Scoop: Mitigation of Recapture Attacks on Provenance-Based Media Authentication

Yuxin (Myles) Liu, Habiba Farrukh, Ardalan Amiri Sani, Gene Tsudik

TrussLab

UCI University of California, Irvine

Sharad Agarwal

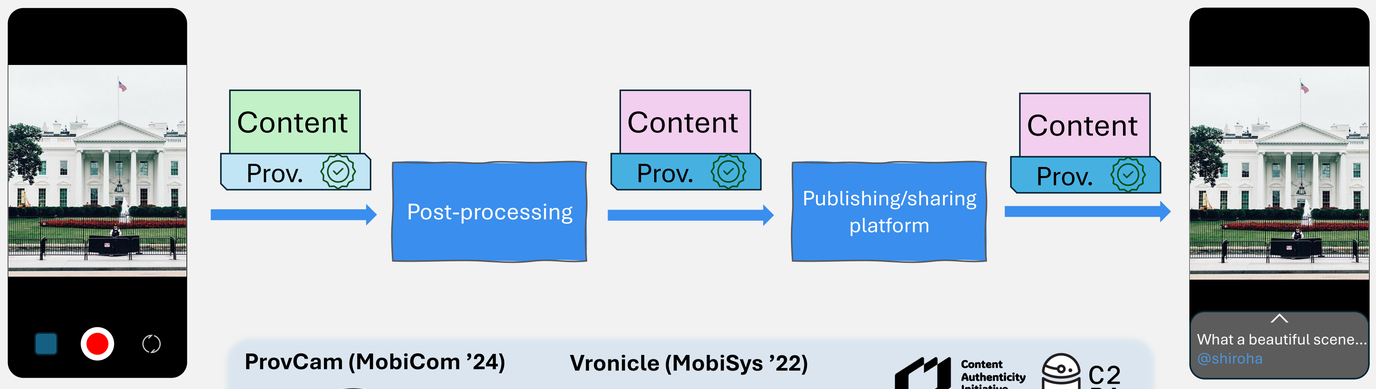
Microsoft

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

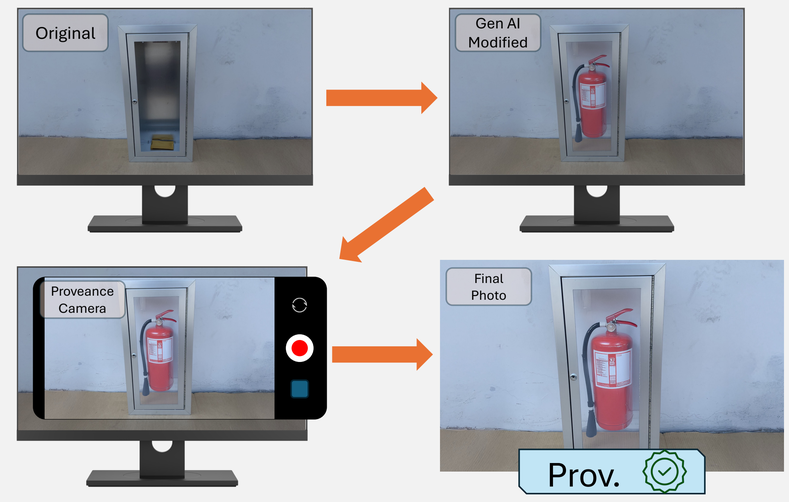
ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

Provenance-based media authentication

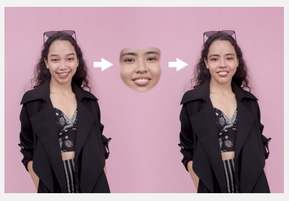


Recapture attack in the provenance era



Recapture attack is not new, but it is getting more powerful and dangerous

- Advances in content manipulation/fabrication and display technologies



(e.g., face swapping)

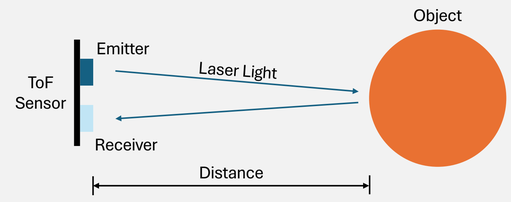
(e.g., bus with no real window)

- Two types of recapture attacks: screen-based and print-based
- Existing countermeasures are based on prior knowledge of the recapture medium and/or the camera
- Attackers are **in control** here (recapture medium and camera)

- A user study with 16 photos (8 recaptured and 8 original)
- 43 adult participants
- Average correct classification rate: 50.15% ($t(42) = 0.071, p = 0.944$)

