Multimedia Forensics for Traitors Tracing

K. J. Ray Liu

Department of Electrical and Computer Engineering

University of Maryland, College Park

Acknowledgement: Wade Trappe, Z. Jane Wang, Min Wu, and Hong Zhao.

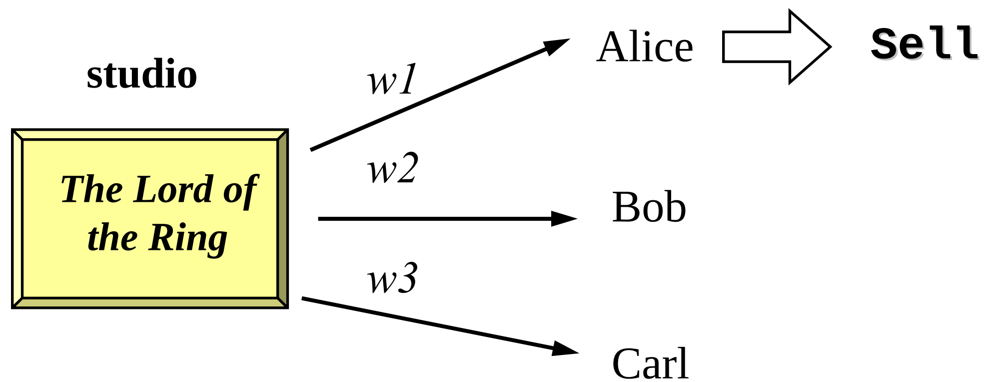
Talk Overview

- Digital Fingerprinting and Traitors Tracing
  - Motivation of digital fingerprinting
  - Background: e.g. additive spread spectrum embedding
  - Collusion attacks: collusion schemes, analysis and comparison
- Orthogonal Fingerprinting and variations
  - Capacity of tracing colluders by using orthogonal modulation
  - Group-oriented fingerprinting
- Coded Fingerprinting
  - Anti-collusion codes and code modulated fingerprints
  - Colluder identification schemes
- Traitors Behavior Dynamics in Collusion

Digital Fingerprinting and Traitors Tracing

Digital Fingerprinting and Tracing Traitors

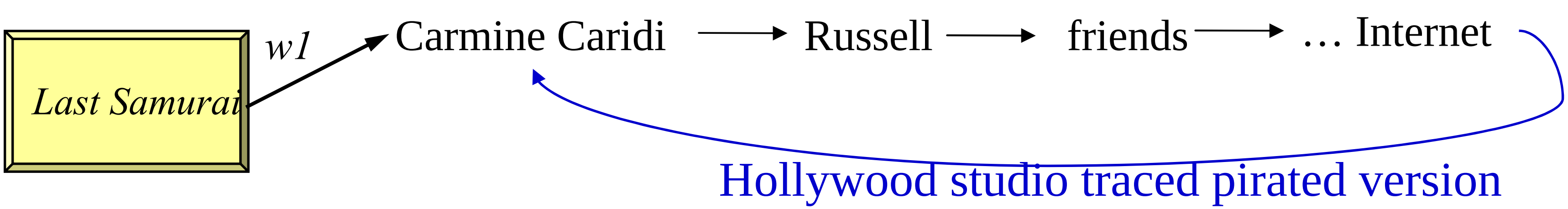
- Leak of information as well as alteration and repackaging poses serious threats to government operations and commercial markets
  - e.g., pirated content or classified document



- Promising countermeasure: robustly embed digital fingerprints
  - Insert ID or "fingerprint" (often through conventional watermarking) to identify each user
  - Purpose: deter information leakage; digital rights management(DRM)
  - Challenge: imperceptibility, robustness, tracing capability

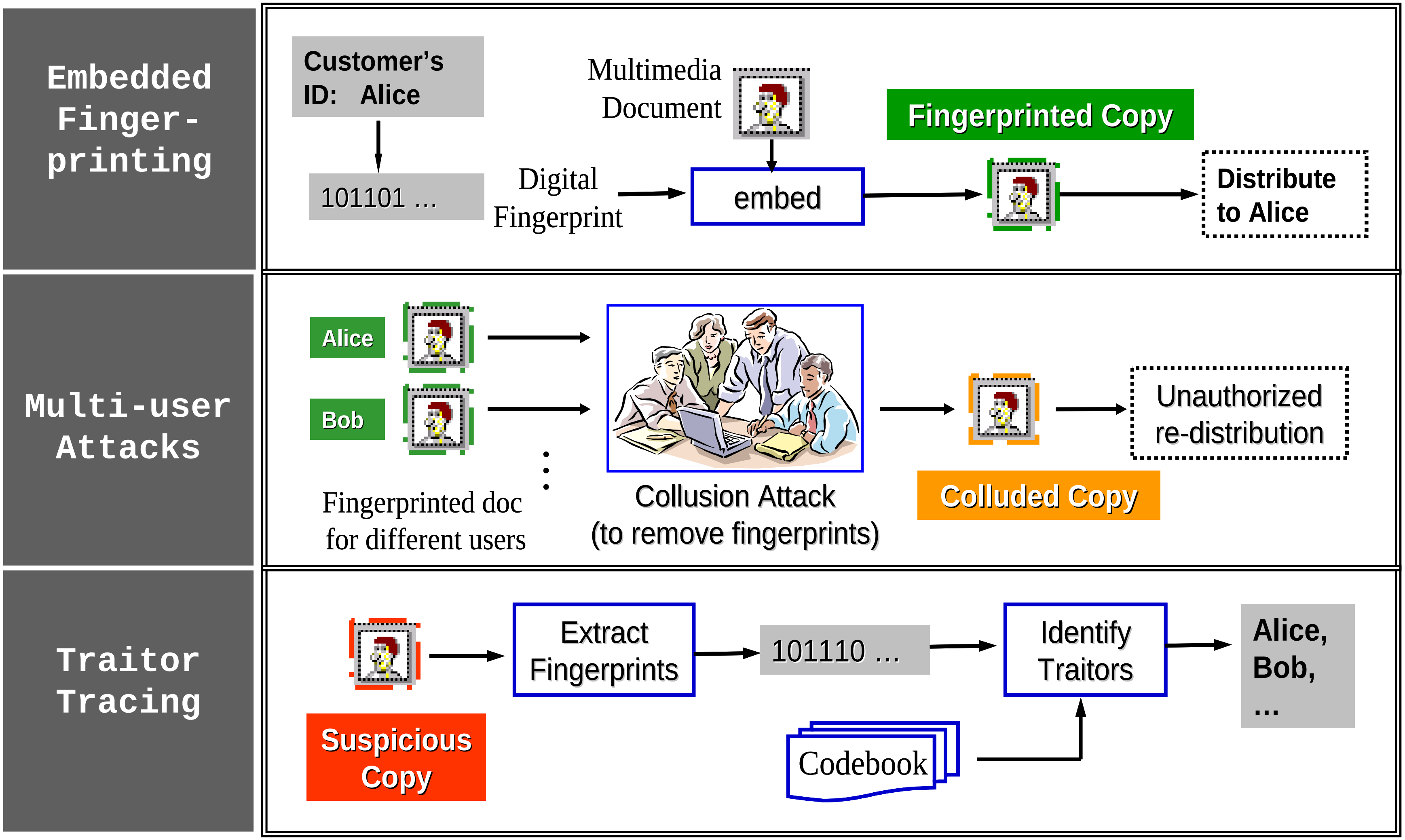
Case Study: Tracing Movie Screening Copies

- Potential civilian use for digital rights management (DRM)
  - *Copyright industry – $500+ Billion business ~ 5% U.S. GDP*
- Alleged Movie Pirate Arrested (23 January 2004)
  - A real case of a successful deployment of 'traitor-tracing' mechanism in the digital realm
  - Use invisible fingerprints to protect screener copies of pre-release movies

