Seeing the Invisibles:
A Backstage Tour of Information Forensics

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 research with Wei-Hong Chuang, Adi Hajj-Ahmad, Ravi Garg, Hongmei Gou, Shan He, K.J. Ray Liu, Christine McKay, Hui Su, Ashwin Swaminathan, Wade Trappe, Avinash Varna, Jane Wang, Chau-Wai Wong, and Hong Zhao.

Role Play as Sherlock Holmes in our Digital Era

1. Leak: A proprietary image sent to 10 people got leaked out
   ➔ Who leaked the info?

A Decade+ of Research on Info. Forensics

- Our life and work are forever changed …
  - By advances in electronics, computing, communications, sensing, and signal processing

- So much multimedia info and content right at our hand …
  - Keep us entertained
  - Used as important evidences & records

- Gather traces of evidence
  - Origin, history, integrity, etc.
  - A broad range of applications

Role Play as Sherlock Holmes in our Digital Era

1. Leak: A proprietary image sent to 10 people got leaked out
   ➔ Who leaked the info?

2. Source: Picture of a heavily guarded xPhone7 prototype showed up on web
   ➔ Is it a real photo or a graphic rendition? Who in the company took it using his/her camera?

3. When/Where: an audio clip with incriminating words showed up
   ➔ were its content and recording time true as claimed?
Role Play as Sherlock Holmes in our Digital Era

1. **Leak**: A proprietary image sent to 10 people got leaked out
   - Who leaked the info?
2. **Source**: Picture of a heavily guarded xPhone7 prototype showed up on web
   - Is it a real photo or a graphic rendition? Who in the company took it using his/her camera?
3. **When/Where**: an audio clip with incriminating words showed up
   - Were its content and recording time true as claimed?

---

Example: Replacing the Last Bit of Pixels

Replace LSB with Pentagon’s MSB

---

Robust Watermarking via Spread Spectrum Embedding

- Embedding domain tailored to media characteristics & application requirement

---

Min Wu (UMD): Multimedia Information Forensics
**Fingerprinting Topographic Map**

- Traditional protection: intentionally alter geospatial content
- Embed much less intrusive digital fingerprint for a modern protection

- 9 long curves are marked; 1331 control points used to carry the fingerprint

**Collusion-Resistant Fingerprinting: Examples**

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

**Joint Coding-Embedding via Anti-Collusion Codes**

User-1 \((-1, -1, -1, 1, 1, 1, ..., 1)\)  
User-4 \((-1, 1, 1, 1, 1, 1, ..., -1, 1, 1, 1)\)

Extracted fingerprint code \((-1, 0, 0, 1, ..., 0, 0, 1, 1)\)

Collude by Averaging

Uniquely Identify User 1 & 4

16-bit ACC for detecting up to 3 colluders out of 20

**Applications: From Government to Hollywood**

Insert special signals to identify recipients
- Deter leak of proprietary documents
- Consider imperceptibility, robustness, traceability

Rights management by copyright industry ($500+Billion ~ 5\% U.S. GDP)

- Successfully catch media pirates => Wide adoption now
  - Track down illicit sharing of digital TV access – Daqing, China (Nov. 2007): found and convicted perpetrator
Explore More …

  - Joint Coding and Embedding: fundamental tradeoffs
  - Large scale video fingerprinting; special media type such as maps
  - Group based fingerprinting; behavior forensics
- Recent directions: probabilistic fingerprint/tracing code
- Industry R&D: by movie industry (e.g. Technicolor R&D, MovieLab) and printing/marketing (e.g. Digimarc Inc.)

Role Play as Sherlock Holmes in our Digital Era

1. **Leak**: A proprietary image sent to 10 people got leaked out
   ➔ Who leaked the info?
2. **Source**: Picture of a heavily guarded xPhone7 prototype showed up on web
   ➔ Is it a real photo or a graphic rendition? Who in the company took it using his/her camera?

Metadata in header can be forged 😞

**Exploit Intrinsic Fingerprints via Component Forensics**

- 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 proc. chain beyond multimedia

**Intrinsic Traces Representing Group Properties**

- **“Digital / software”** components of device or processing system
- Ensemble properties of analog components:
  - e.g. statistical noise profile of sensors

![Diagram](image-url)
**Photography vs Computer Graphics?**

- $P_F$ – prob. of false alarm
  - (% of photographic images misclassified)
- $P_D$ – prob. of correct decision
  - (% of computer generated images classified correctly)

**Intrinsic Traces Link to Individual Devices**

- Individual variation from “analog” part of sensors
  - “Unreproducible” properties due to manufacturing variability
- **Challenges** to overcome
  - Picture content variability, post-processing, anti-forensics, etc.

**Matching Sensor Noise via Correlation Metrics**

- Measure similarity by normalized cross-correlation (NCC)
  - NCC gives a sharp peak at the right alignment of right match
  - May include weights from measurement reliabilities
- Robust peak measurement
  - Normalize with “ambient” correlation values (Fridrich et al.)

