Multimedia Fingerprinting for Tracing Traitors

Min Wu ~ 吳旻

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, Wade Trappe, Jane Wang, and Hong Zhao.

Digital Fingerprinting for Tracing Traitors

- Leak of information poses serious threats to government operations and commercial markets
  - e.g., pirated content or classified document
- Promising countermeasure: robustly embed digital fingerprints
  - Insert ID or “fingerprint” (often through robust watermarking) to identify each user
  - Purpose: deter information leakage; digital rights management
    - provide post-delivery protection complementary to encryption
  - Challenge: imperceptibility, robustness, tracing capability

Applications of Digital Fingerprinting

1. Trace classified info in government/military and companies
2. Commercial use for digital rights management (DRM)
   - Copyright industry – $500+ Billion business ~ 5% U.S. GDP

- Successful case by Hollywood for tracing leaked movie
  - Use invisible watermark as fingerprints to protect screener/preview movies
  - Alleged Movie Pirate Arrested thanks to fingerprints (Jan. 2004)
  - Hollywood is seeking collusion-resistant technologies to combat against sophisticated pirates in the coming years

Information Forensics, Multimedia Security & Content Protection

Real World Scene
Captured by what device? What technologies are used?
Photos, maps, documents, audio, video …
How to efficiently and securely deliver contents to multi users?
Who leaked the info? Have content been tampered?

- Information forensics
  - Embed digital fingerprints in multimedia for forensic analysis & traitor tracing;
  - Non-intrusive forensic techniques, e.g. media hash and image-based camera identification;

- Digital watermarking and data embedding
  - Develop embedding techniques, and analyze attacks and countermeasures for content protection and fraud prevention;
  - Novel cross-disciplinary applications, e.g. data embedding in computer program for enhancing run-time performance while preserving instruction-set architecture;

- Extension of security & multimedia research to communication issues
  - Dynamic resource allocation for wireless video streaming;
  - Secure communications in group and sensor network scenarios.
**Collusion Attacks by Multiple Users**

- **Collusion**: A cost-effective attack against multimedia fingerprints
  - Users with same content but different fingerprints come together to produce a new copy with diminished or attenuated fingerprints
  - Fairness: *Each colluder contributes equal share through averaging, interleaving, and nonlinear combining*

![Diagram of collusion attacks](image)

**Embedded Fingerprinting for Multimedia**

- **Embedded Fingerprinting**
  - **Customer’s ID**: Alice
  - **Multimedia Document**
  - **Digital Fingerprint**
  - **Fingerprinted Copy**
  - **Embed**
  - **Distribute to Alice**

**Multi-user Attacks**
- **Fingerprinted doc for different users**
- **Collusion Attack** (to remove fingerprints)
- **Unauthorized redistribution**

**Traitor Tracing**
- **Extract Fingerprints**
- **Suspicious Copy**
- **Identify Traitors**
- **Alice, Bob, ...**

**Road Map on Media Fingerprinting Research**

- **Robust Embedding**
  - **Orthogonal Fingerprints**
  - Represent how many users? Resist how many colluders?
  - “most effective” collusions?

- **Correlated Fingerprints**
  - **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

**Key Issues**

- **How to construct fingerprints?**
  - Identify individual users
  - Resist multi-user collusion

- **How to embed fingerprints in media data?**
  - Tailor to the media characteristics for robustness and imperceptibility

- **Interaction between choices of fingerprint construction, embedding, and detection**
**Background: Robust Watermark / Data-Embedding**

- Embedding domain tailored to media characteristics & application requirement

**Detection of Spread Spectrum Watermark**

- Detection can be formulated as a hypothesis testing problem
- Optimal detector can be calculated from assumptions on distortion (host media and noise from attacks).
- If distortion is i.i.d. $N(0, \sigma_d^2)$ then optimal detector is a correlator:

$$H_0: \langle (x + noise), w \rangle$$
$$H_1: \langle y + noise, w \rangle = \langle w + (x + noise), w \rangle$$

or

$$H_0: \langle (x + noise) - x, w \rangle = \langle noise, w \rangle$$
$$H_1: \langle y + noise - x, w \rangle = \langle w + noise, w \rangle$$

**Example: Orthogonal Fingerprint for Curves/Graphics**

- Use (approx.) orthogonal sequences as FPs for different users
- Detection by looking for high correlation result
- Embed in parametric modeling domain of curve
- Perturb B-spline parameters according to spread spectrum sequences

**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
**Resistant to Collusion Attacks**

- 2-User Interleaving Attack
- 5-User Averaging Attack
- Also survive combination attacks of collusion + print + scan

**Issues Limiting Collusion Resilience of OrthoFP**

1. Orthogonal fingerprints get attenuated with more colluders
   - leads to reduced detection statistics corresponding to colluders
2. Probability of false alarm increases as total # of users increases
   - the detector need to correlate with more orthogonal fingerprint signals
   - false alarm depends on maximum detection statistics with innocent users ~ it becomes larger as # users increases

Two design metrics: (1) # colluders to resist, (2) total # users to assign FP to.

