Today’s topic is about Collusion Attack

Before starting, let us...
Recall of collusion attack

**Collusion:** A cost-effective attack against multimedia fingerprint

- 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

---

It is said in [6]: with colluders employ multiple-input single-output linear shift invariant (MISO-LSI) filtering plus additive Gaussian noise, if the fingerprints are independent and have identical statistical characteristics, the optimal MISO-LSI attack involves each user weighting their marked documents *equally* prior to adding noise [6].
Why not consider non-collusion attack?

- Spread spectrum embedding are robust to non-collusion attacks [1], [2]

- You may argue about geometric distortion?
  - Indeed, such as Rotation, Scaling, Shift, Cropping…, they are believed to be effective!
  - These attacks are also being studied, possibly handled by
    - Synchronization or registration
      - adding a small set of salient points [3]
      - registering to the original image (non-blind detection) and invert the distortion.
        The alignment error can be approximated by additive noise [4]
    - Invariant watermark, extensive search, etc…[5]

- Therefore, a category of papers concentrate on collusion attack!
Robust MC-CDMA-Based Fingerprinting Against Time-Varying Collusion Attacks

Cha and Kuo, IT Information Forensics and Security, 2009

2009.12.09

余其曄 Chi-Yeh Yu
National Taiwan University
Overview of MC-CDMA, Hara, ICM 1997 (1)

Direct sequence code division multiple access (DS-CDMA), Qualcomm 1989

History: In July 1985, seven industry veterans came together in the den of Dr. Irwin Jacobs' San Diego home to discuss an idea. Those visionaries — Franklin Antonio, Adelia Coffman, Andrew Cohen, Klein Gilhousen, Irwin Jacobs, Andrew Viterbi and Harvey White — decided they wanted to build QUALity COMMunications and outlined a plan that has evolved into one of the telecommunications industry's greatest start-up success stories: Qualcomm Incorporated.
1993, three types of multiple access combining CDMA and OFDM were proposed:

- Multi-carrier CDMA (MC-CDMA) by Linnartz, Yee (UC Berkeley)
- Multi-carrier DS-CDMA
- Multi-tone CDMA (MT-CDMA)
Overview of MC-CDMA, Hara, ICM 1997 (3)

Comparison

Insight: MC-CDMA receiver the received signal is combined, in a sense, in the frequency domain, therefore, the receiver can always employ all the received signal energy scattered in the frequency domain. This is the main advantage of the MC-CDMA scheme over other schemes.

Multi vs. single-carrier

Pros:
- robust to frequency selective fading
- longer symbol duration ‡ easier time synchronization

Cons:
- Non-constant envelope with large PAPR ‡ sensitive to nonlinear amplification
- Narrow frequency carrier spacing‡ sensitive to frequency offset
Collusion Attack Previous Works (1)

- **Category: Independent Fingerprint**
    - Pseudo noise sequence
    - Orthogonal modulation
Collusion Attack Previous Works (2)

- Category: Coded Fingerprint
    - In orthogonal modulation, detection complexity from $O(n) \leq O(K\log(n/k))$
    - BIBD Anti-collusion code
    - CDMA sequence sets satisfying the Welch Bound Equality (WBE), with sphere decoding
    - Joint coding and embedding
MC-CDMA Fingerprint Abstract

Problem Formulation
- Watermark contains user message which is encoded from user id
- Design a watermark to detect collusion attack, and the watermark is not limited to a certain embedding method

Motivation for (MC-)CDMA
- CDMA allows multiple user transmission with no interference from each other, provided perfect timing synchronization
- MC-CDMA provides better time synchronization, and robust equalization
- If watermark is designed as MC-CDMA signal, which modulates the user message, then traitor is traced by demodulating the MC-CDMA signal for the user id

Contribution
- Collusion identification (by correlation and decoding to get BEP)
- Collusion weight estimation (by pilot symbols)
- Collusion detection (by MC-CDMA equalization)
MC-CDMA Fingerprint Generation (1)

