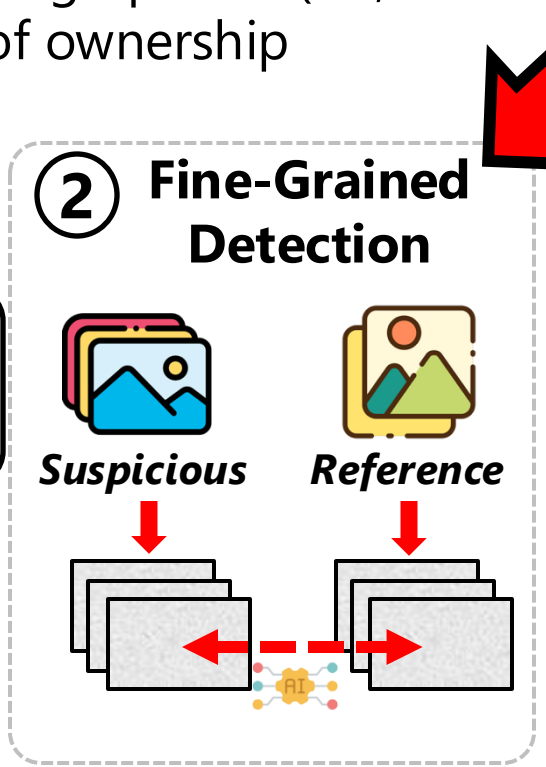
Our Work: *CAMPrints*

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



Charlie provides **reference photos** taken by his device

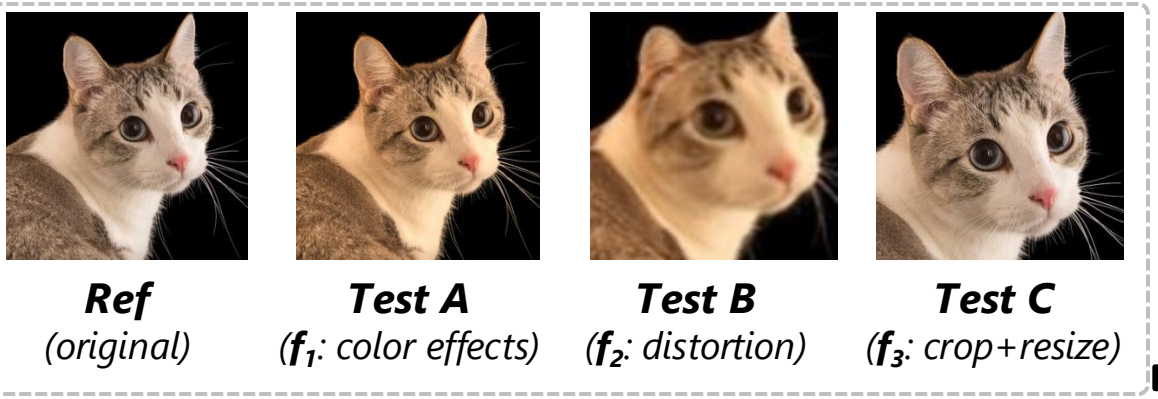




Notify Charlie

Core Idea of *CAMPrints*

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

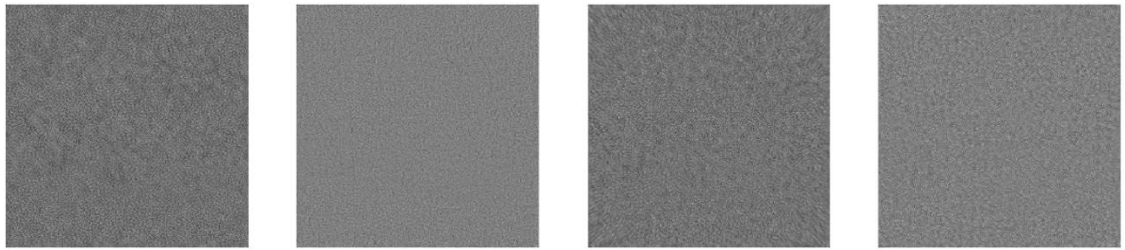


Ref *(original)*

Test A *(**f**$_1$: color effects)*

Test B *(**f**$_2$: distortion)*

Test C *(**f**$_3$: crop+resize)*



Core Idea of *CAMPrints*

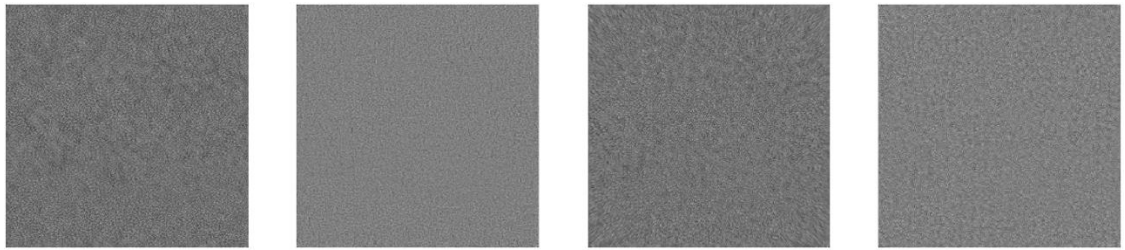
- A noise pattern should be **recognizable** even after transformations

Ref *(original)*

Test A *(f_1: color effects)*

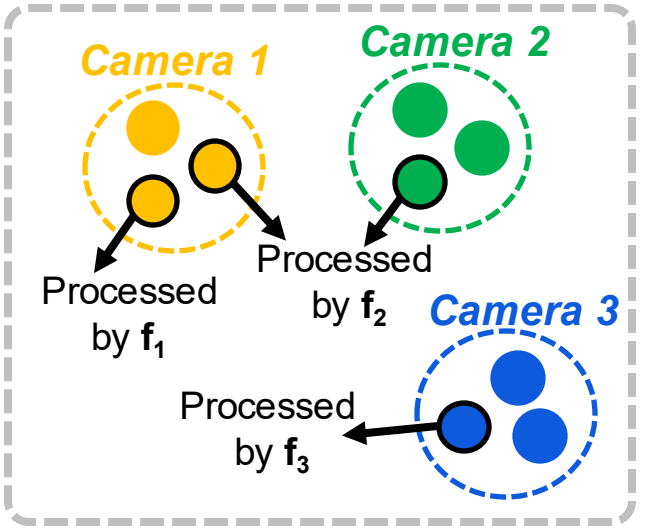
Test B *(f_2: distortion)*

Test C *(f_3: crop+resize)*



Representation Learning

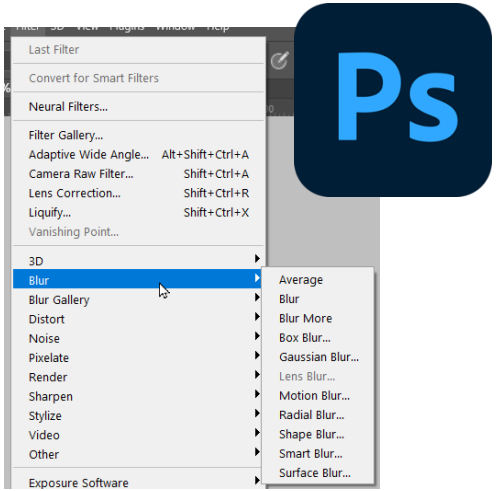
form tight clusters regardless of transformations (f_n)



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**

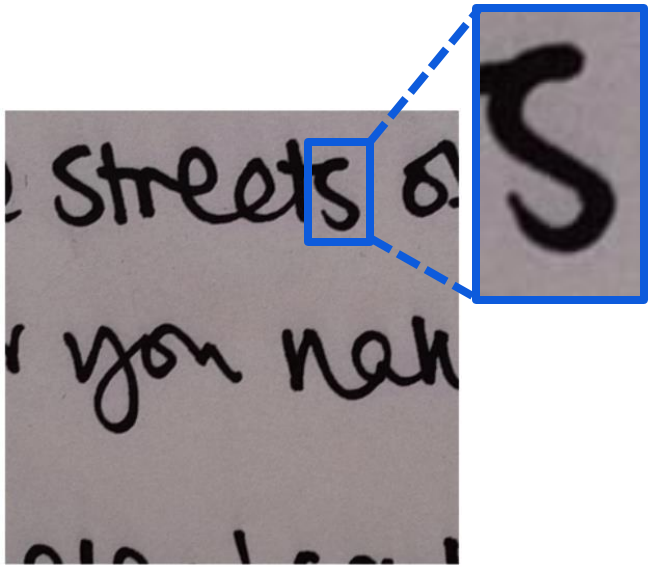
Examples of image editing operations on iOS