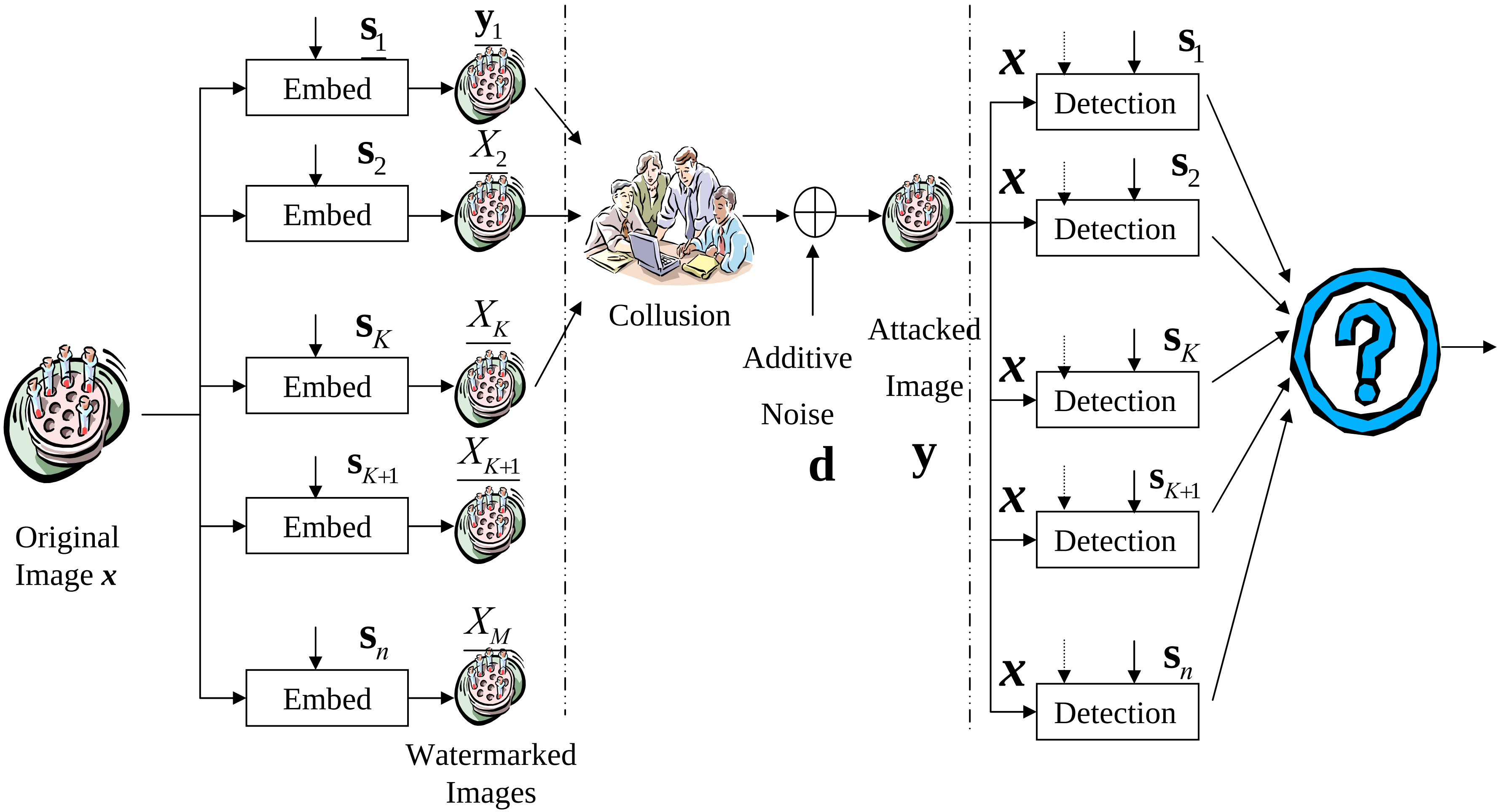


http://www.msnbc.msn.com/id/4037016/

Embedded Fingerprinting for Multimedia



Model



Original Image x
Embed
Embed
Embed
Embed
Embed
$\mathbf{s}_1$
$\mathbf{s}_2$
$\mathbf{s}_K$
$\mathbf{s}_{K+1}$
$\mathbf{s}_n$
$\mathbf{y}_1$
X_2
X_K
X_{K+1}
X_M
Watermarked Images
Collusion
Additive Noise
$\mathbf{d}$
Attacked Image
$\mathbf{y}$
x
Detection
Detection
Detection
Detection
Detection

Modulation Scheme for Embedded Fingerprinting

- Typical watermark-to-noise (WNR) ratio: -20dB in blind detection, 0dB in non-blind detection.
- Choice of modulation schemes:

Orthogonal modulation $\mathbf{s}_j = \mathbf{u}_j$

# of fingerprints = # of ortho. bases

(Binary) coded modulation $\mathbf{s}_j = \sum_{i=1}^{v} b_{ij} \mathbf{u}_i$

for $b_{ij} \in \{0,1\}$ or $b_{ij} \in \{\pm 1\}$

# of fingerprints >> # of ortho. bases

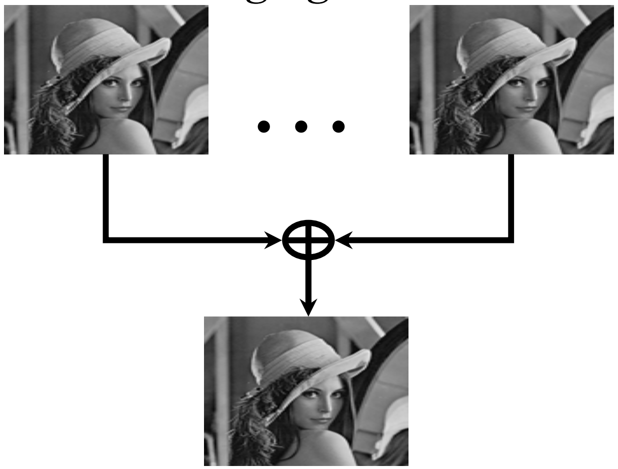
Performance Criteria

- Capture one: The major concern is to identify at least one colluder with high confidence without accusing innocent users.
- Capture more: The major concern is to catch more colluders, possibly at a cost of accusing more innocents. Tradeoff between the expected fraction of colluders that are successfully captured and the expected fraction of innocent users that are falsely placed under suspicion.
- Capture all: The goal is to capture all colluders with a high probability. Tradeoff between the efficiency rate which describes the amount of expected innocents accused per colluder and the probability of capturing all colluders.

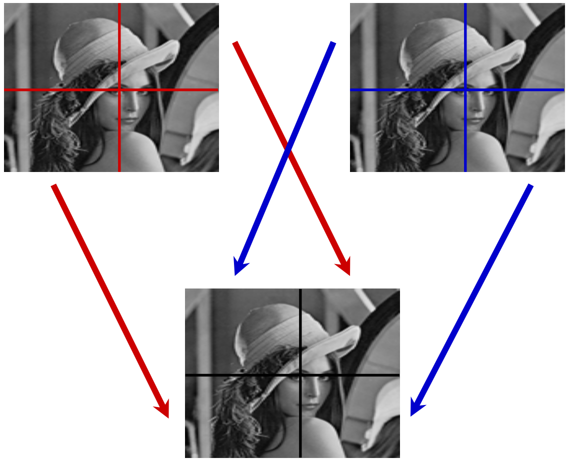
Collusion Attacks by Multiple Users

- Collusion: A cost-effective attack against multimedia fingerprints
- Result of fair collusion:
  - Each colluder contributes equal share through averaging, interleaving, and nonlinear combining
  - Energy of embedded fingerprints may decrease

Averaging Attack



Interleaving Attack



Collusion Attacks (cont'd)

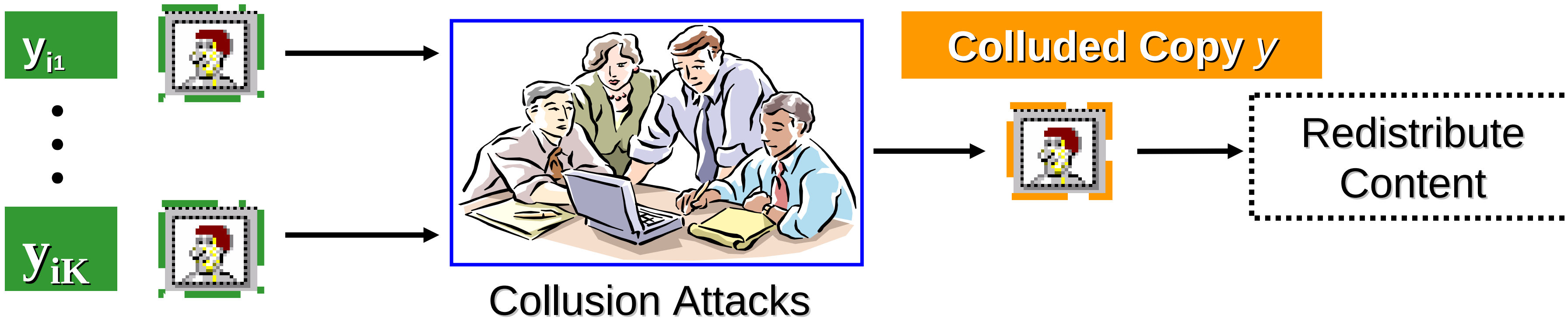
- Though linear collusion is simple and effective, in fact, for each component, the colluders can output any value between the minimum and maximum values, and have high confidence that such spurious value is within the range of JND. Therefore,