Block Diagram

User Message Encoding

<table>
<thead>
<tr>
<th>Scheme</th>
<th>$B_{id}$</th>
<th>$B_r$</th>
<th>$B_m$</th>
<th>$B_n$</th>
<th>$B_f$</th>
<th>$L$</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>24</td>
<td>8</td>
<td>32</td>
<td>8</td>
<td>256</td>
<td>$2^{23} \times 8 = 2^{26}$</td>
</tr>
<tr>
<td>B</td>
<td>256</td>
<td>0</td>
<td>256</td>
<td>1</td>
<td>256</td>
<td>$2^{255}$</td>
</tr>
<tr>
<td>C</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>256</td>
<td>256</td>
<td>$2^8 = 256$</td>
</tr>
</tbody>
</table>
MC-CDMA Fingerprint Generation (2)

- Code Spreading by $S_N$

\[
S_N = S_2 \otimes S_{N/2} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} S_{N/2} & S_{N/2} \\ S_{N/2} & -S_{N/2} \end{pmatrix}
\]

where $N = 2^r$ ($r \geq 2$) and $\otimes$ is the Kronecker product.

- IDFT transformation in MC-CDMA transmission

\[
[F]_{k,l} = \frac{1}{\sqrt{N}} e^{j(2\pi kl/N)},
\]

$k = 0, \ldots, N-1$ and $l = 0, \ldots, N-1$. 
MC-CDMA Fingerprint Colluder Identification

Two stage identification

- Despreading, then compare a threshold, and guess if it is suspect
  - With colluder
    \[ v_l = m_l \sum_{n=0}^{N-1} \lambda_l(n) + \sum_{k \in \Omega, k \neq l} IGI_{l-k} + \sum_{n=0}^{N-1} e_l(n)s_l^*(n) \]
    where
    \[ IGI_{l-k} = \sum_{n=0}^{N-1} \lambda_k(n)s_k(n)s_l^*(n) \]
  - Without colluder
    \[ v_l \approx \sum_{n=0}^{N-1} \sum_{j \notin \Omega} \lambda_j(n)s_j(n)s_l^*(n) + \sum_{n=0}^{N-1} e_l(n)s_l^*(n) \approx 0 \]

- Decoding, then compare for Bit Error Probability (BEP), and judge if it is colluder
  - By comparing the received message and the original message for each of the identified colluders, the detector can calculate BEP. The lower the BEP, the higher the confidence level
MC-CDMA Fingerprint Colluder Weight Estimation

- Using pilot symbols
  - The estimation of colluder weights can be performed in the same manner as the uplink of multi-user communication. The receiver has to have some knowledge of channels in order to apply advanced symbol detection techniques. In practice, the channel information is estimated using pilot symbols.
MC-CDMA Advanced Colluder Detection (1)

- MRC detector
- PIC detector
MC-CDMA Advanced Colluder Detection (2)

- MRC detector

\[
v_k = \sum_{n=0}^{N-1} \left( \sum_{t \in \Omega} m_t \lambda_l(n) s_l(n) \right) \tilde{h}_k^*(n) s_k^*(n)
\]

- PIC detector

\[
v_k^{(0)} = m_k \sum_{n=0}^{N-1} |\lambda_k(n)|^2 + \sum_{t \in \Omega, t \neq k} m_t \sum_{n=0}^{N-1} \lambda_l(n) s_l(n) \tilde{h}_k^*(n) s_k^*(n) + \hat{e}_k
\]

\[
v_k^{(c+1)} = v_k^{(c)} - \sum_{t \in \Omega, t \neq k} \text{sgn} \left[ \text{Re} \left\{ v_l^{(c)} \right\} \right] \sum_{n=0}^{N-1} \lambda_l(n) s_l(n) \tilde{h}_k^*(n) + \hat{e}_k
\]
Performance

- Identified colluder vs. Number of colluder
Performance

- Comparison of PN and WH spreading code

PN as spreading code will be affected by IGI more severely
Performance

- Number of iteration in PIC

When colluder becomes more and more, eliminate other colluder is helpful to detect current colluder.
Performance

Consider Noise effect and Quantization effect

Fig. 18. Performance of the MC-CIDMA-based fingerprinting system on audio (A) and video (V) data under the impact of (a) noise and (b) quantization.
Reflection

Consult the author by email:

Question

- HW code is generally used in MC-CDMA system, but is there any side-effect in using it for finger-print? For example, I would be worry if the attackers know the HW code set and try to despread all of them and hack the fingerprint by canceling each of them.