**Group-Oriented Forensics**

- Overcome the limitations of orthogonal fingerprinting
  - Recall: orthogonal FP treats everybody equally
  - Orthogonal strategy has to suspect more to nail down a true colluder
- Colluders often come together in some foreseeable groups
  - Due to their geographic, social, or other connections
- Our approach: design users’ FP in a correlated way
  - Cluster users into groups based on prior knowledge
    - Intra-group collusion is more likely than inter-group
  - Add correlation to same group to help narrow down suspicion group
    - A fingerprint signal contains user part $e_{ij}$ and group part $a_i$

$$s_j = \sqrt{1 - \rho} e_{ij} + \sqrt{\rho} a_i$$

where \(\{e_{ii}, ..., e_{iM}, a_i\} \sim iid \ N(0, \sigma_n^2 I_N)\)

**Two-Stage Detection Scheme**

- Basic idea: first identify groups containing colluders, then identify colluders within each possible guilty group
- ROC Curves $P_d$ vs. $P_{fp}$ under different collusion settings
  - Constraint: equal energy $E[\|y_t\|^2] = E[\|y_0\|^2] = \|s\|^2$

$$s = \sqrt{1 - \rho} e + \sqrt{\rho} a$$
Road Map on Media Fingerprinting Research

- **Robust Embedding**
  - Orthogonal Fingerprints
  - Represent how many users?
  - Resist how many colluders?
  - “most effective” collusions?

- **Correlated Fingerprints**
  - Group-based FP to exploit Attacker Behavior

- **Coded Fingerprints**
  - 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

Fingerprinting Multimedia: Coded vs. Non-coded

- **Spread-spectrum embedding**
  - Provide a good tradeoff on security, imperceptibility, and robustness

- **Choice of modulation schemes**
  - Orthogonal modulation
    - \( w_j = u_j \)  
    - # of fingerprints
    - # of orthogonal spreading seq.
  - (Binary) coded modulation
    - \( w_j = \sum_{i=1}^{B} b_j u_i \)
    - # of fingerprints
    - >> # of orthogonal spreading seq.

  - Support of spreading sequences: overlapped (CDM) or not (TDM)
  - Extend to non-binary codes
    - Use fewer and shorter spreading sequences to represent users;
      - May have efficient detection in computation and bookkeeping

Coded Fingerprinting: Prior Work and New Issues

- **Collusion-secure codes** for generic data
  - Abstract collusion model “Marking assumptions” (Boneh-Shaw ‘95)
    - Colluders can only change the symbols where the corresponding values in their copies are different (or data may become useless)
  - Binary codes are too long to be reliably embedded
    - Require millions bits for 1000 users
  - Focus on tracing one of the colluders

- **New issues with multimedia**
  - “Marking assumptions” may no longer hold …
  - Some code bits may become erroneously decoded due to strong noise and/or inappropriate embedding
  - Can choose appropriate embedding to prevent colluders from arbitrarily changing the embedded fingerprint bits
  - May desire to identify as many colluders as possible

Spreading + Combinatorial Coded Fingerprint

- **Explore unique issues associated with multimedia**
  - Consider interaction b/w fingerprint encoding, embedding, & detection
  - Use appropriate embedding to prevent arbitrary manipulation on code

- **Build correlated fingerprints in two steps**
  - Use antipodal coded modulation to embed fingerprint codes
    - Via orthogonal spread spectrum sequences
    - Shared bits get sustained and used to identify colluders
  - Binary Anti-collision fingerprint codes resist up to K colluders
    - Any subset of up to K users share a unique set of code bits
16-bit ACC for Detecting ≤ 3 Colluders Out of 20

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

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

Embed fingerprint via HVS-based spread spectrum embedding in block-DCT domain

Collude by Averaging

Uniquely Identify User 1 & 4

Anti-Collusion Codes via Combinatorial Design

- Simplified assumption (can be relaxed by using soft detection)
  - Fingerprint codes follow logic-AND operation after collusion
- ACC code via combinatorial design
  - Balanced Incomplete Block Design (BIBD)
  - K-resilient AND ACC code: binary codeword \(\{c_1, c_2, \ldots, c_n\}\)
    - Logical AND operation of any combination of up to K codevectors is distinct from “AND” of any other combinations of up to K codevectors
- Shorter code length: \(O(n^{0.5})\) dozens-to-hundreds bits for 1000 users
  - Prior art by Boneh-Shaw ~ millions bits
- Detection via joint code extraction and colluder identification
  - Explore soft info. than hard thresholding