  We conduct studies on non-linear attacks

  - Few previous works: H. Stone suggested several nonlinear collusion attacks

☞ *What is the best attack for collusions?*

Nonlinear Collusion Attacks



- Assumption
  - Colluders pick value in the range of min and max of $\{y_j(i)\}_{j \in S_C}$
  - FP embedding and collusion attack are in the same domain
- Order statistics based collusion: for each component i, i=1,…,N,

$$y(i) = x(i) + \alpha \cdot JND(i) \cdot g(s_j(i))_{j \in S_C}$$

$$V(i)^{ave};\quad V(i)^{\min};\quad V(i)^{\max};\quad V(i)^{median}$$

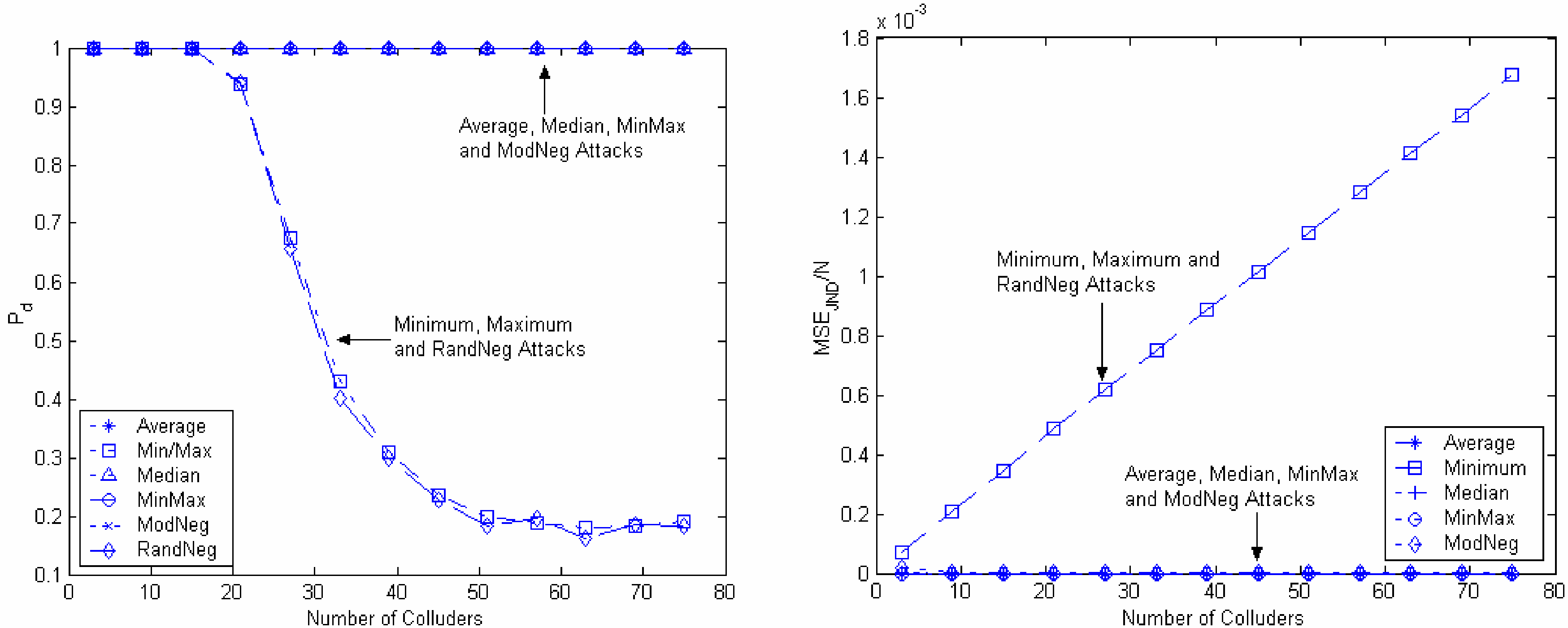
$$V(i)^{\min\max} = average\left(V(i)^{\min}, V(i)^{\max}\right)$$

$$V(i)^{\mathrm{mod}\,neg} = V(i)^{\min} + V(i)^{\max} - V(i)^{med}$$

$$V(i)^{randneg} = \begin{cases} V(i)^{\min} & \text{w.p. } p \\ V(i)^{\max} & \text{w.p. } 1-p \end{cases}$$

p=0.5 in randomized negative attack and is indep. of {s(i)}

Example: use T_n Statistic



– Assume the host signal has N=10,000 embeddable coefficients and there are a total of n=100 users. $P_{fp}=10^{-3}$ is fixed and i.i.d. fingerprints ~N(0,1/9).

– Randomized negative attack is the most effective attack (without normalizing the distortion level introduced by different attacks).

– Minimum, maximum and randomized negative attacks introduce much larger distortion in the colluded copy

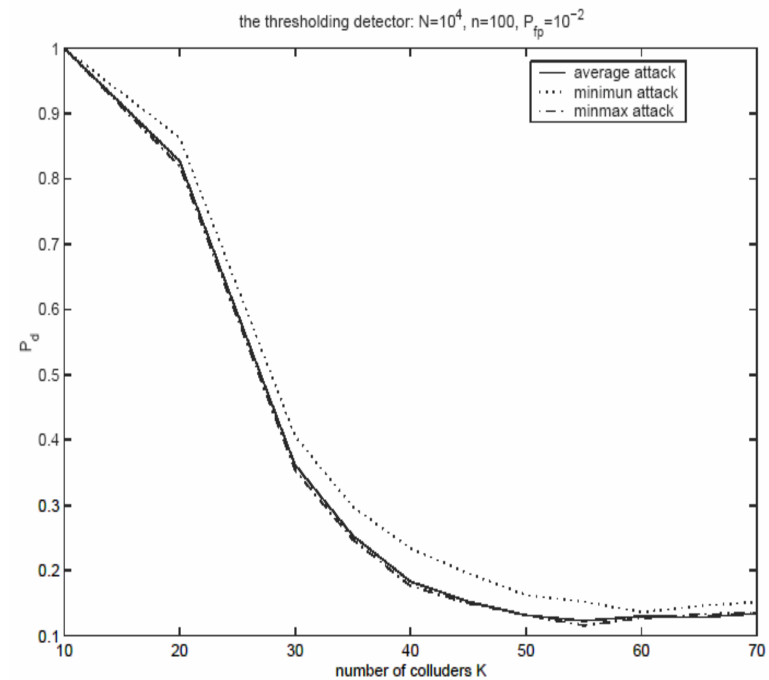
Averaging and Nonlinear Collusions (cont'd)

Thresholding detector is robust to different types of attacks: *averaging collusion; order-statistic based (min, max, …)*

Rationale from detector's view point

Detection statistics of averaging and many nonlinear collusions are (approx.) Gaussian distributions with same mean

=> Yield similar performance if the overall distortion is the same.



$$g(\mathbf{s}_j, j \in S_c) + \mathbf{d}_1 \longrightarrow \text{nonlinear attacks}$$

$$\frac{1}{K}\sum_{j \in S_c} \mathbf{s}_j + \mathbf{d}_2 \longrightarrow \text{average attacks}$$

Linear vs. Nonlinear Collusion

- Conditions: - distortion introduced to the host signal is equal
- Observation: the underline model of attacks doesn't matter much from the detector point of view.
- All types of attacks can be modeled as attacks by averaging: the models

$$\boxed{\begin{aligned} \mathbf{y}_1 &= g(\mathbf{s}_j, j \in S_c) + \mathbf{d}_1 \\ \mathbf{y}_2 &= \frac{1}{K}\sum_{j \in S_c} \mathbf{s}_j + \mathbf{d}_2 \end{aligned}}$$