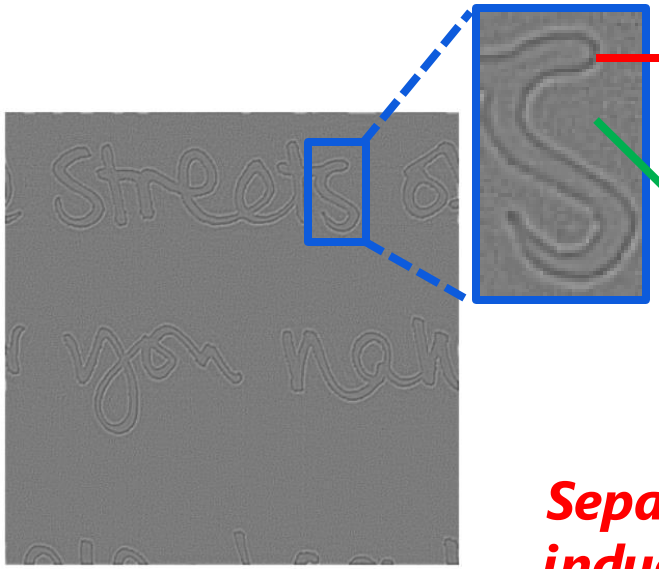
Examples of image editing operations on Photoshop

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)

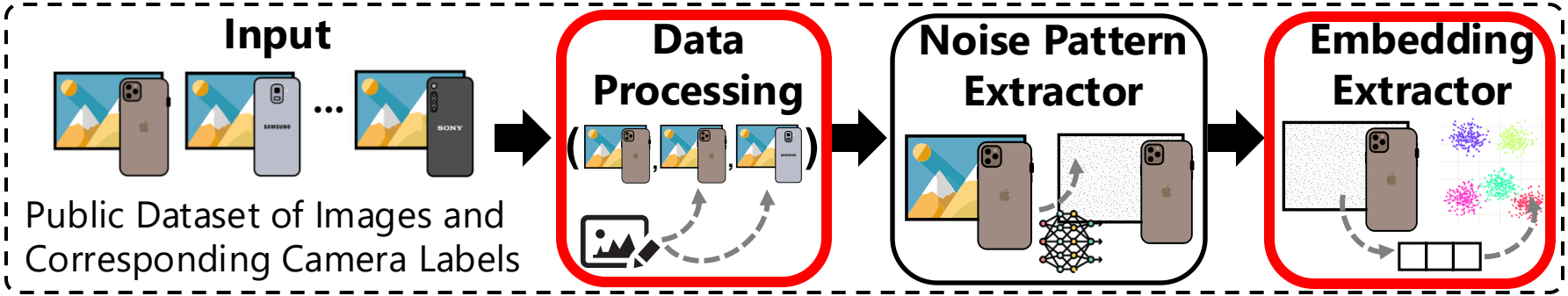
Separate content-induced noise and sensor noise

Design of *CAMPrints*

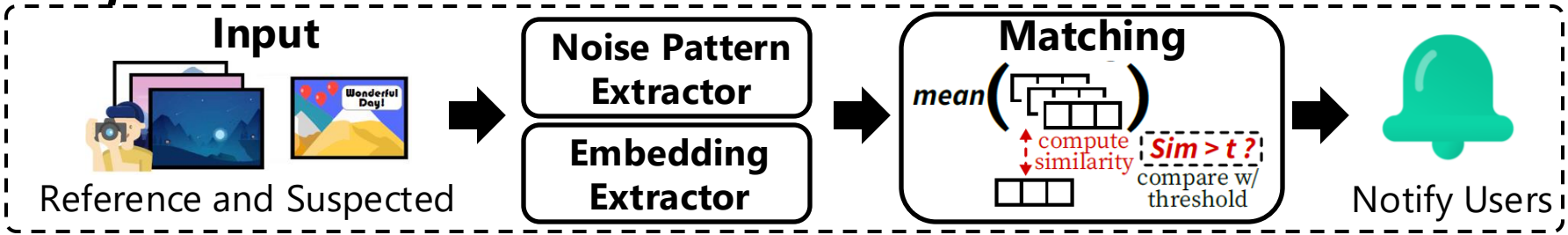
For Challenge #1
Image Editing Operations