Thoughts Learned and Issues Raised from ACC

- Benefit to consider coding + embedding + detection together
  - Appropriate embedding layer can confine attackers’ strategy
  => Joint coding & embedding (analogous to cross layer design in comm.)
- Correlation vs. Separation between fingerprints
  - Most prior work tried to separate fingerprints
    - via orthogonal seq., large minimum code distance, ...
  - BIBD ACC shows the potential benefit of using correlation to help catch colluders
  => How much correlation / separation is good for traitor tracing?
- How to further conserve “resources”? (esp. nec. for video application)
  - Reduce the number and length of spreading sequences
  - Shall we embed same or different FP in different frames for video?

Illustration of ECC based Fingerprinting

Host Signal

\[ A \quad B \quad C \quad D \]

Codebook

\[ A \quad C \quad B \quad A \quad D \quad C \]

User 1 \(\rightarrow\)

Colluded

User 2 \(\rightarrow\)

Interleaving Collusion

\(\text{Correlation detector}\)

\[ D \quad C \quad B \quad A \quad B \quad C \]

Extracted Code

\(\text{Colluded code}\)

\(\text{Guilty codeword}\)

\(\text{Innocent codeword}\)

\[ D > \left(1 - \frac{1}{c}\right)L \]

\(\text{Alice}\)

\(\text{Bob}\)

\(\text{x}\)

\(\text{z}\)
Explore Error Correcting Codes for Fingerprinting

- Limited collusion-resistance by conventional ECC FP
  - Finite alphabet is double-edge sword
    - Enable efficient FP construction, detection, and distribution;
      symbol based FP codes are attractive for frame-based media (e.g., video)
    - Code structure confines # colluder to resist and/or total # users
  - Example: 32-ary R-S code of length 30  
    resist 5 colluders out of 1024 users
  - Each symbol needs about 10^3 feature samples to carry it reliably.

- Propose two new joint coding and embedding techniques
  - Permuted subsegment embedding (with soft detection)
  - Group based joint coding and embedding (GRACE)

- Main Results
  - Overcome code-level limitation and enhance collusion resistance
  - Provide better trade-off b/w collusion resistance and efficient detection
  - Demonstrates advantages by joint coding-embedding in fingerprint design

Permed Sub-segment Embedding: Example

\[ \beta = 3 \]

Fingerprint Sequence

\[ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 \]

Random Permutation

\[ 3, 1, 7, 8, 14, 15, 16, 10, 5, 13, 12, 11, 9, 6, 4, 2 \]

Interleaving Collusion

Inverse permutation

Conventional ECC FP  
PSE based ECC FP

A Unified Framework

Unified view of fingerprint construction using code modulation

1. Orthogonal fingerprinting:
   - Equivalent code matrix \( B = \text{identity matrix} \)
   \[ w_j = \sum_{i=1}^{B} b_{ij} u_{ij} \]

2. Coded fingerprinting: a compact way to represent users
   - Boneh-Shaw’s and error correction code based construction
     - Combinatorial based ACC code: take advantage of shared bits

3. General correlated fingerprints
   - Allow real-valued codes such as in group-oriented fingerprinting

Key: how to strategically introduce correlation and separation

between fingerprints to capture individual & multiple colluders

Conclusions on Anti-Collusion FP Studies

- Important to design anti-collusion fingerprint for multimedia
  - Collusion is a cost-effective attack against fingerprinting
  - Anti-collusion fingerprints can allow us trace traitor and deter unauthorized information leakage
- Good news: a promising framework by joint coding and embedding
  - We can tolerate about a few dozens colluders (for image document)
  - We can accommodate more users through coding
- Challenges
  - One may find enough colluders to circumvent the system => further research will lead to better designs and increase collusion resistance
  - Large scale challenge: collusion-resilient FP for millions users?

Ref on Multimedia Fingerprinting Research @ UMD

- Analytic understanding on linear and nonlinear collusions:
- Analyzing the limit on collusion resistance by orthogonal fingerprinting:
- Leveraging prior info. on collusion pattern via group fingerprinting:
- Proposing a new framework promoting the joint coding, embedding, and detection, with a demonstration through new combinatorial based ACC
- Joint coding and embedding approach for ECC-based fingerprinting
- Data hiding in curves with application to fingerprinting maps and innovative protection of geospatial data