Invisible Traces in Pixels and Bits

Min Wu

Media and Security Team (MAST)
ECE Department / UMIACS
University of Maryland, College Park

http://www.ece.umd.edu/~minwu/research.html

Include joint work with Hongmei Gou, Shan He, K.J. Ray Liu, Christine McKay, Ashwin Swaminathan, and Avinash Varna.

THE A. JAMES CLARK SCHOOL of ENGINEERING | UNIVERSITY OF MARYLAND

Multimedia Security and Forensics: Where Sherlock Holmes Meets Signal Processing

- Ensure content to be used by authorized users for authorized purpose
- To reconstruct what have happened to the content and answer who has done what, when and how.
- Cross-disciplinary approaches involving signal processing, machine learning, communications, cryptography …

Captured by what device? What technologies are used?

Photos, maps, documents, audio, video, medical records …

How to efficiently and securely deliver contents to multiusers?

Who leaked info? Have content been tampered?

Many Forms of "Digital Fingerprints"

Many types of fingerprints for multimedia protection & management

I. C. E.

Embedded Fingerprint

Embed unique ID/signal as digital fingerprints to track individual copy and trace unauthorized use

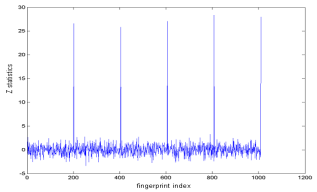
Content-based Fingerprint

Compact content signature for content identification, and also useful for watermarking and content authentication

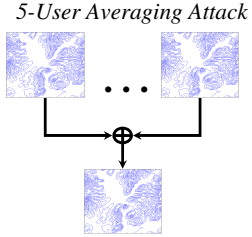
Intrinsic Fingerprint

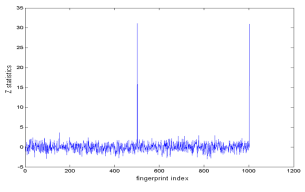
Examine inherent traces left on multimedia by device or processing – Provide non-intrusive forensics to determine origin, integrity, etc.

Collusion-Resistant Fingerprinting: Examples

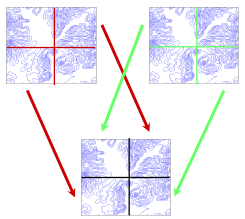


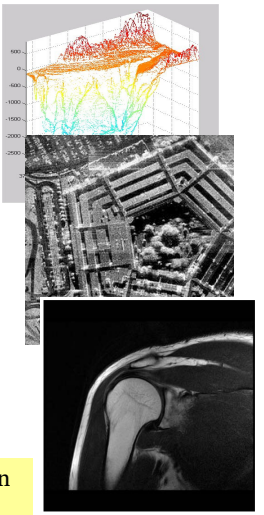
5-User Averaging Attack





2-User Interleaving Attack



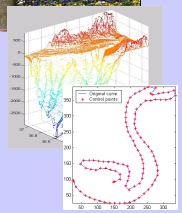


=> Can survive combination attacks of collusion + print + scan and detect fingerprint from hard copies

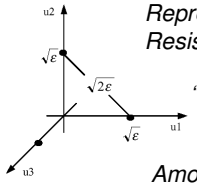
Road Map on Media Fingerprinting Research

Robust Embedding

adapt to media characteristics



Orthogonal Fingerprints



Represent how many users? Resist how many colluders?

"most effective" collusions?

Correlated Fingerprints

Amount of resources used?

Group-based FP to exploit Attacker Behavior

Coded FP

- *Combinatorial codes + CDM*
- *Error correcting codes + TDM*

Joint Coding-Embedding Framework

overcome prior work's problems of long code length, low resilience, and limited scalability

When No Proactive Protections are available …

Can we answer many forensic questions?

- On the integrity, origin, and provenance of increasingly popular audio/visual data
- Arise from homeland security, law enforcement, medical, and financial, and IT applications
  - What type of sensor was used?
  - Which camera brand took this picture? What model?
  - What processing has been done?
    - *Has it been tampered? manipulated?*
  - What imaging technologies were used?