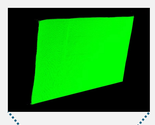
Depth-enabled provenance

- Time-of-Flight depth sensors (dToF and iToF)
- Measure distance to a target
- Equipped on modern smartphones (e.g., iPhone)



Not all flat surfaces are recaptures; not all recaptures are misleading

Photo of a recapture



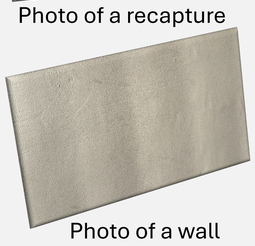
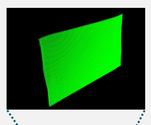
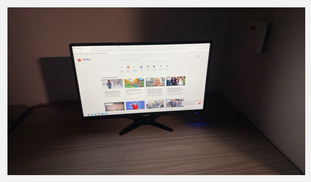


Photo of a wall

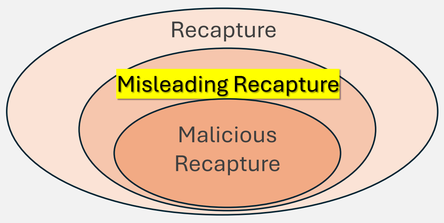


- According to point clouds (reconstructed with provenance depth), they're both flat



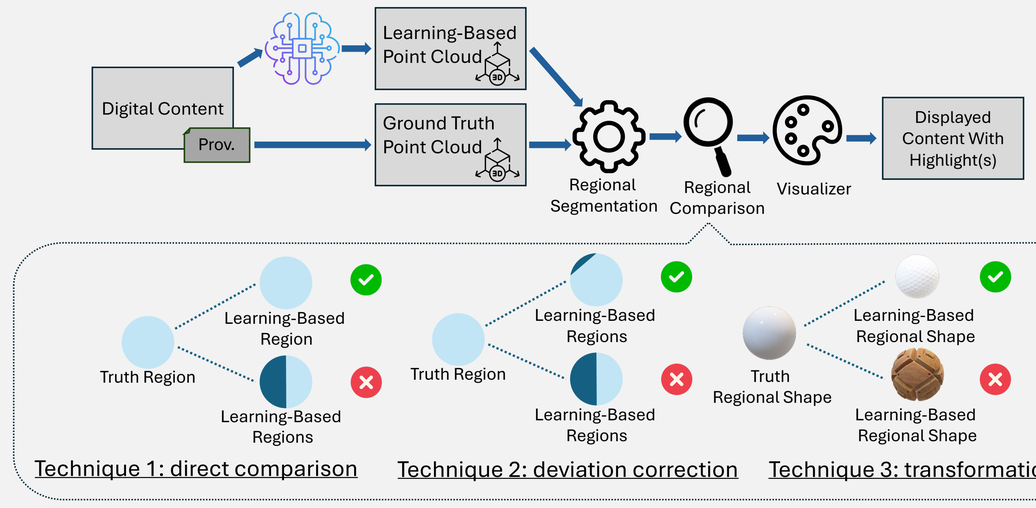
- These two photos contain recapture, but they're not misleading