**Tampering Detection**

Explore intrinsic fingerprints left by various processing modules

- To infer the algorithms and parameters employed in various components of the digital device and processing systems
- New traces or vanished old traces suggests potential post-camera operations

![Diagram showing tampering detection process](image-url)
Explore More …

- Early years’ research:
  
  **Special Issue on Digital Forensics**
  by IEEE Signal Processing Magazine (March 2009)
  Edited by E. Delp, N. Memon and M. Wu
  
  and a concurrent special issue in
  IEEE Security & Privacy Magazine


- New DARPA “MediFor” program

---

**Role Play as Sherlock Holmes in our Digital Era**

1. **Leak:** A proprietary image sent to 10 people got leaked out
   ➔ Who leaked the info?

2. **Source:** Picture of a heavily guarded xPhone7 prototype showed up on web
   ➔ Is it a real photo or a graphic rendition? Who in the company took it using his/her camera?

3. **When/Where:** an audio clip with incriminating words showed up
   ➔ were its content and recording time true as claimed?

---

**Ubiquitous Forensic Fingerprints from Power Grid**

- **Electric Network Frequency (ENF):** 50 or 60 Hz nominal
  - Change slightly due to demand-supply
  - Main trends consistent in same grid

![Power ENF signal](image-url)
**Ubiquitous Forensic Fingerprints from Power Grid**

- **Electric Network Frequency (ENF):** 50 or 60 Hz nominal
  - Change slightly due to demand-supply
  - Main trends consistent in same grid
- ENF can be “seen” or “heard” in sensor recordings
  - Power grid influences electronic sensing (E/M interference, vibration etc)
  - Help determine recording time/location, detect tampering, etc.

**Tampering Detection**

- Adding a clip into original video leads to **discontinuity** in ENF
  - Clip insertion can also be detected by comparing the video ENF signal with the power ENF at corresponding time

**“Forensic Binding” of Audio and Visual Tracks**

- **High correlation** of ENFs in audio & video captured at same time
  - => can extend to synch multiple media streams
- **Anti-Forensic Study:** possible to remove narrow-band ENF; but much harder to tamper/transplant a valid ENF w/o being caught

**From Time Stamps to Location**

- Match with ENF references over times + grids
  - Verify or exhaustively search for the matching location on grid level

Source: US Grid image is from InTech online
Explore Machine Learning to Infer Location

- **Inter-Grid location-of-recording** estimation from sensing signals containing ENF traces
  - Identified useful features for average 94% accuracy on audio

From Time Stamps to Location

- **Match with ENF references over times + grids**
  - Verify or exhaustively search for the matching location on grid level

Can ENF Pinpoint to Locations Within a Grid?

- **Main trend of ENF** is known to be the same in a grid
- **“Microscopic” traces**
  - Aggregated effect of local events and propagations from elsewhere
- **Our multi-location studies** in U.S. east and west grids
  - Relate pairwise ENF correlations between query and anchor points with geographic and wireline distances

ENF in Historical Recordings

- **Two ENFs** may appear in digitized tape recordings
  1) original ENF; and
  2) ENF at time of digitization
  => Provide digital preservation guidelines to better utilize invisible traces
- **Distortions and artifacts**
  - Drifting; low SNR; etc.
- **Ongoing**: create a historical ENF database
  - Timestamp recordings of historic importance
**Speed Restoration: ENF as Intrinsic Freq. Reference**

Before Restoration

After Restoration

**Immersive Media: Synch Streams via ENF in Audio**

**Demo-1:**
Videos in Gym

(different viewing angles)

**Demo-2:**
Videos at different locations of Lab Building

Video after synchronization

2 synched stopwatches (as ground truth)

---

**ENF Research & References**

**Estimate ENF Signal**
(instantaneous freq.): 
Robust, high resolution; 
Exploit harmonics
SPL’13, APSIPA ’12, 
ACM MM’11, TIFS’13

**Visual Modality:**
Handle aliasing 
– exploit rolling shutters; 
Handle motion
TIFS’13, ICIP’14, 
ACM MM’14 Immersive Media

**Modeling & Analysis:**
Statistically modeling of 
ENF signals; 
Anti-Forensics. 
WIFS’12, CCS’12, twoTIFS’13

**Novel Applications:**
Location & integrity; 
Stream alignment; 
Digital humanity (historic audio)
ICASSP’12-13, WIFS’13 / TIFS’15, 
iConf’14, ACM MM’14 Immersive

---

“Information Forensics: An Overview of the First Decade,”
by M. Stamm, M. Wu, K.J.R. Liu,

**MediFor:** Newly Launched DARPA Program on media forensics aiming at restoring “Seeing is Believing”

See also Special Issue on Digital Forensics by IEEE Signal Processing Magazine (March 2009) Edited by E. Delp, N. Memon and M. Wu; and a concurrent special issue in IEEE Security & Privacy Magazine
THANKS to many who paved ways ...

Include joint work with collaborators:
K.J. Ray Liu, Wade Trappe, Jane Wang, Hong Zhao; Kari Klaus, Douglas Oard.

Min Wu: Info Forensics & Media Security
• Provide assurance for proper use of content
  – Answer who has done what, when and how.
• Cross-disciplinary and balancing theory & practice
  – Analytic modeling for fundamental understanding
  – Design effective and efficient algorithms with synergy from signal proc., comm, machine learning, crypto …

Include joint work with graduate & undergrad students

Min Wu (UMD): Multimedia Information Forensics