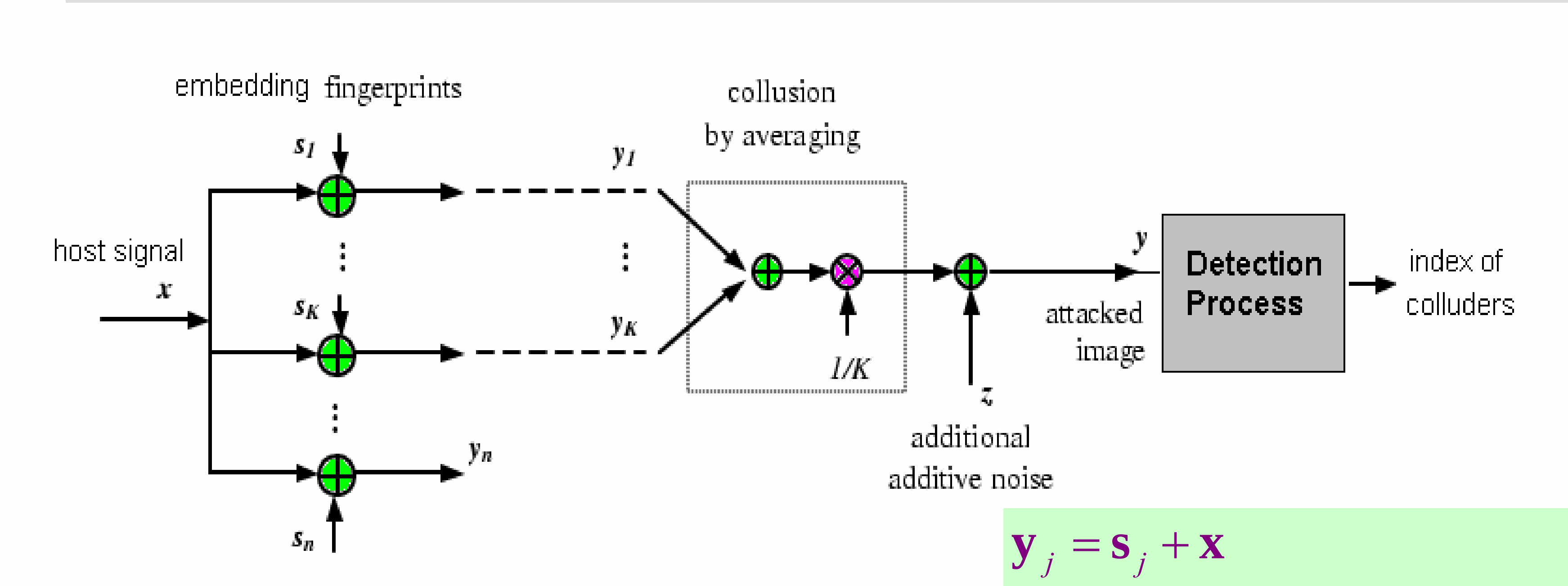
→ nonlinear attacks

→ average attacks

yield similar performance. The detector is robust to different types of attacks.

☞ *We shall focus on average attack for analysis simplicity*

Average Attack



$$\mathbf{y} = \frac{1}{K}\sum_{j\in S_c}\mathbf{y}_j + \mathbf{z} = \frac{1}{K}\sum_{j\in S_c}\mathbf{s}_j + \mathbf{d}$$

$$\mathbf{y}_j = \mathbf{s}_j + \mathbf{x}$$

$$d(i) \sim N(0, \sigma_d^2),\ \text{for } i = 1, \ldots, N.$$

$$\mathbf{s}_j \perp \mathbf{s}_k, \forall j \neq k$$

$$WNR : \eta = \|\mathbf{s}\|^2 / \|\mathbf{d}\|^2$$

Problem: determine the number of colluders K and the subset S_c

Talk Overview

- Digital Fingerprinting and Traitor Tracing
  - Motivation of DF
  - Background introduction: e.g. additive spread spectrum embedding
  - Collusion attacks: how to colluder, analysis and comparison
- Orthogonal Fingerprinting and variations
  - Capacity of tracing colluders by using orthogonal modulation
  - Group-oriented fingerprinting
- Coded Fingerprinting
  - Anti-collusion codes and code modulated fingerprints
  - Colluder identification schemes
- Summary

Orthogonal Modulation for Fingerprinting

Orthogonal Fingerprinting

- Straightforward concept and easy to implement
  - Prior works by Cox et al., Stone, Killian et al.
  - Advantage in distinguishing individual fingerprints
- Two issues limit the anti-collusion capability:
  - Orthogonal fingerprints get attenuated with more colluders
    - leads to reduced detection statistics corresponding to colluders
  - Probability of false alarm increases as the total # of users increases
- Tracing Capability: How many colluders out of how many users are sufficient to break down a fingerprinting system?
- To meet desired probability of detection (P_d) & false alarm (P_{fp})
  - We can analyze the maximum allowable colluders

=> This provides design guidelines to fingerprinting systems for applications with different protection requirements

Formulations for Max. Number of Colluders

- Thresholding detector: $$\hat{\mathbf{j}} = \arg\max_{j=1,..,n} \{T_N(j) \geq h\}$$
  (index of colluders)

- Performance criteria: $$P_{fp} = P_r\{\hat{\mathbf{j}} \cap \bar{S}_c \neq \emptyset\} = 1 - (1 - Q(h/\sigma_d))^{n-K}$$
  (Catch one:) $$P_d = P_r\{\hat{\mathbf{j}} \cap S_c \neq \emptyset\} = 1 - (1 - Q(\frac{h - \|s\|/K}{\sigma_d}))^K$$

- System requirement: $$\begin{cases} P_{fp} \leq \varepsilon \\ P_d \geq \beta \end{cases} \Longrightarrow K_{\max}$$

  – The desired P_{fp} determines the threshold for the detector

  – The desired P_d determines the maximum # of colluders allowed by the fingerprinting system

Bounds for Max. Number of Colluders

- Lower bound and Upper bound for K_{max}
  - Obtained by analytic approximations on Q-functions

$$K_{\max} \geq \min\{n, K_L\}, \text{where } K_L = \frac{\sqrt{\eta N}}{h_H} = \sqrt{\frac{\eta N}{\log(n^2/(2\pi\varepsilon^2 \log(2\pi n^2)))}} \sim \sqrt{\frac{\eta N}{\log(n)}}$$

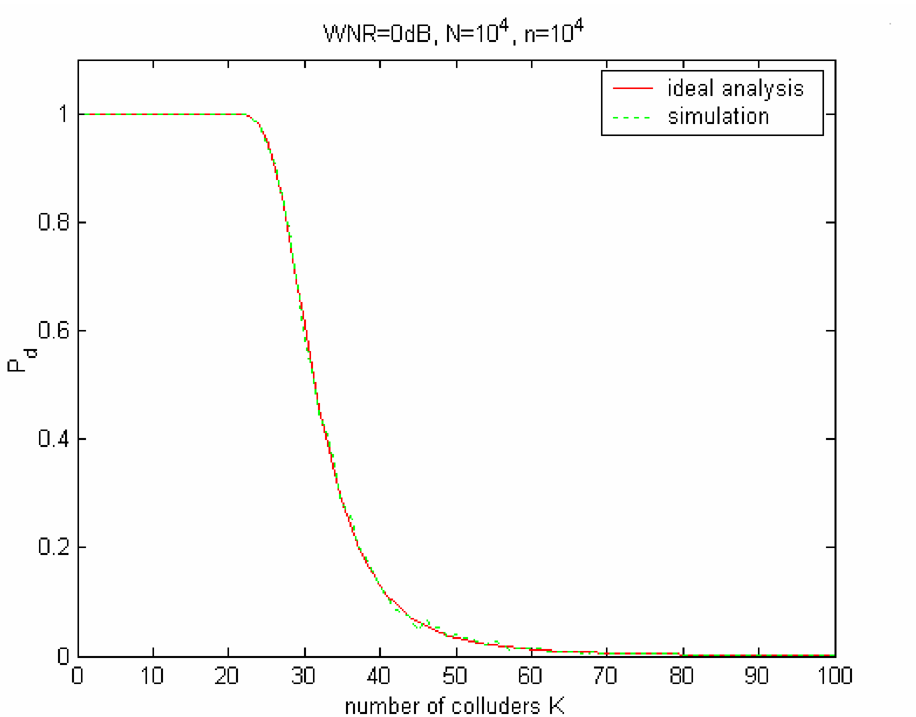
$$K_{\max} \leq \min\{n, K_H\}, \text{where } K_H = \frac{\sqrt{\eta N}}{h_L - Q^{-1}(1 - \sqrt[\tilde{K}]{1-\beta})}$$