Many Forms of "Digital Fingerprints"

Many types of fingerprints for multimedia protection & management

I. C. E.

Embedded Fingerprint

Embed unique ID/signal as digital fingerprints to track individual copy and trace unauthorized use

Content-based Fingerprint

Compact content signature for content identification, and also useful for watermarking and content authentication

Intrinsic Fingerprint

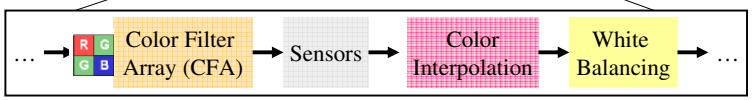
Examine inherent traces left on multimedia by device or processing – Provide non-intrusive forensics to determine origin, integrity, etc.

Exploit Intrinsic Fingerprints via Component Forensics

Real world scene

Camera Components

Digital image



- Break down the info. processing chain into individual components
- Identify algorithms and parameters employed in major components of a digital device or processing system
- Concept extensible to general info processing chain beyond multimedia
  - E.g. forensics on communication channels, etc.

Ref: Swaminathan/Wu/Liu in ICASSP'06 and IEEE Trans. Info Forensics & Security ('07)

Types of Component Forensics

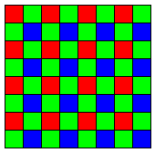
- Intrusive forensics
  - Devices in hand
  - Break it apart and identify every component

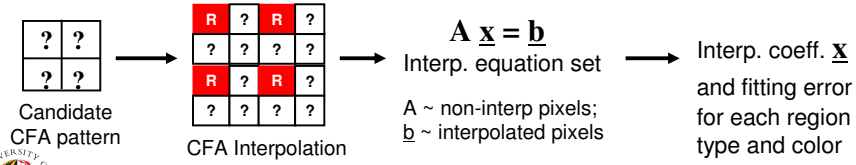
- Semi non-intrusive forensics
  - Devices in hand but not to break it apart
  - Design test conditions and inputs to improve estimation accuracy

- Completely non-intrusive forensics
  - Products /devices not in hand
  - Sample outputs from devices available

Forensic Estimation and Identification

- Establish a processing model and estimate parameters
  - Small # possibilities => exhaustive search or by classifier design
  - More continuous valued parameters => analyze based on estimation theory
- Example: color interpolation in digital camera
  - Approximate by texture classification and linear filter
    (one set of interp. coeff. for smooth, horizontal & vertical)
  - Find best linear estimate of filter coeff. in each class
    (least-square type of method for robustness)
  - Find CFA pattern in a search space that minimizes fitting errors





Detecting Which Camera Brand Took an Image

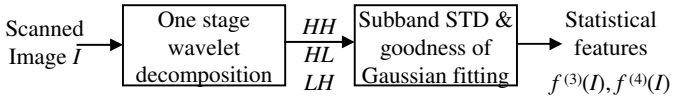
- Average accuracy: 90% for 9 camera brands on uncontrolled scenes

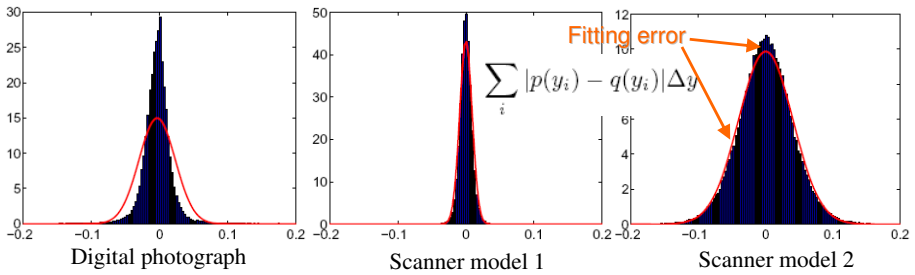
=> Features inspired by component forensics perform better than empirical features: *less dependent on input scene, tolerate compression.*

19 cameras, 200 image blocks per camera model; color interpolation coeff. features

	Camera Model		Camera Model
1	Canon Powershot A75	11	Olympus C3100Z/C3020Z
2	Canon Powershot S400	12	Olympus C765UZ
3	Canon Powershot S410	13	Minolta DiMage S304
4	Canon Powershot S1 IS	14	Minolta DiMage F100
5	Canon Powershot G6	15	Casio QV-UX2000
6	Canon EOS Digital REBEL	16	FujiFilm Finepix S3000
7	Nikon E4300	17	FujiFilm Finepix A500
8	Nikon E5400	18	Kodak CX6330
9	Sony Cybershot DSC P7	19	Epson PhotoPC 650
10	Sony Cybershot DSC P72		