For Challenge #2
Multiple Sources of Noises

Training Phase



Verification Phase

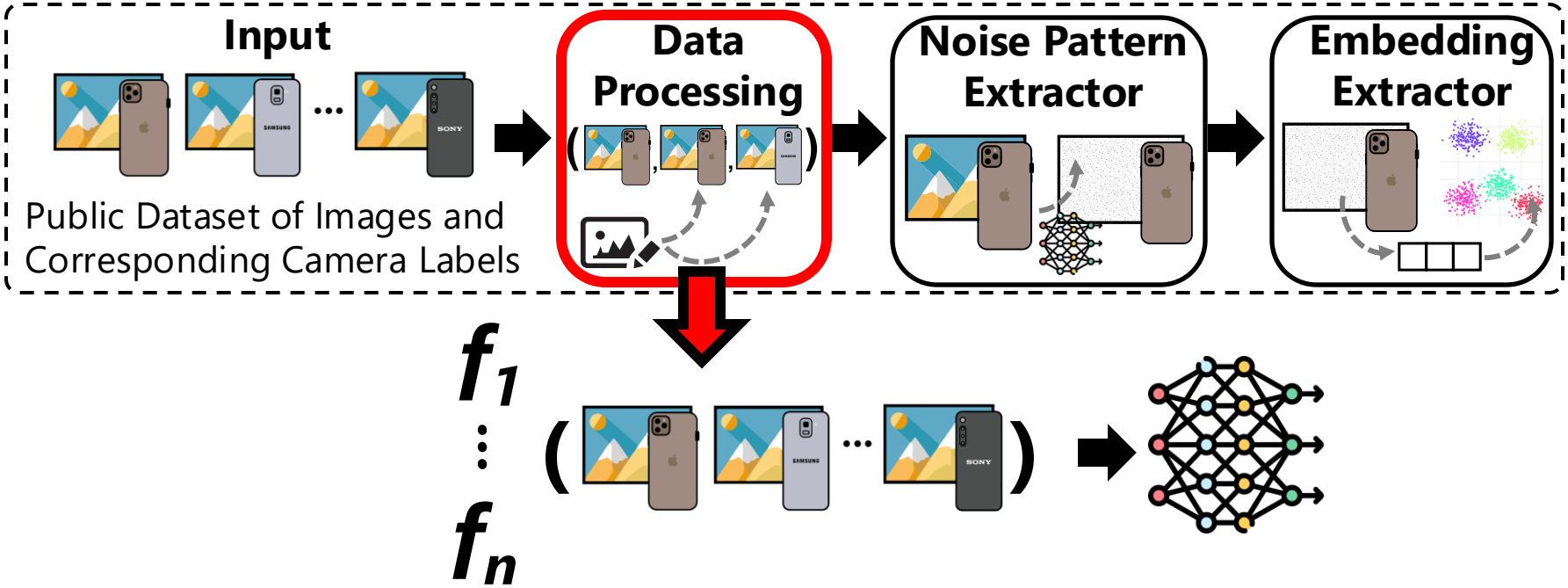


Design of *CAMPrints*

For Challenge #1

Training Phase

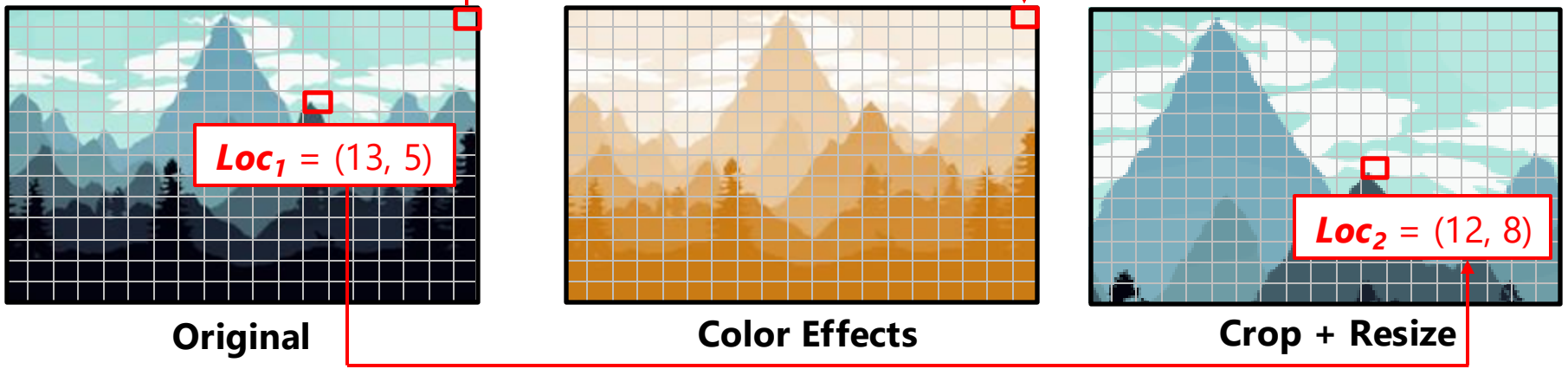
Image Editing Operations



Data Processing: Representative Image Editing

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

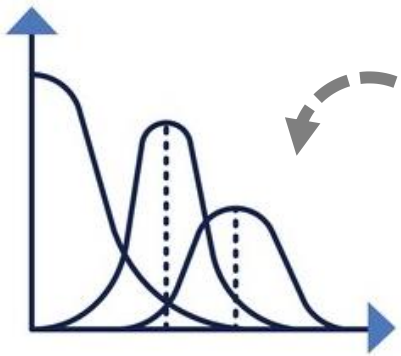
Effect (1) Pixel value changes from ***$Color_1$*** to ***$Color_2$***



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

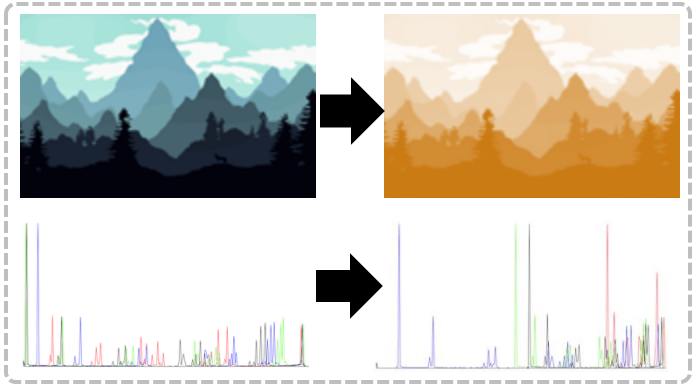
Data Processing: Representative Image Editing

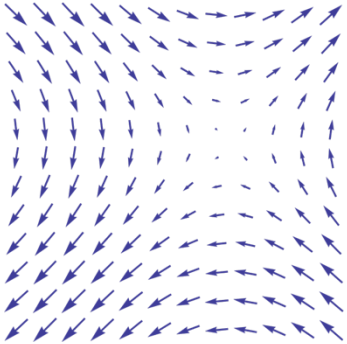
- Quantify pixel value changes using histograms
- Quantify pixel location shifts using motion vectors



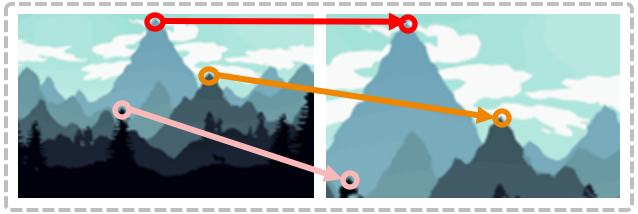
Color Histogram Difference

Effect (1)





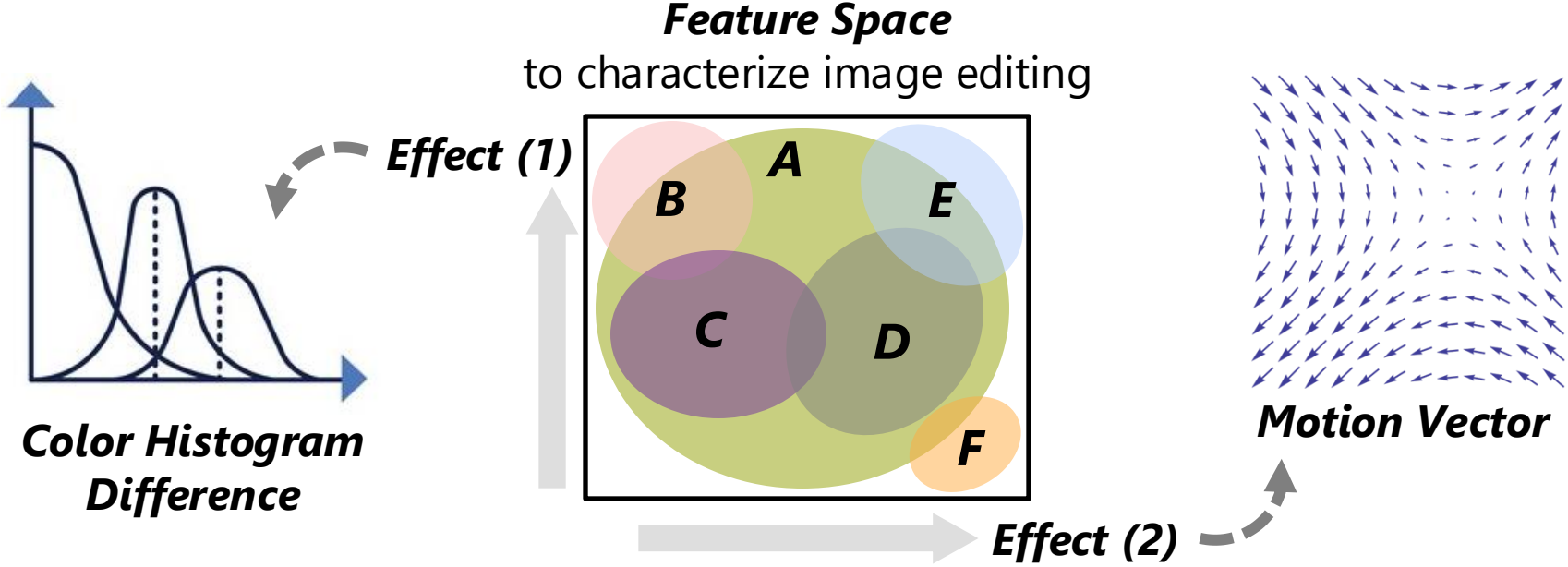
Motion Vector



Effect (2)

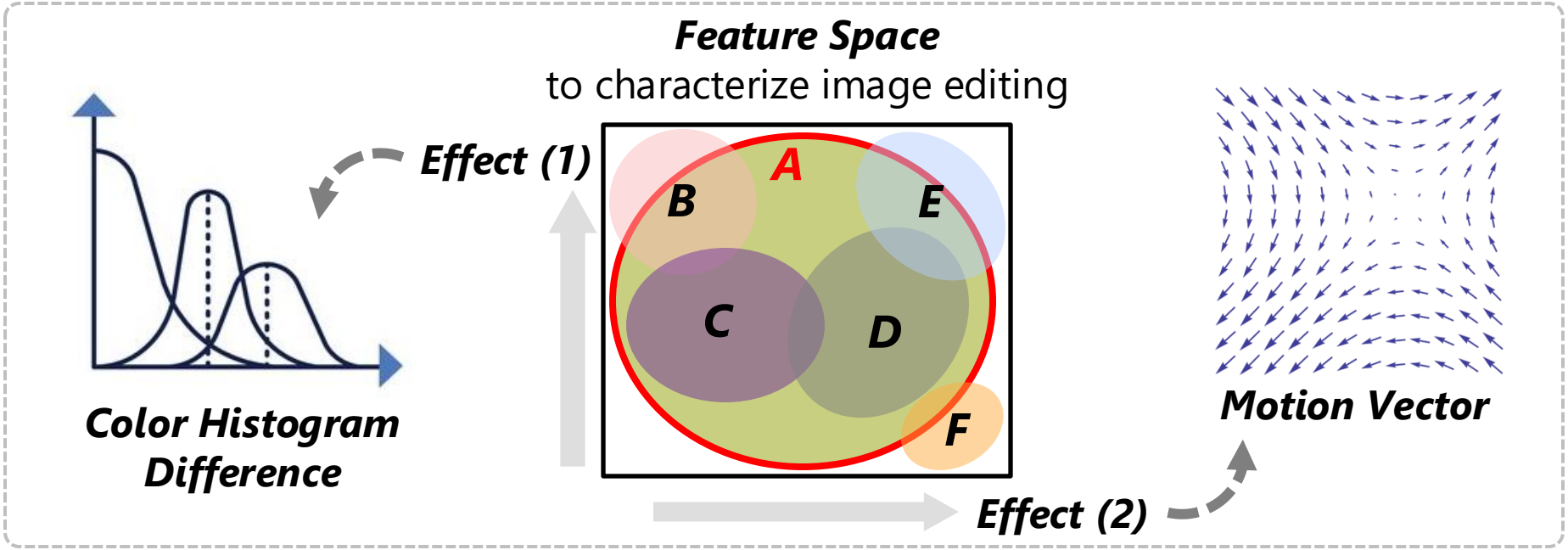
Data Processing: Representative Image Editing