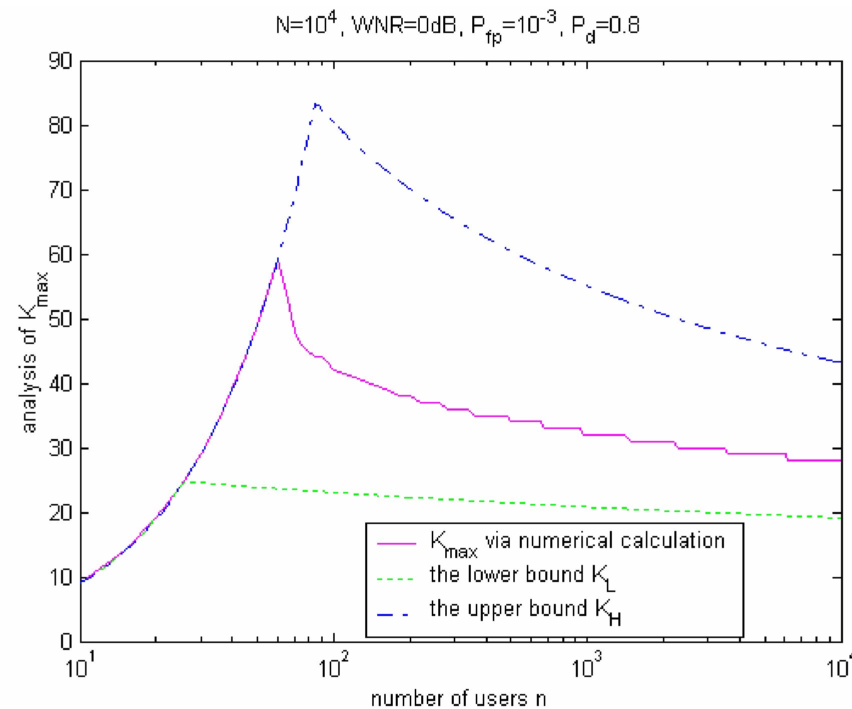
  - two auxiliary variables are defined as

$$h_L = \sqrt{\log(2\pi n^2)}$$

$$\tilde{K} = \frac{\sqrt{\eta N}}{h_L - Q^{-1}(1 - \sqrt[n]{1-\beta})}$$

Results





- Stringent requirement: correct identification of at least one colluders without falsely accusing any
- The colluder tracing capabilities for a thousand-user system is limited to several dozens colluders

Different Performance Criteria

- Catch more

the expected fraction of innocents falsely suspected: $r_i = Q(h/\sigma_d)$

the expected fraction of colluders successfully captured: $r_c = Q(\frac{h - \|\mathbf{s}\|/K}{\sigma_d})$

- Catch all

$$R = \frac{\text{the expected number of innocents captured}}{\text{the expected number of colluders captured}}$$

$$P_d = P_r(S_c \subseteq \hat{\mathbf{j}})$$

Different sets of performance criteria were studied. It seems that an orthogonal fingerprinting system can resist to the collusion attacks based on a few dozen independent copies.

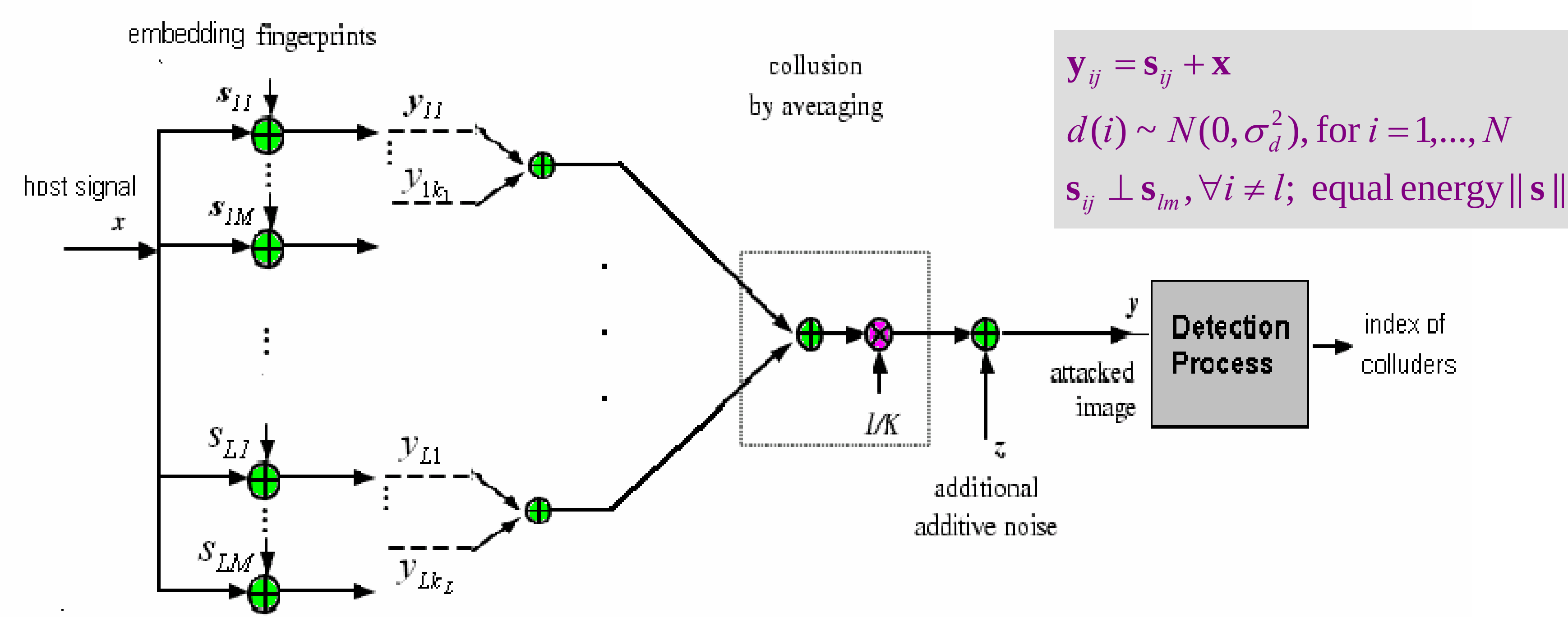
Group-Oriented Forensics

- Overcome the limitations of orthogonal fingerprinting
  - Recall: orthogonal FP treats everybody equally
- 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*
- Design of collusion-resistant fingerprinting systems:
  - Design of anti-collusion fingerprints to trace traitors and colluders
  - Design of detection schemes

Proposed Group Fingerprinting

Design of collusion-resistant fingerprinting systems:

- Design of anti-collusion fingerprints to trace traitors and colluders
- Design of detection schemes



$$\mathbf{y}_{ij} = \mathbf{s}_{ij} + \mathbf{x}$$

$$d(i) \sim N(0, \sigma_d^2), \text{ for } i = 1, \ldots, N$$

$$\mathbf{s}_{ij} \perp \mathbf{s}_{lm}, \forall i \neq l; \text{ equal energy } \|\mathbf{s}\|$$

Solution: construct intra-group FP in two parts, and use threshold detector (at desired intra-group false alarm) to avoid estimating k_i

Group Fingerprint Design

- Orthogonal modulation between groups
  - Design L orthogonal sub-systems to represent independent groups
  - M users per group => Total: n = M x L users
- Assumption: users in the same group are equally likely to collude with each other.
- Real-valued code modulation within a group
  - Introduce equal correlation within a group

    $$\mathbf{S} = [\mathbf{s}_{i1,}\mathbf{s}_{i2},\ldots,\mathbf{s}_{iM}]$$

    the correlation matrix of $\{\mathbf{s}_{i,j}\}$ is $\mathbf{R}_s$

    $$\mathbf{R}_s = \begin{bmatrix} 1 & \rho & \cdots & \rho \\ \rho & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \rho \\ \rho & \cdots & \rho & 1 \end{bmatrix}$$

  - Each fingerprint consists of common one and individual one:

$$\mathbf{s}_{ij} = \sqrt{1-\rho}\,\mathbf{e}_{ij} + \sqrt{\rho}\,\mathbf{a}_i, \text{ where } \{\mathbf{e}_{i1},\ldots,\mathbf{e}_{iM},\mathbf{a}_i\} \sim iid\ N(0,\sigma_u^2\mathbf{I}_N)$$