Categorization of recapture

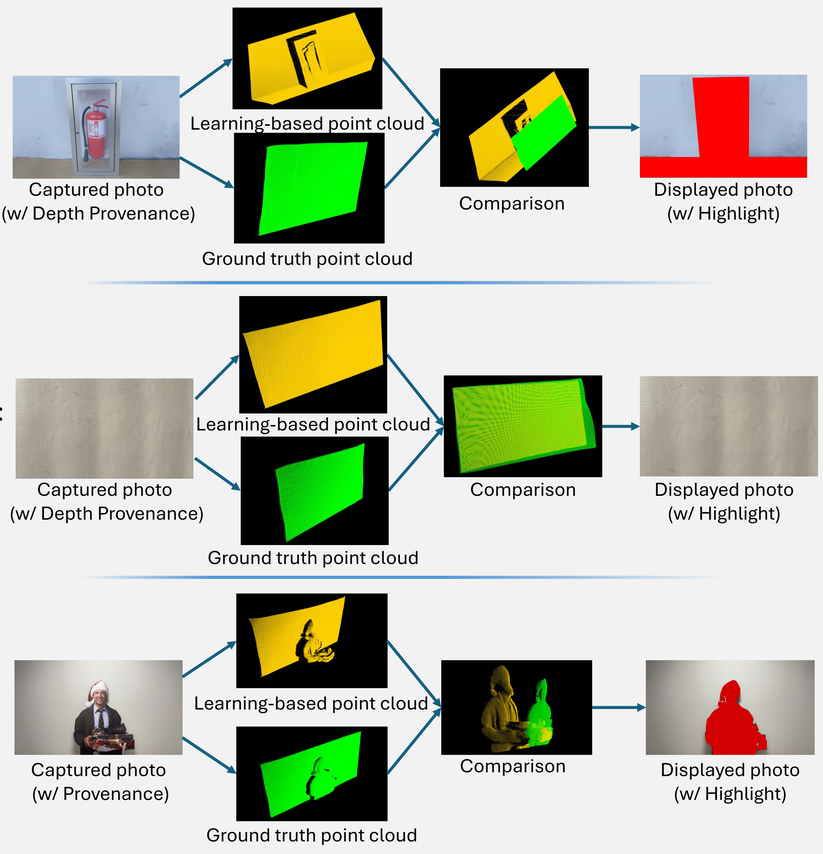


- Finding misleading recapture can assist people in identifying malicious recapture
- Need to compare human perception of depth with provenance depth
- Use learning-based monocular depth estimation to estimate human's perception of depth

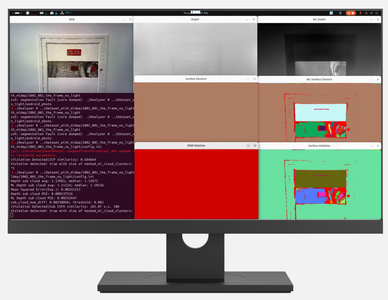
Scoop's workflow



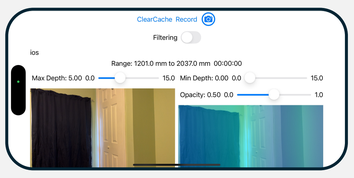
Scoop in action



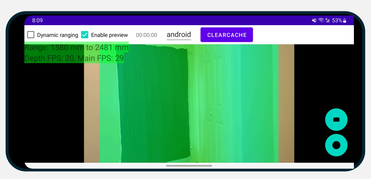
Prototype



Desktop viewer application (OpenCV and PCL)



iOS camera application

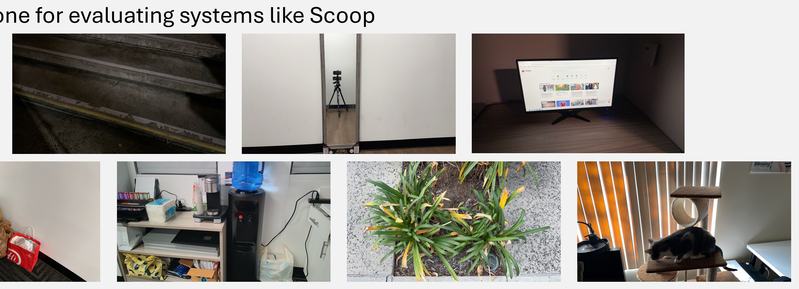


Android camera application

Dataset and evaluation

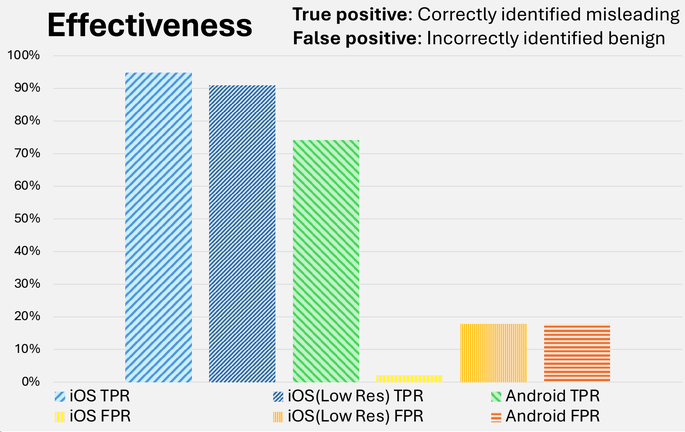
A first-of-its-kind dataset

- Captured using our two smartphone camera prototypes
- Includes 122 unique data points with 78 recapture scenarios (TVs, cardboard cutouts, projector, and mixed)
- Both photos and videos
- A cornerstone for evaluating systems like Scoop

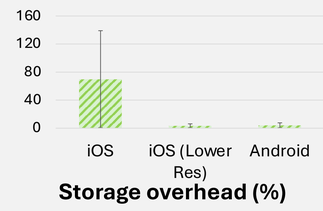


Effectiveness

True positive: Correctly identified misleading
False positive: Incorrectly identified benign



Runtime overhead (s)



Storage overhead (%)