Security & Forensics: Signals, Content & Devices

Prof. Min Wu / Media and Security Team

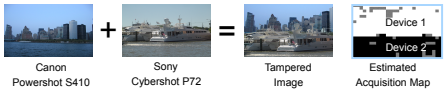
Media & Security Team at UMD
MAST

ISR @25
The Institute for Systems Research
A. JAMES CLARK SCHOOL OF ENGINEERING

Intrinsic Fingerprinting

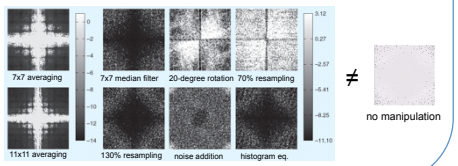
- Answer forensic questions about a digital image
  - How is the image created?
  - What type of device captured the image?
  - Has the image been manipulated after capture? If so, how?
- Developed methodologies to extract intrinsic traces left by an image capturing device
- Applications: imaging type classification, device tracing, and tampering detection

Detecting Inconsistency of camera characteristics



Canon Powershot S410 | Sony Cybershot P72 | Tampered Image | Estimated Acquisition Map

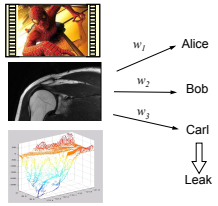
Detecting tampering via approximate/empirical "frequency response" of post-camera operations



Embedded Fingerprinting

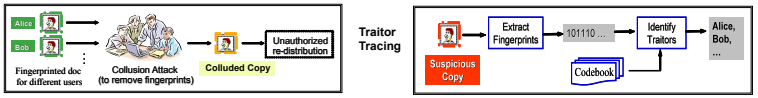
Leak of information poses serious threats to government operations and commercial markets

⇨ Promising countermeasure: Embedded Digital Fingerprints



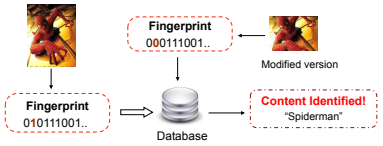
- Insert special signals (called "fingerprints") to identify recipients
- Challenges: fidelity, robustness, tracing capability

Collusion-Resistance Identify malicious users involved in multi-user collusion attack



Content Fingerprinting

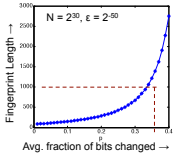
A compact, robust, and unique representation of multimedia content used for automated identification and management



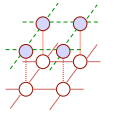
Focus of Our Research

- Gain a more solid understanding of current systems and devise guidelines for designing new systems
- Complement experimental evaluations to predict how performance scales as multimedia database size increases
- Examine possible attacks and devise counter-attack strategies

Tradeoff b/w fingerprint length, accuracy, and robustness



Markov Random Field model for fingerprints

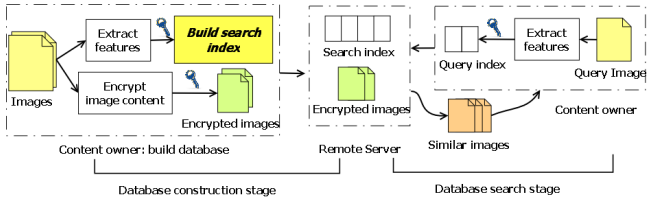


Confidentiality-Preserving Multimedia Search

Enable content-based search over encrypted multimedia for utilizing private information stored in the cloud

Gmail Flickr

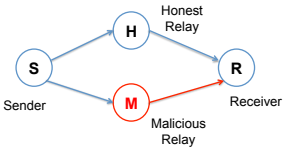
- Protect visual features: distance-preserving encryption by bit-plane randomization, random projection
- Secure search indexes: secure inverted index and min-hash based on bag-of-words representation



Secure Localization in Wireless Sensor Networks

- Obtain accurate estimate of node positions efficiently in the presence of malicious nodes
- Developed a computationally efficient iterative method for secure localization
- Robust against coordinated attacks by up to 50% of the nodes and non-coordinated attacks by > 50% of the nodes
- Localization accuracy comparable to existing methods with lower computational and memory requirements

Cross-Layer Approaches for Tracing Malicious Relays



- Conventional application-layer cryptography can detect anomaly but insufficient to pinpoint adversarial nodes
- Leverage physical layer to embed tracing signals in the data
- Classifying adversary and cooperator by signal correlation

Data Hiding in Programs for High-Performance Trusted Computing

- Traditional designs of computing systems separately deal with high performance vs. trustworthy computing
- Ability to tag computer instructions with side information may bring system-wide performance enhancement
- Develop new framework for hiding information in programs to simultaneously achieve high-performance and trusted computing
- Approach: Leverage unequal presence of operand combinations to ensure minimum change/cost in instruction set and hardware
- Verified by simulation and FPGA prototyping

Acknowledgement: Include joint research with ISR faculty/alumni K.J.R. Liu, G. Qu, W. Trappe, Z.J. Wang, H.V. Zhao, and MASTers (W-H. Chuang, R. Garg, H. Gou, S. He, W. Lu, Y. Mao, A. Swaminathan, and A.L. Varna). Funded in part by NSF, ONR, AFRL/AFOSR, and MovieLab.