Two-Stage Detection Scheme

- Basic idea: first identify groups containing colluders,
  then identify colluders with each possible guilty group
- Stage-1: group detection

$$\boxed{\hat{\mathrm{i}} = \arg_{i=1}^{L}\{T_G(i) \geq h_G\}}$$

(the indices of groups)

the correlator $T_G(i) = \dfrac{(\mathbf{y}-\mathbf{x})^T(\mathbf{s}_{i1}+\mathbf{s}_{i2}+\ldots+\mathbf{s}_{iM})}{\sqrt{\|\mathbf{s}\|^2[M+(M^2-M)\rho}}$, for $i = 1,\ldots,L$

$$p(T_G(i)\,|\,K,\{k_i\},\sigma_d^2) = \begin{cases} N(0,\sigma_d^2), & \text{if } k_i = 0 \\ N(\frac{k_i}{K}\|s\|r,\sigma_d^2), & \text{o.w.} \end{cases}$$

$$r = \sqrt{[1+(M-1)\rho]/M}$$

Two-Stage Detection Scheme (cont'd)

- Stage-2: Identify colluders within each group

Define the correlator: $T_{ei}(j) = \dfrac{\sqrt{1-\rho}(\mathbf{y}-\mathbf{x})^T \mathbf{e}_{ij}}{\|\mathbf{s}\|}$, for $i = 1, \ldots, L$

$$\boxed{\hat{\mathrm{j}}_{\mathrm{i}} = \arg_{j=1}^{M}\{T_{ei}(j) \geq h\}}$$

(the indices of colluders within group i)

h does not depend on i

$$p(\mathbf{T}_{ei} \mid K, S_{ci}, \sigma_d^2) = N(\boldsymbol{\mu}_{ei}, \sigma_d^2 \mathbf{I}_M),$$

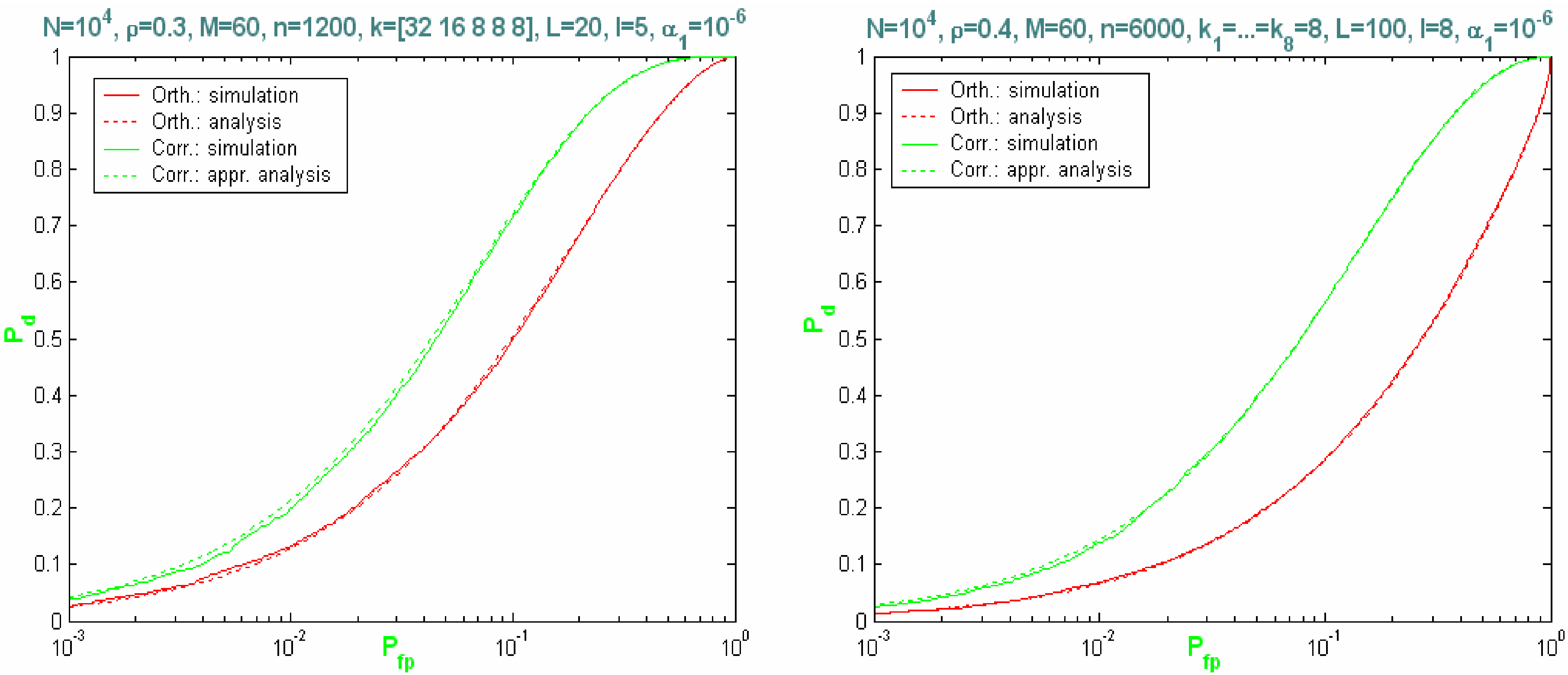
$$\text{with } \mu_{ei}(j) = \begin{cases} \dfrac{1-\rho}{K}\|\mathbf{s}\|, & \text{if } j \in \mathrm{S}_{\mathrm{ci}} \\ 0, & \text{o.w.} \end{cases}$$

$T_{ei}(j)$'s are independent

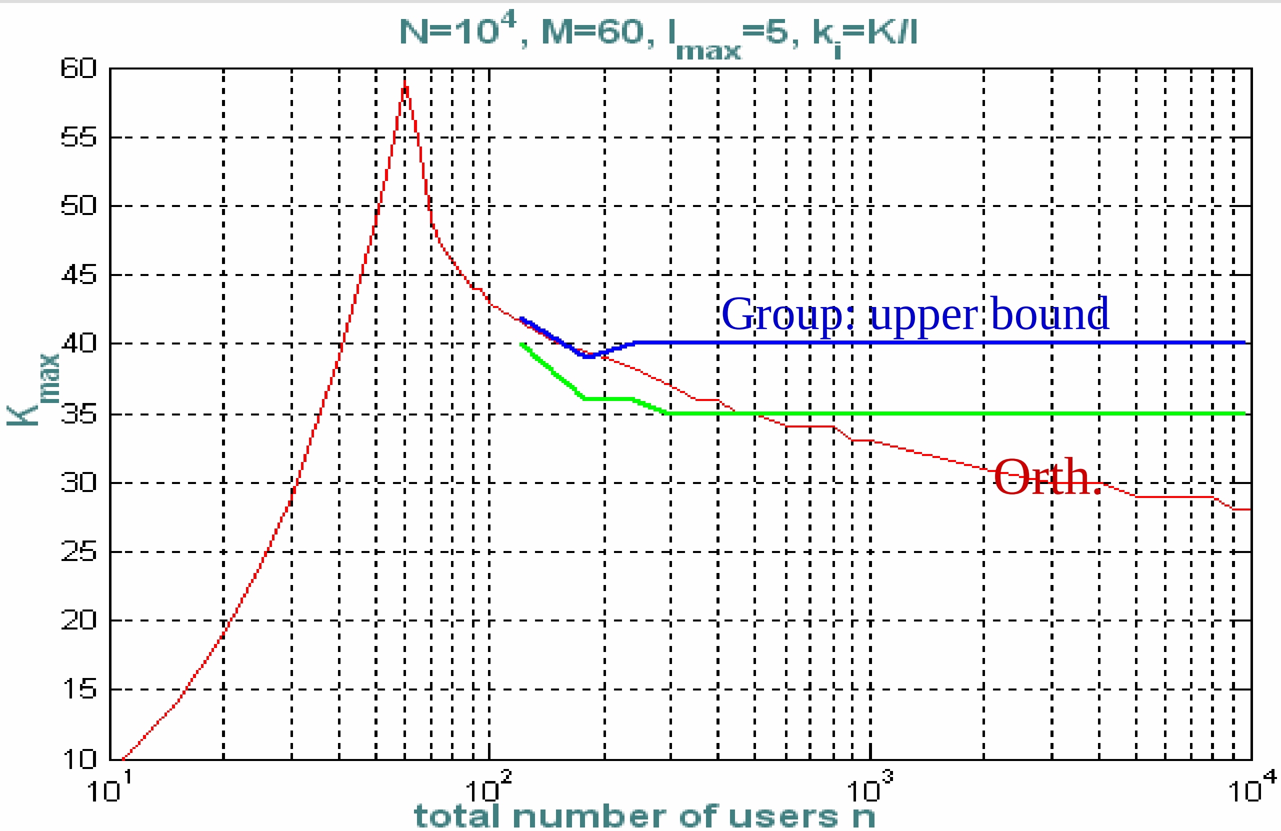
Example:

ROC Curves P_d vs. P_{fp} under different collusion settings

Constraint: equal energy $E\{\|\mathbf{y}_c\|^2\} = E\{\|\mathbf{y}_0\|^2\} \equiv \|\mathbf{s}\|^2$



Collusion Resistance of Group FP: K_{max} vs. n

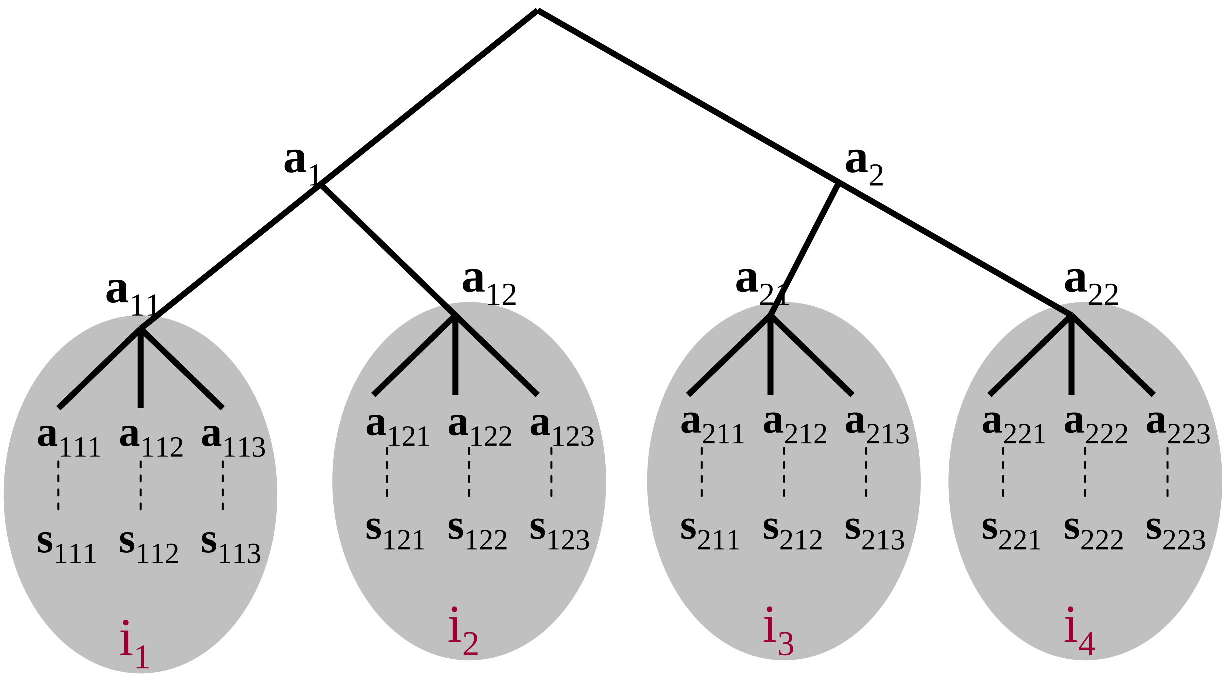


$$P_{fp} \leq 10^{-3}$$
$$P_d \geq 0.8$$

- K_{max} of the proposed scheme is larger than that of the orthogonal scheme (the solid line), when n is large.
- Difference between the lower bound and upper bound is due to the fact that k_i=K/| i| in our simulations (symmetric collusion pattern).
- The smaller the number of guilty groups, the better chance performance.

Extension: Tree-based Fingerprint Design

- Use tree structure to construct fingerprints combining shared and distinct components
- Unified view of fingerprint construction using code modulation
  - With hierarchically organized basis vectors
  - Allow for real-valued codes



Talk Overview

- Digital Fingerprinting and Traitor Tracing
  - Motivation of DF
  - Background introduction: e.g. additive spread spectrum embedding
  - Collusion attacks: how to colluder, analysis and comparison
- Orthogonal Fingerprinting and variations
  - Capacity of tracing colluders by using orthogonal modulation
  - Group-oriented fingerprinting
- Coded Fingerprinting
  - Anti-collusion codes (ACC) and code modulated fingerprints
  - Colluder identification schemes
- Summary

Coded Modulation for Fingerprinting

Coded Fingerprinting: Prior Work and New Issues

- Collusion-secure codes by Boneh and Shaw '98
  - Targeted at generic data with "Marking assumptions"
    - ~ *an abstraction of collusion model*
  - Codes are too long to be reliably embedded & extracted (Su et al.)
    - ~ *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
- Want to trace as many colluders as possible

Spreading + Combinatorial Coded Fingerprinting

- Overall idea of embedded combinatorial fingerprinting
  - Explore unique issues associated with multimedia in fingerprint encoding, embedding & detection
  - Use appropriate embedding to prevent arbitrary change on code

$$\mathbf{w}_j = \sum_{i=1}^{B} b_{ij} \mathbf{u}_i \qquad b_{ij} \in \{\pm 1\}$$

- Build correlated fingerprints in two steps
  - Binary Anti-collusion fingerprint codes resist up to K colluders
    - *any subset of up to K users share a unique set of code bits*
  - Use antipodal coded modulation to embed fingerprint codes
    - *via orthogonal spread spectrum sequences*
    - *shared bits get sustained and used to identify colluders*

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, 1, …, -1, 1, 1, 1) *User-4*

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

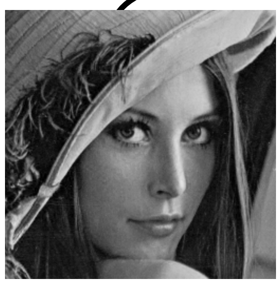
Collude by Averaging

Uniquely Identify User 1 & 4

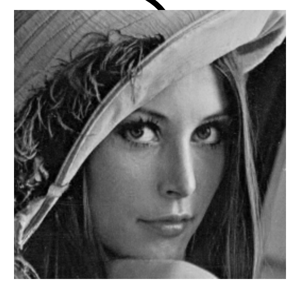
Extracted fingerprint code **(-1, 0, 0, 0, 1, …, 0, 0, 0, 1, 1, 1)**

ACC Codes Under Averaging Collusion

User 1:	-1	-1	-1	-1	1	1	1	1	1	1	1	1	1	1	1	1
User 4:	-1	1	1	1	1	1	1	1	1	1	-1	-1	-1	1	1	1
User 8:	1	-1	1	1	1	1	-1	1	-1	1	1	1	1	1	-1	1
User(1,4) Average:	-1	0	0	0	1	1	1	1	1	1	0	0	0	1	1	1
User(1,4,8) Average:	$-\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	1	1	$\frac{1}{3}$	1	$\frac{1}{3}$	1	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	1	$\frac{1}{3}$	1
After thresholding:	0	0	0	0	1	1	0	1	0	1	0	0	0	1	0	1


User-1


User-4


User-8

- Averaging of multimedia domain leads to averaging in code-domain, and corresponds to AND operation after thresholding
- Can distinguish colluded bits from sustained bits statistically with appropriate modulation and embedding, and the sustained bits are unique with respect to colluder set

Anti-Collusion Codes (ACC)

- ACC code via combinatorial design
  - Balanced Incomplete Block Design (BIBD)