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



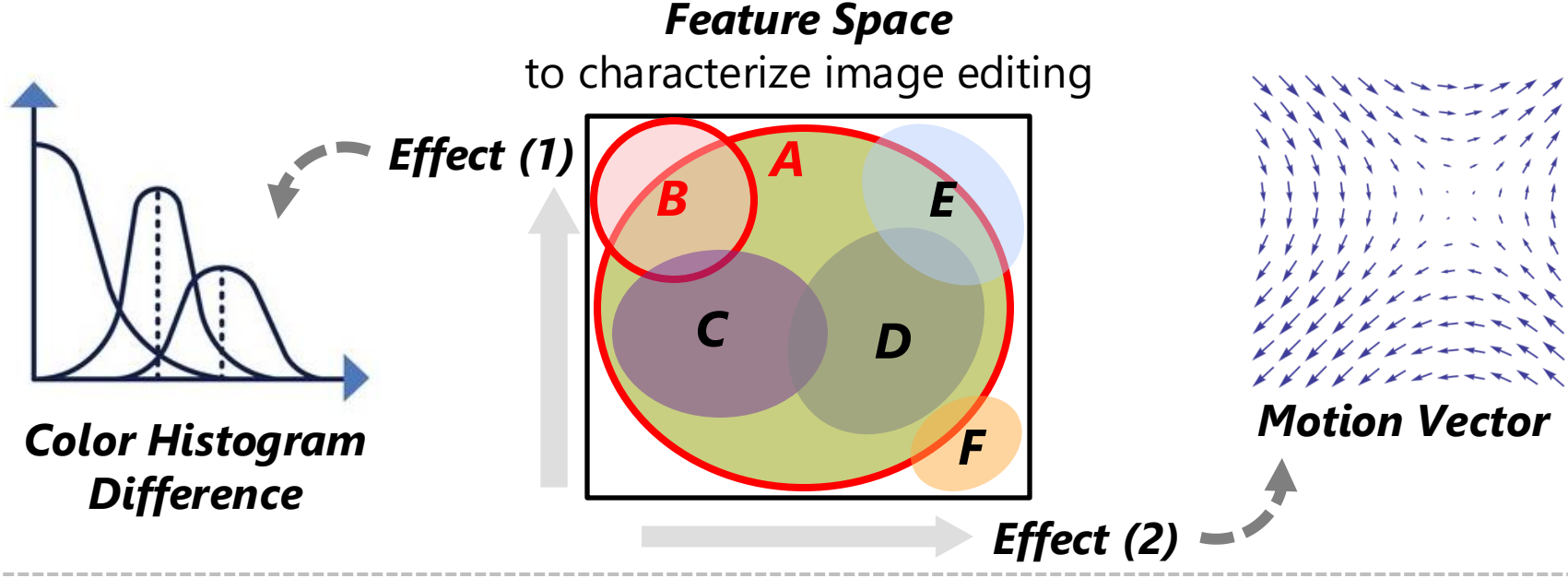
Data Processing: Representative Image Editing

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



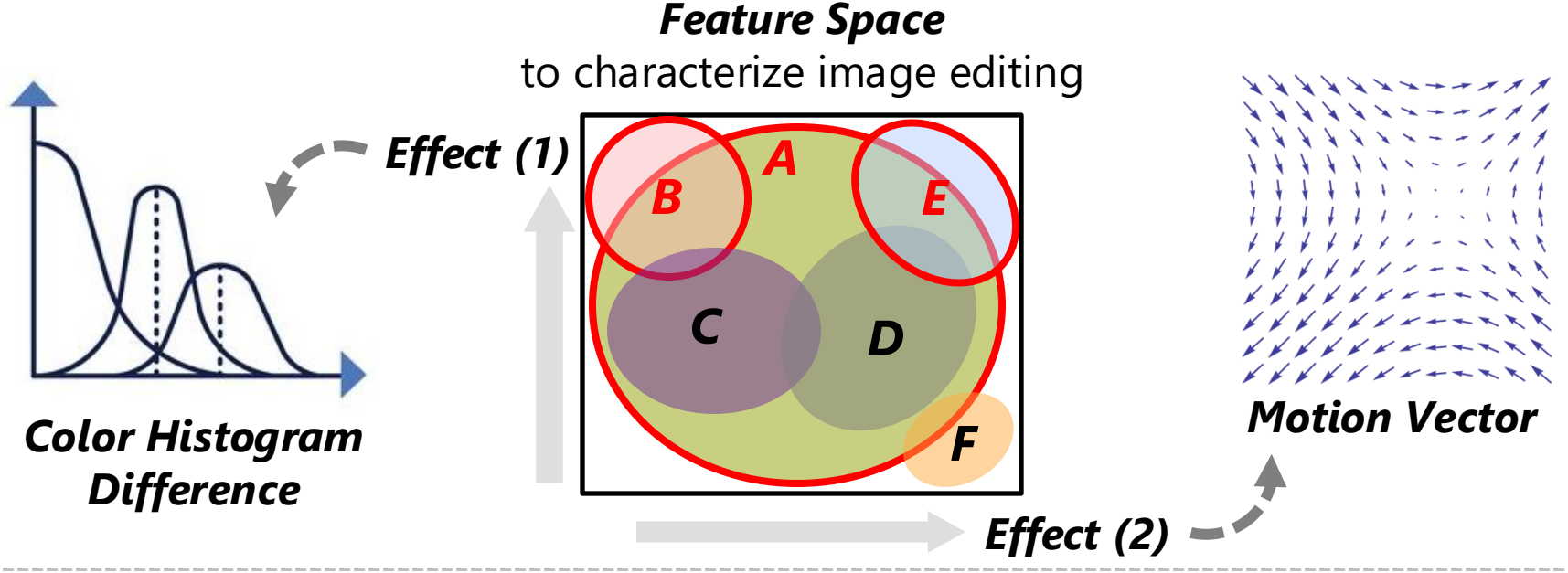
Data Processing: Representative Image Editing

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



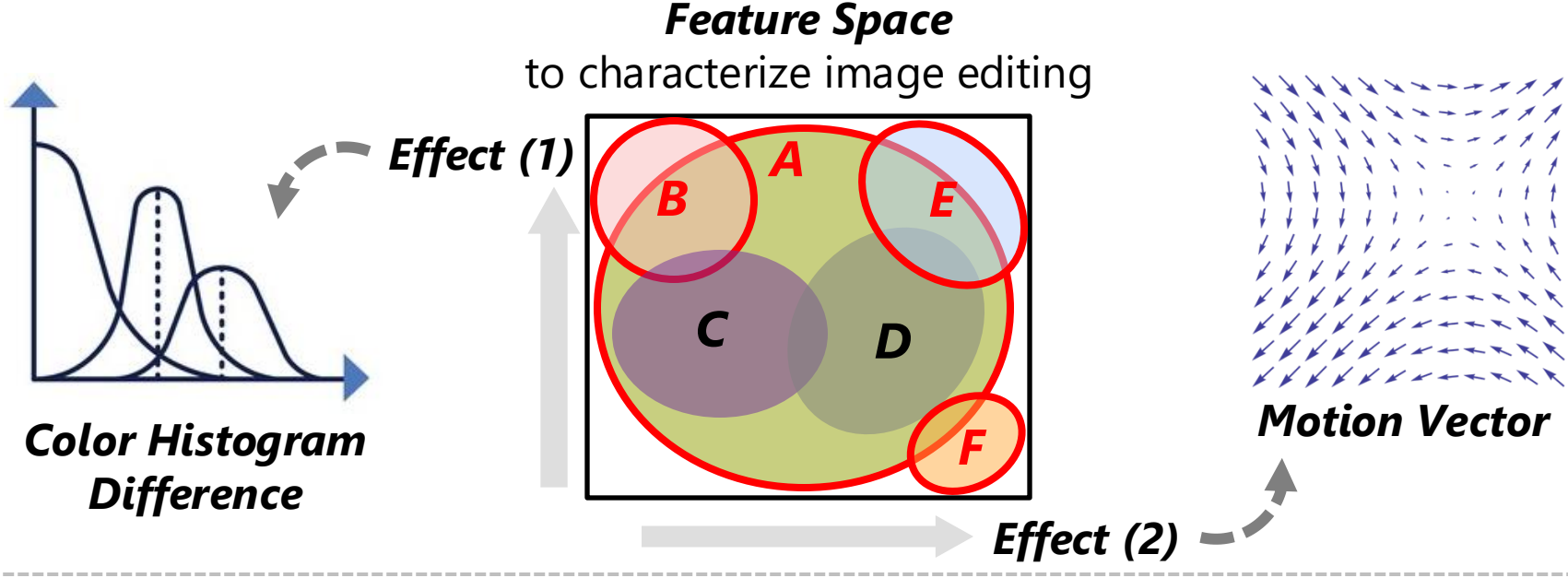
Data Processing: Representative Image Editing