Reply

- I think this thought might be out of scope in this paper, but it is very good question. This side-effect must be rigorously studied in the steganalysis area, and the trade-off relationship between security and robustness should be researched in several security evaluations.
Proposal

Three methods to prevent hack (malicious elimination of fingerprint)

- Random Permutation before embedding
- Multiplied with scrambling code
- Using random orthogonal code instead of HW code

Basic approach by gram-schmidt algorithm

Efficient approach by subgroup algorithm

Diaconis & Shahshahani (1987) later generalized as the "subgroup algorithm" (in which form it works just as well for permutations and rotations). To generate an \((n + 1) \times (n + 1)\) orthogonal matrix, take an \(n \times n\) one and a uniformly distributed unit vector of dimension \(n + 1\). Construct a Householder reflection from the vector, then apply it to the smaller matrix (embedded in the larger size with a 1 in the bottom corner).
Further Analysis (1)

- Recall concept from “Improved Spread Spectrum: A New Modulation Technique for Robust Watermarking”, Malvar, ITSP 2003
  - Traditional SS only use fixed scaling parameter for watermark
    - It doesn’t consider the cover work interference, which is dominant interference in watermark detection
    - Scaling parameter should consider original image
  - Improved scaling parameter in linear form
    - Optimum scaling for minimum watermark detection BEP
    - Optimum scaling for largest AWGN noise sustained \( \pm \) max noise tolerance gain
    - Improved further with limited distortion
  - Improved scaling parameter in non-linear form (optimum ISS)
Further Analysis (2)

From ISS paper,

(1) if we use embedding as: $s = x + bu$
    with channel model: $y = s + n$

    then, for correlation based detection, the error probability $p = \frac{1}{2} \text{erfc} \left( \frac{\sigma_u^2 N}{2(\sigma_x^2 + \sigma_n^2)} \right)$

(2) if we use new embedding as: $s = x + (\alpha b - \lambda x)u$

    the error probability $p = \frac{1}{2} \text{erfc} \left( \frac{N \sigma_u^2 - \lambda^2 \sigma_x^2}{2(\sigma_n^2 + (1-\lambda)^2 \sigma_x^2)} \right)$
Further Analysis (3)

n Apply to MC-CDMA fingerprint:

By Parseval's theorem

\[ \frac{1}{N} \sum_{k=0}^{N-1} F(k)^2 = \sum_{n=0}^{N-1} f(n)^2, \text{ where } F(k) \text{ is DFT of } f(n), \text{ both of length } N \]

In our system

\[ \sigma_u^2 = \frac{1}{N} \sum_{k=0}^{N-1} \sigma_u^2 = \sum_{n=0}^{N-1} \sigma_u^2 = N \sigma_u^2 \]

(1) if we use embedding as: \( s = x + bu \)

\[ p = \frac{1}{2} \text{erfc}\left( \sqrt{\frac{\sigma_u^2}{2(\sigma_x^2 + \sigma_n^2)}} \right) \Rightarrow \sigma_u^2 > 2(\text{erfc}^{-1}(2p))^2(\sigma_x^2 + \sigma_n^2) \]

(2) if we use new embedding as: \( s = x + (\alpha b - \lambda x)u \)

\[ p = \frac{1}{2} \text{erfc}\left( \sqrt{\frac{\sigma_u^2 - \lambda^2 \sigma_x^2}{2(\sigma_n^2 + (1-\lambda)^2 \sigma_x^2)}} \right) \]

Insight: MC-CMDA use average power of watermark as a criterion to achieve a certain error probability \( p \)
Reference


Thank you!

chiyehyu@gmail.com