E.g.: Noise Features from Wavelet Analysis

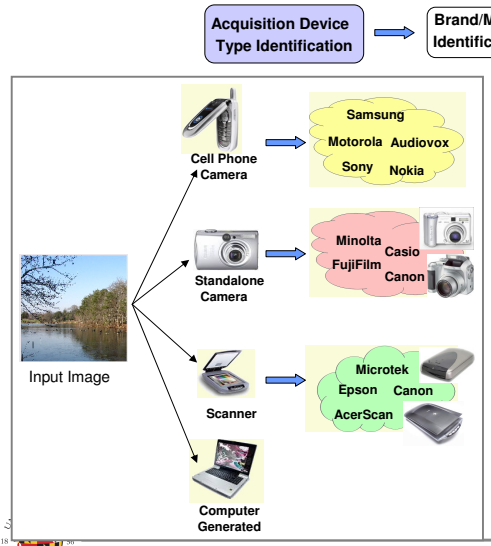




Histogram → Mean and STD → Gaussian distribution → Goodness of Gaussian fitting

HH,HL,LH sub-bands
RGB components
2x3x3 = 18 features

Acquisition Forensics: Noise + Interp. Features



Q1) What type of device was used to capture the image?

- 94% accuracy in identifying device type

Q2) What brand/model of the device captured the image?

- **Cellphone cameras:** 98% accuracy over 5 brands
- **Standalone cameras:** 90% over 19 camera models from 9 camera brands
- **Scanners:** 93% accuracy over 9 scanner brands

Applications in Technology Business Intelligence

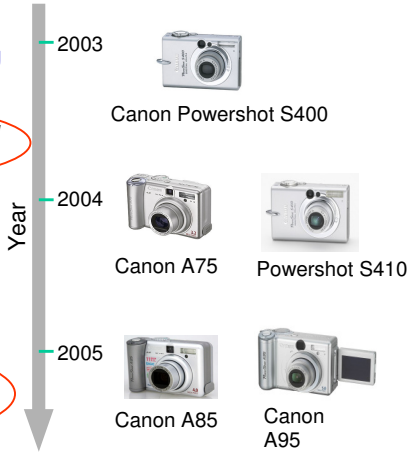
Quantitative assessment on similarity & differences of major components

- Between brands
  - High similarity suggests either Licensing or potential IP Infringement

=> Improve efficiency + efficacy from existing practice using soft/hardware documentation

- Evolution Forensics
  - Different models over time/price tier
  - What components were modified? What remain the same?

=> Facilitate companies to understand competitors' technologies and develop alliance strategies for future innovations



Many Forms of "Digital Fingerprint"

Many types of fingerprints for multimedia protection & management

I. C. E.

Embedded Fingerprint

Embed unique ID/signal as digital fingerprints to track individual copy and trace unauthorized use

Content-based Fingerprint

Compact content signature for content identification, and also useful for secure watermarking and content authentication

Intrinsic Fingerprint

Examine inherent traces left on multimedia by device or processing – Provide non-intrusive forensics to determine origin, integrity, etc.

"Fingerprints" from Media Content

Content Fingerprints: a compact, robust, and unique representation of multimedia data

- Internet opens up new ways to share multimedia
  - ⇨ Concerns about copyright infringement

    How to help online multimedia communities flourish legally?

Google videos

YouTube Broadcast Yourself™

- Enormous volume of multimedia content generated
  - ⇨ Need better techniques to manage

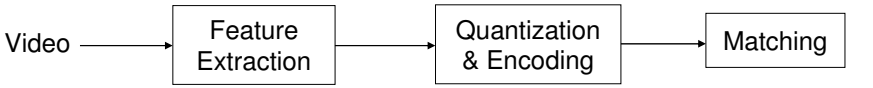
    Enable automatic identification of multimedia?

Shazam app for iPhone

Design and Modeling Framework for Content FP

Analyze the mapping from video to features to bits: how is processing on video translated to changes in hash bits?

Model performance at bit string level



Movie and TV Drama	Spatial: block-based, salient features	Strong Quantization	Exhaustive matching
Animation	Temporal features	Ordinal Ranking	Approximate matching (LSH)
Ads	Transform domain	Quantized difference of features	
Sports	Color-based		

Learn More from Poster Session and Online

- Digital Image Forensics
- Multimedia Content Identification
- Multimedia Fingerprinting & Traitor Tracing
- Privacy-Preserving Multimedia Retrieval

Media And Security Team

http://www.ece.umd.edu/~minwu/research.html