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



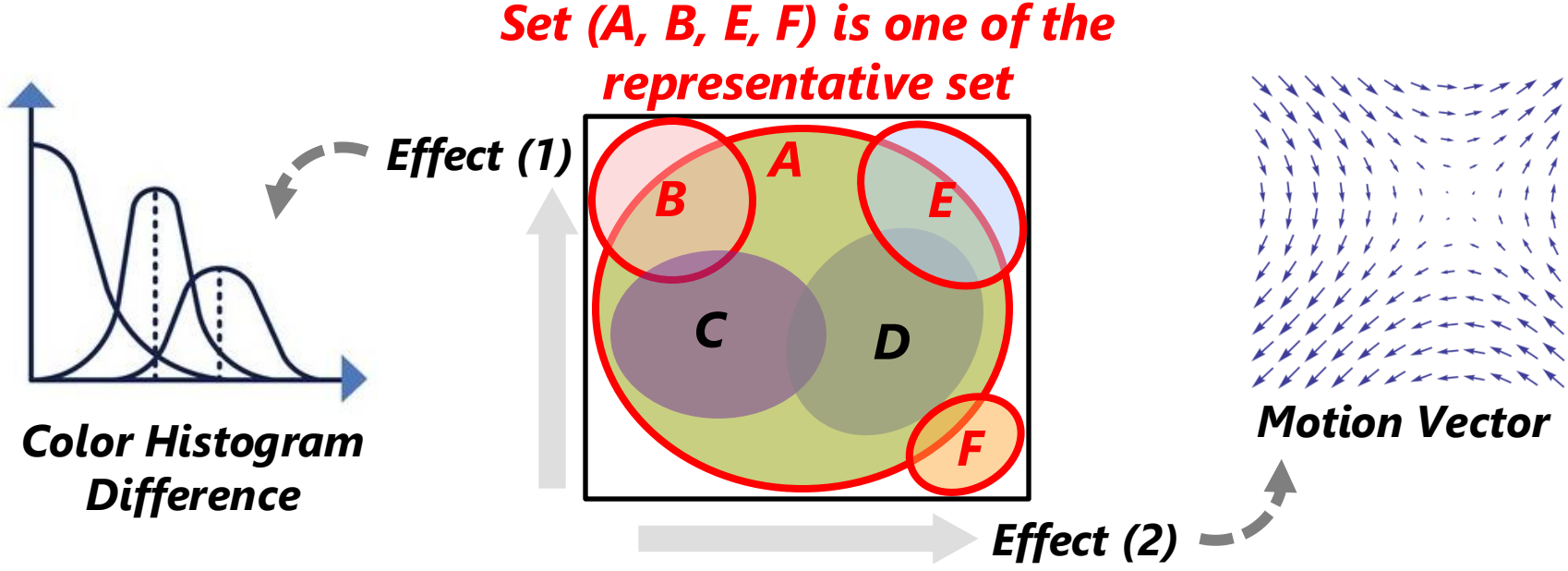
Data Processing: Representative Image Editing

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



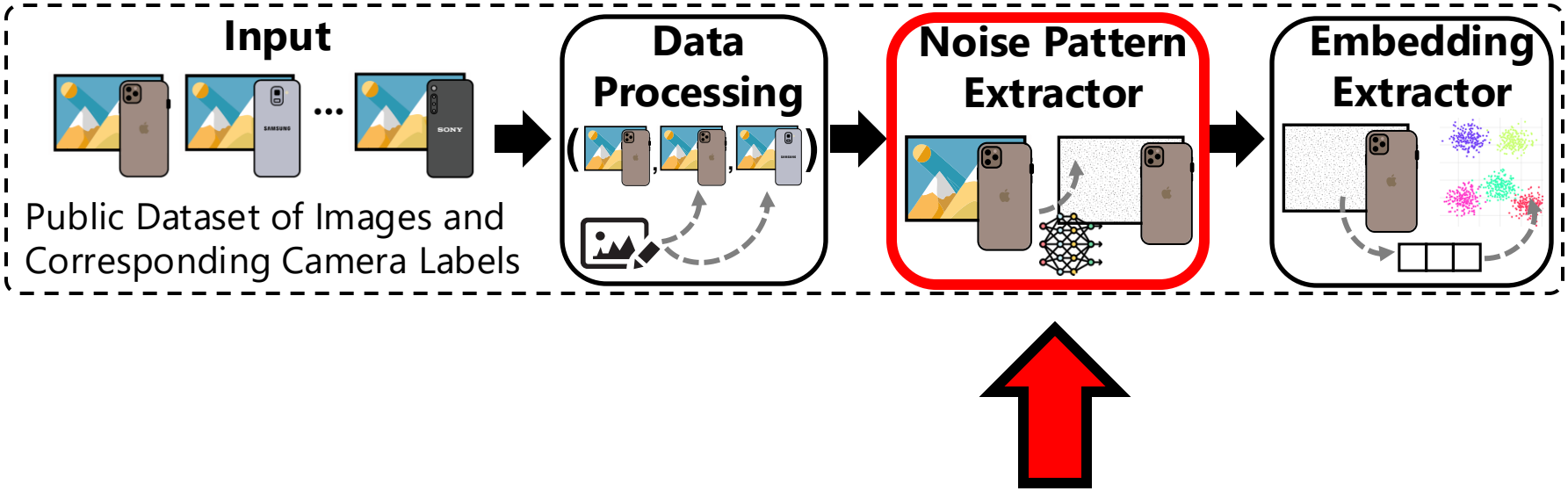
Data Processing: Representative Image Editing

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



Design of *CAMPrints*

Training Phase

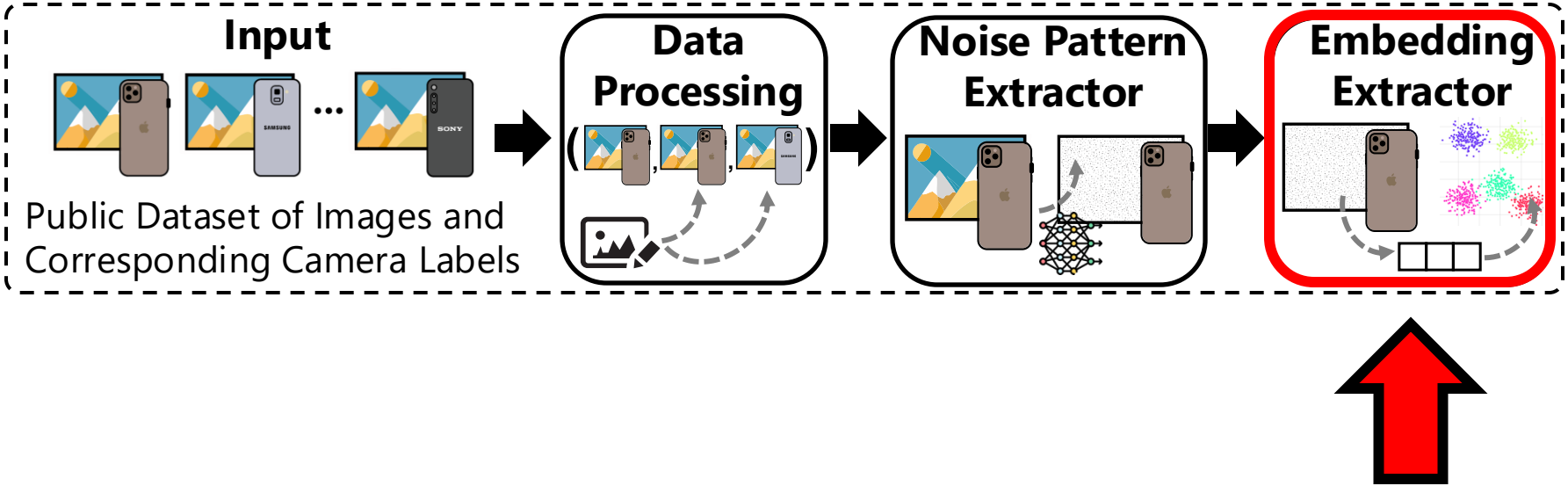


Design of *CAMPrints*

For Challenge #2

Multiple Sources of Noises

Training Phase



Embedding Extractor

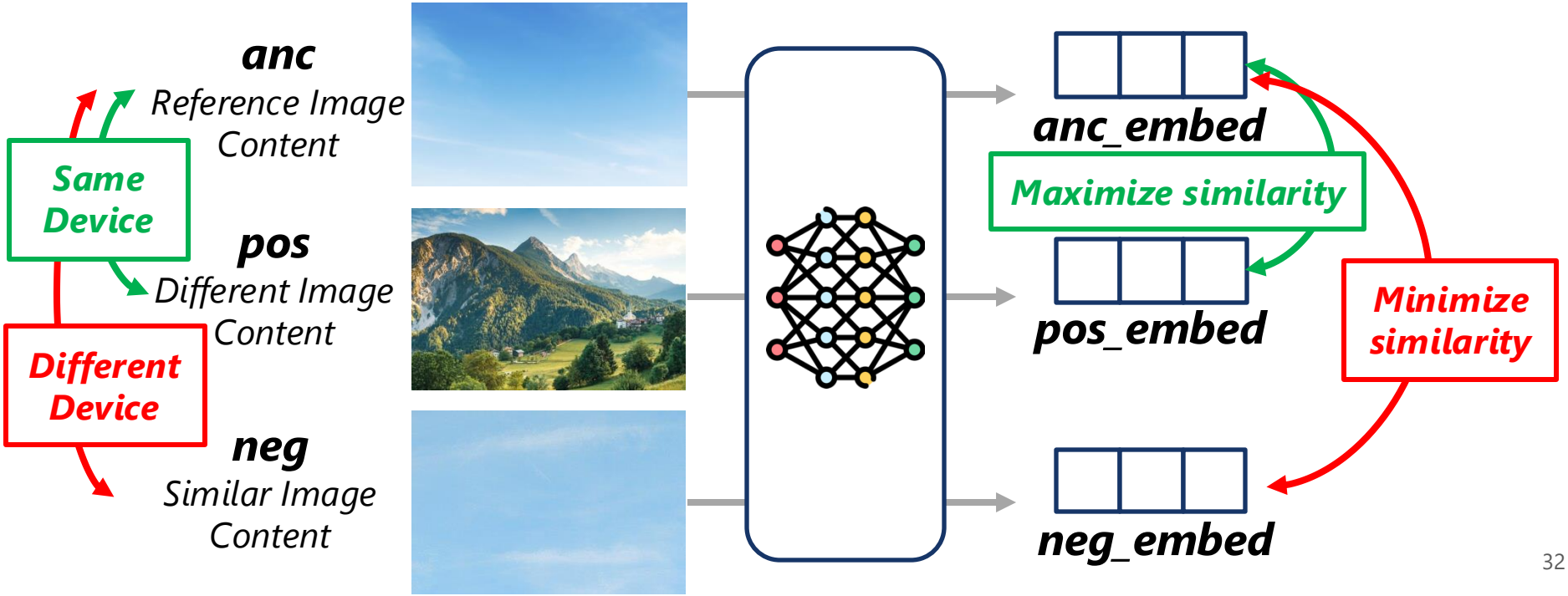
Goal: Encode noise pattern into latent representation to

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

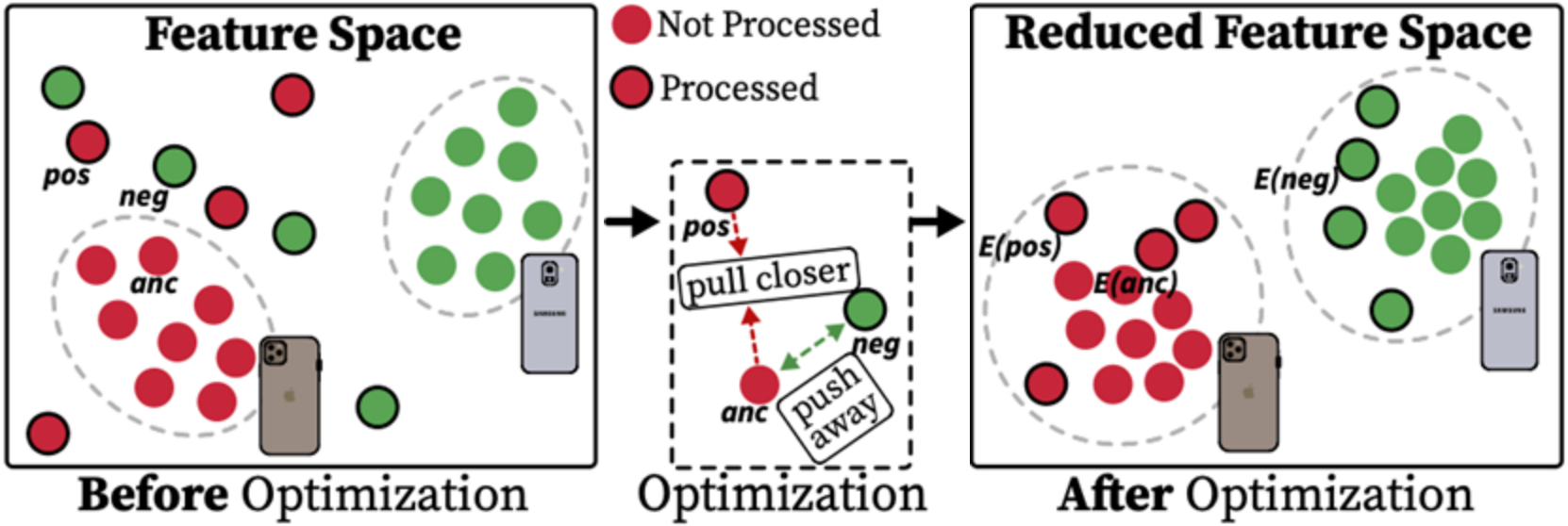
1. Filter out **content-induced noises**



Embedding Extractor

Goal: Encode noise pattern into latent representation to

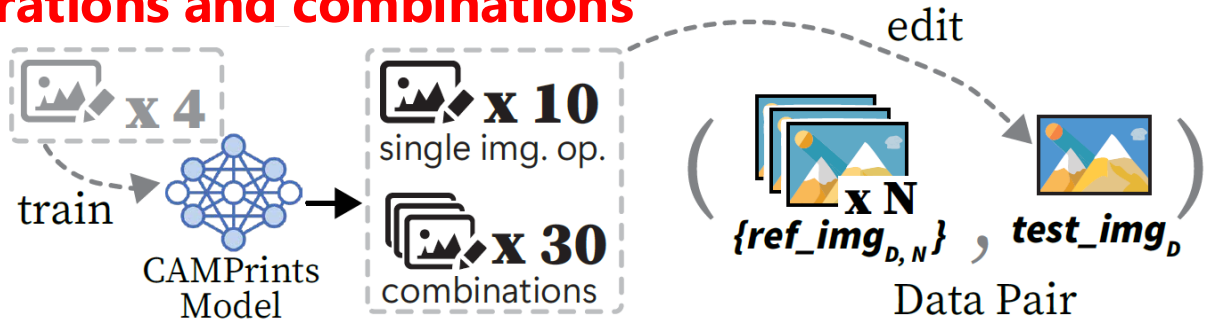
1. Filter out content-induced noises
2. **Maximize similarity between features** originating from same device despite image editing



Experiment setup

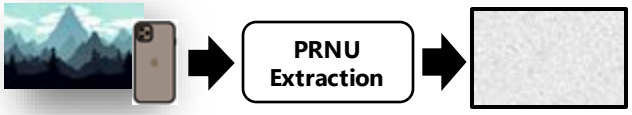
- We ensure **at least three different instances** per make-and-model to evaluate the **instance-level** accuracy

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



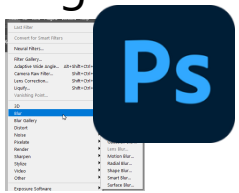
Summary of evaluation results

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

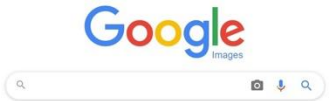


- Remains robust against **number and order** of image operations

- Generalizes to **unseen** image processing operations

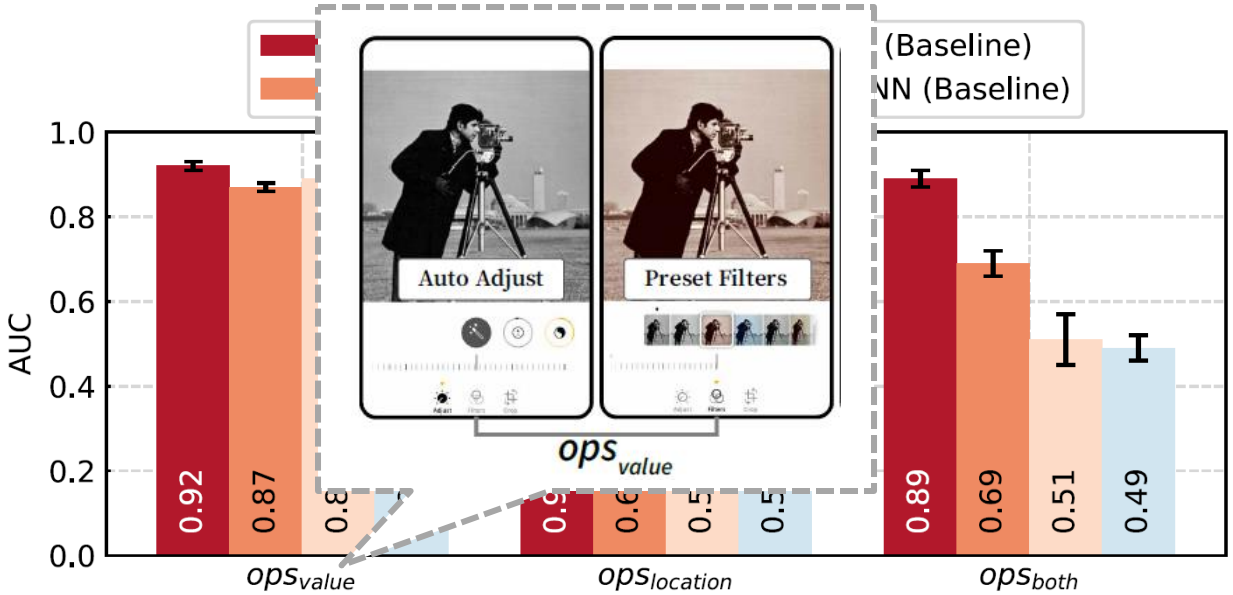


- Generalizes across **commercial software**
- Yields **80% less false positives** compared to Reverse Image Search



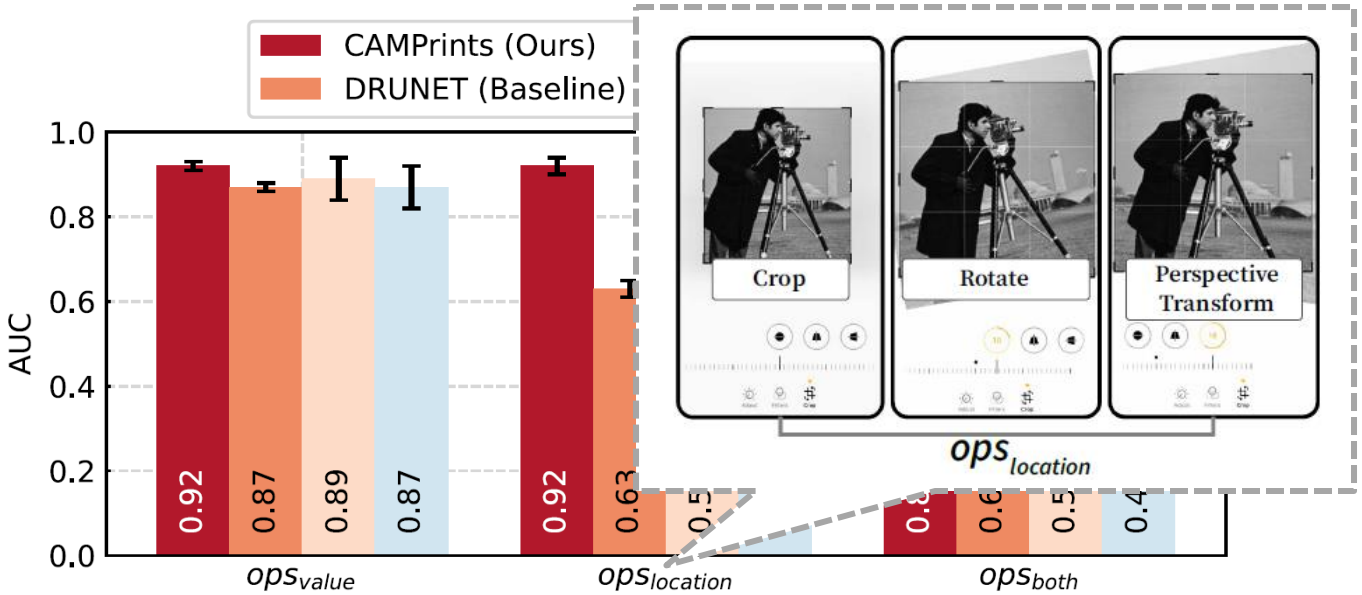
Overall performance

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



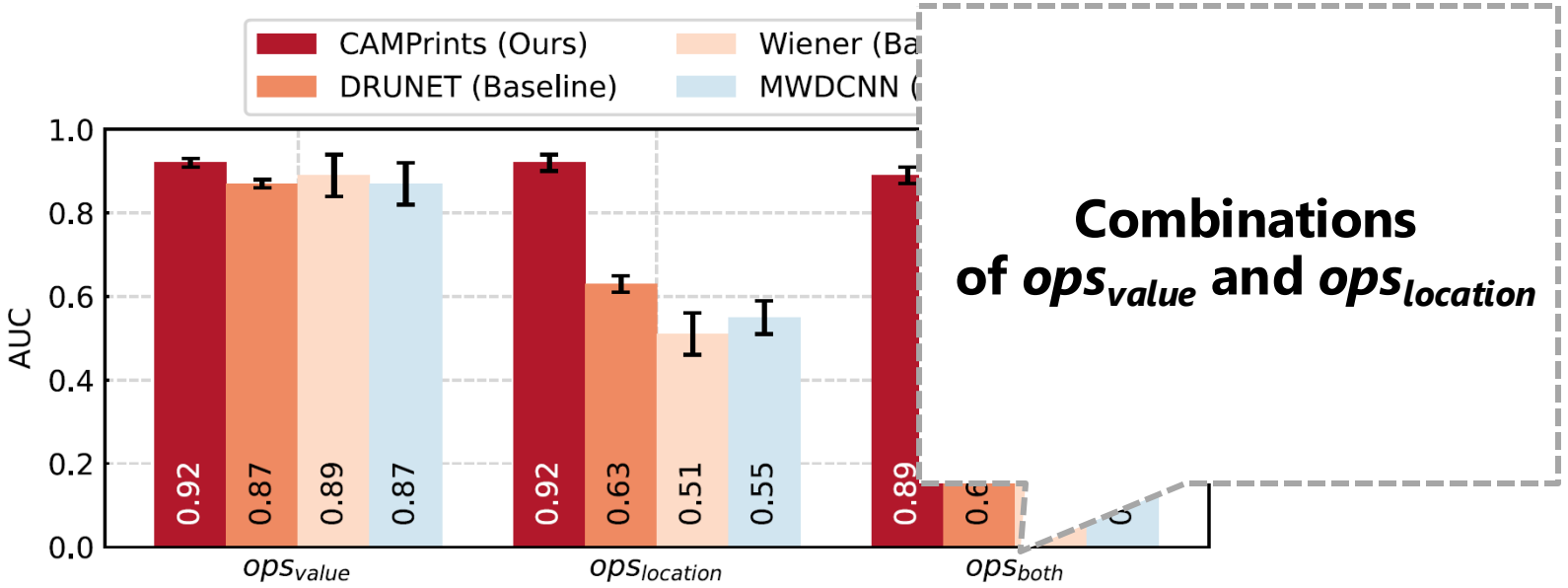
Overall performance

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



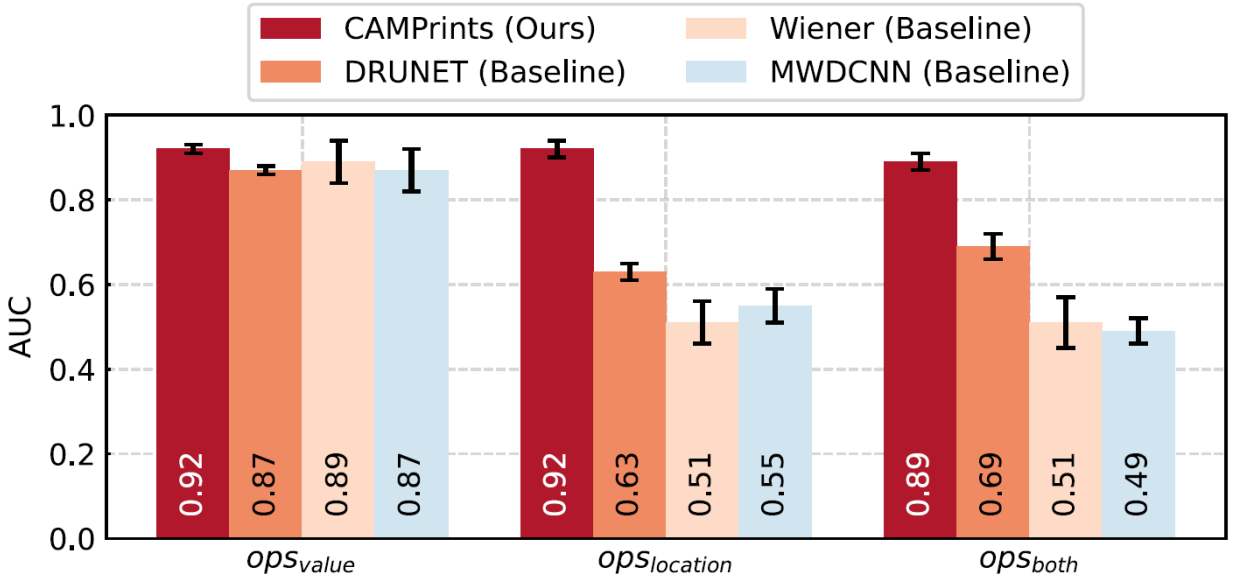
Overall performance

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



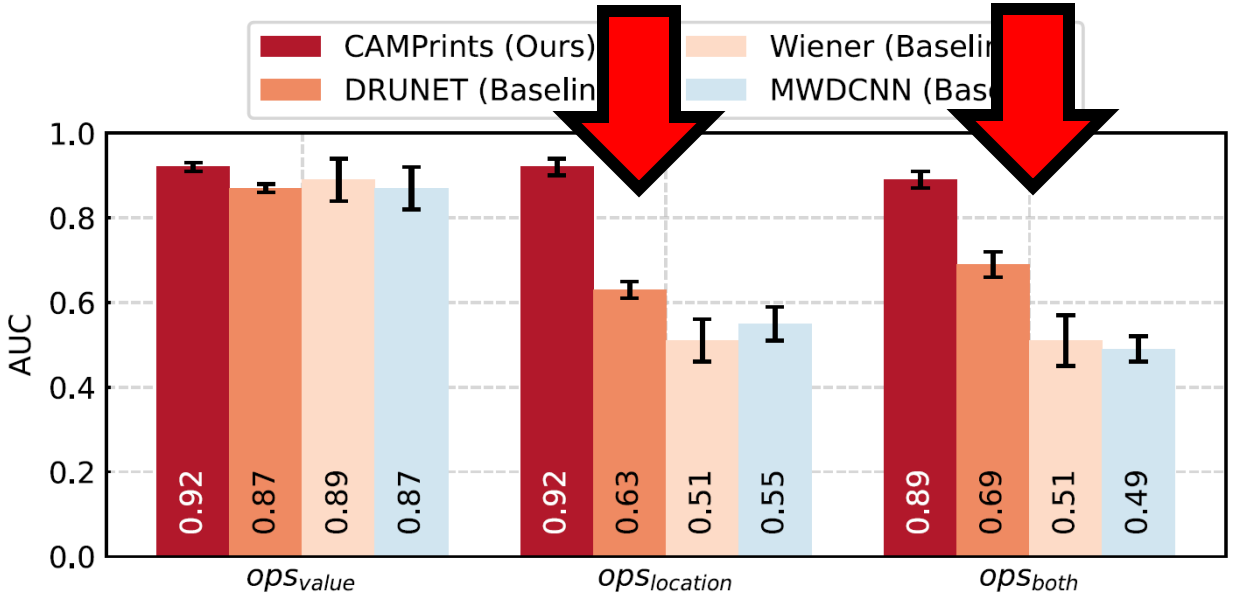
Overall performance

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



Overall performance

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

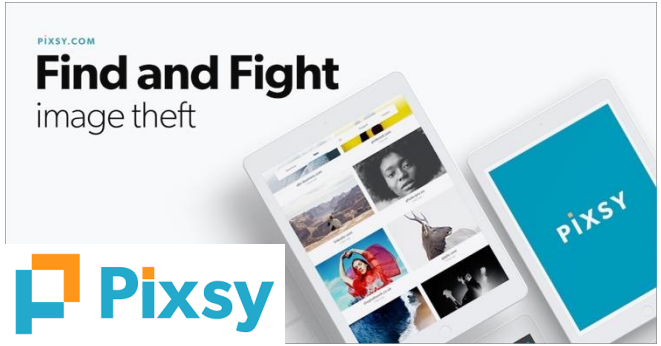


Discussion

Deployment Consideration

Integration into

- Social media and photo sharing platforms
- Copyright monitoring services



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

Extension of CAMPrints

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

CAMPrints + 

- Open standards for authenticity and provenance

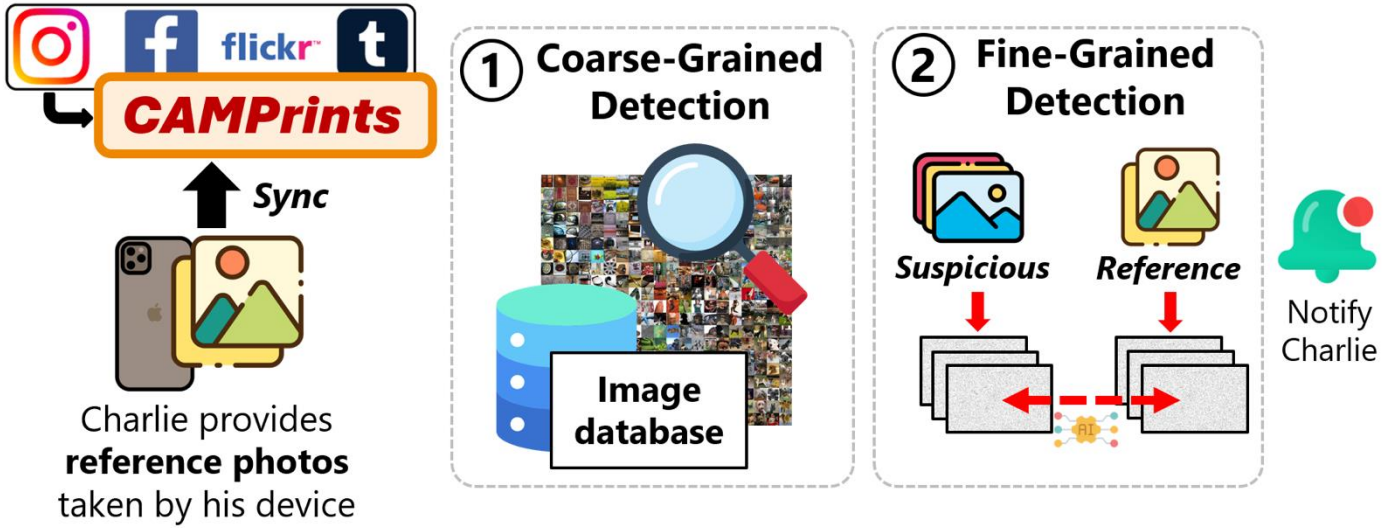
C2PA

- Online media forensics



Conclusion

- Detect online image theft using camera “fingerprints” (i.e., PRNU-induced noise pattern) as physical evidence of ownership
- Spur future research in authenticity and provenance in digital content



Thank you!

Bangjie Sun

Graduate Tutor and **PhD candidate** at the National University of Singapore

I am a passionate researcher in **computer vision**, and **sensing**. I am currently pursuing my Ph.D. in National University of Singapore (NUS). My supervisors are Prof. Jun Han in Yonsei University and Prof. Chan Mun Choon in National University of Singapore. My research interests are in the intersection of computer vision and sensing systems.

Contact: bangjie@comp.nus.edu.sg

I'm looking for a job ☺

Scan me