    Simple Example

    ACC code via (7,3,1) BIBD for handling up to 2 colluders among 7 users

$$C = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

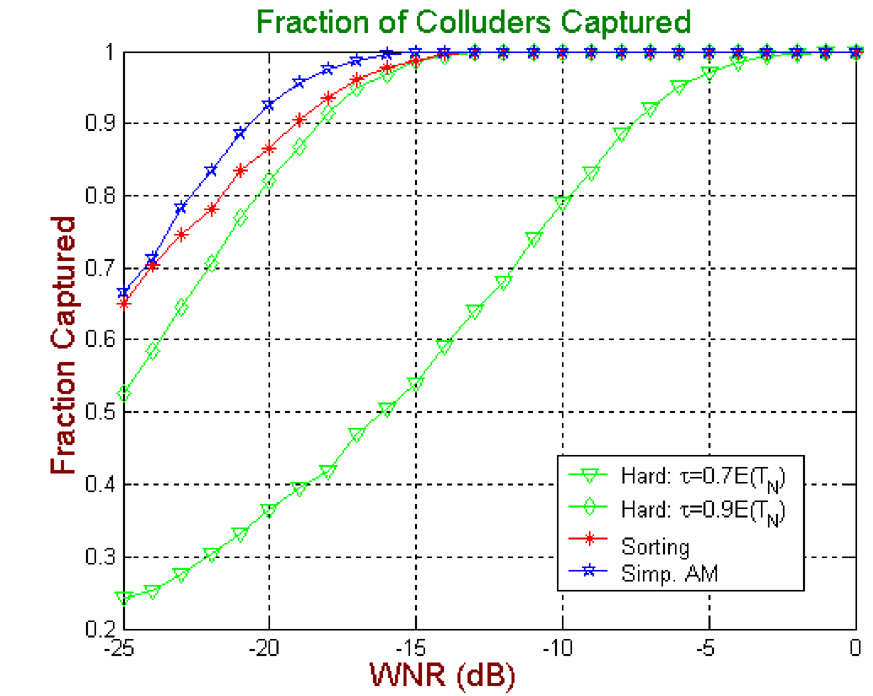
- (v,k,λ)-BIBD is an (k-1)-resilient AND ACC
  - Defined as a pair (X,A)
    - X *is a set of v points*
    - A *is a collection of blocks of* X, *each with k points*
    - *every pair of distinct points is in exactly λ blocks*
  - # blocks $n = \dfrac{\lambda(v^2 - v)}{k^2 - k}$
- Code length for n=1000 users: *O($n^{0.5}$) ~ dozens-to-hundreds bits*
  - Shorter than prior art by Boneh-Shaw O((log n)^6) ~ millions bits

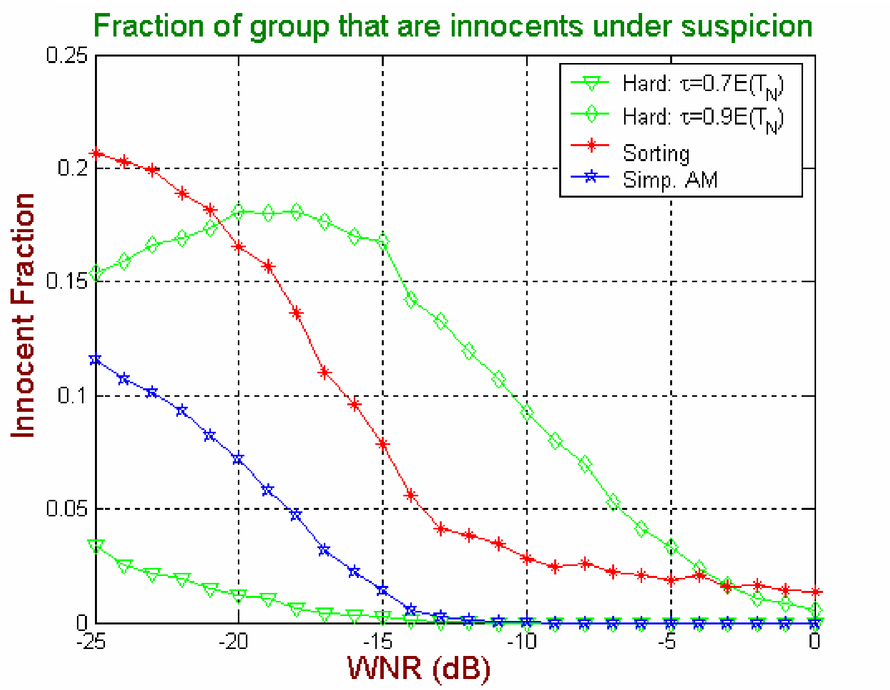
Colluder Detectors

- Hard Detection:
  - Detect the bit values and **then** estimate colluders from these values
  - Uses the fact that the combination of codevectors uniquely identifies colluders
  - Everyone is suspected as guilty and each '1' bit narrows down set

- Soft Detection:
  - Possible candidates for soft detection:
    - *Sorting: Use the largest detection statistics to optimize likelihood function to **first** determine bit values, **then** estimate colluder set.*
    - *Sequential: Iteratively update the likelihood function and **directly** identify the colluder set.*

ACC Experiment with Gaussian Signals



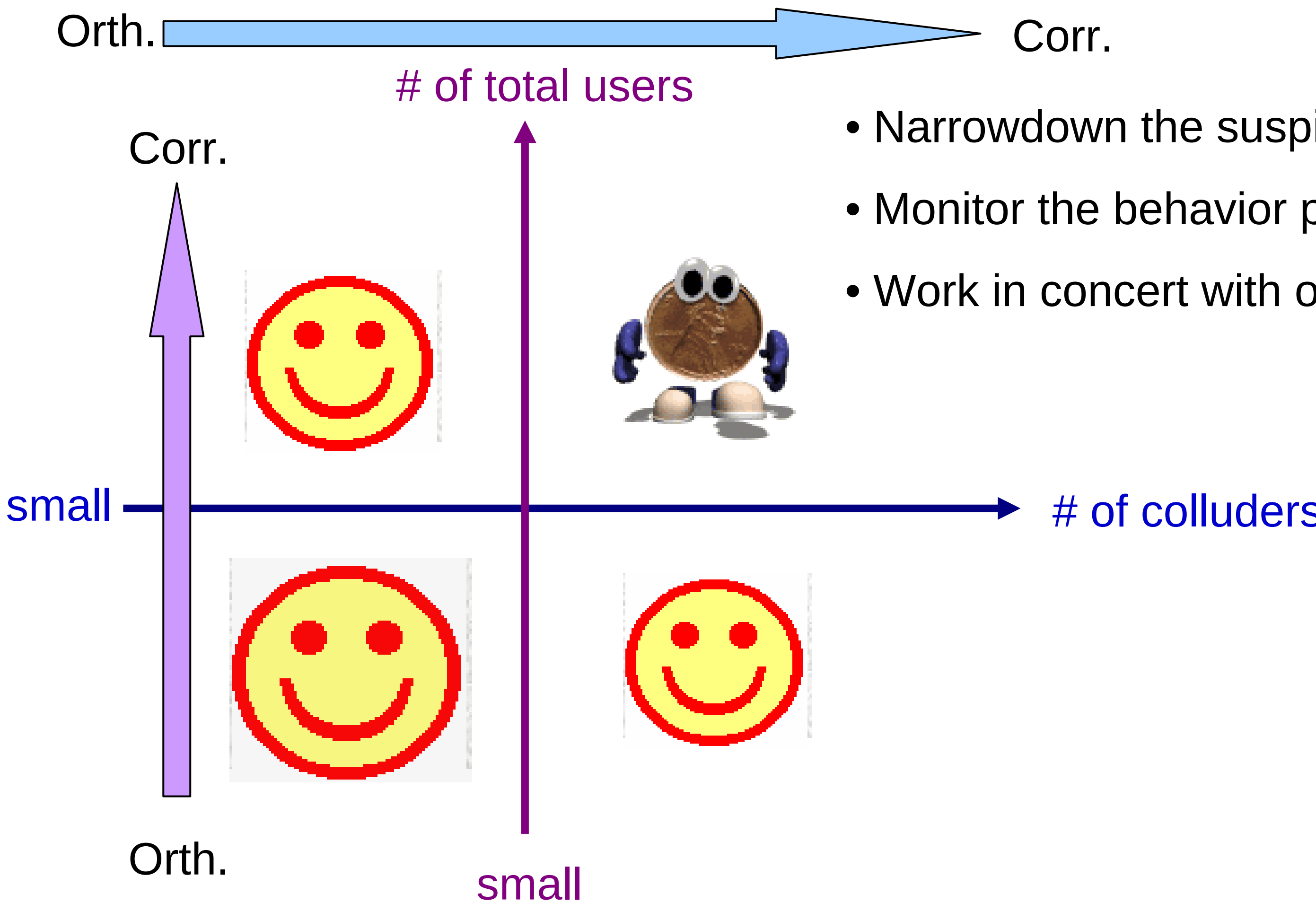


- Higher threshold captures more colluders, but suspects more innocents
- Soft decoding gives more accurate colluder identification than hard decoding
- Joint decoding and colluder identification gives better performance than separating the two steps

Summary

- Important to design anti-collusion fingerprint for multimedia
  - Collusion is a cost-effective attack against fingerprinting
  - Anti-collusion fingerprint can allow us to trace traitor and deter unauthorized information leakage
- Good news
  - We can tolerate about a few dozens colluders
  - We can accommodate more users through the ACC
- Challenge
  - One can find enough colluders to circumvent the system

Conclusions (cont'd)



- Narrowdown the suspicion size;
- Monitor the behavior pattern;
- Work in concert with other operations

- So we have more work do… tomorrow will be better!

Traitors Behavior Dynamics in Collusion

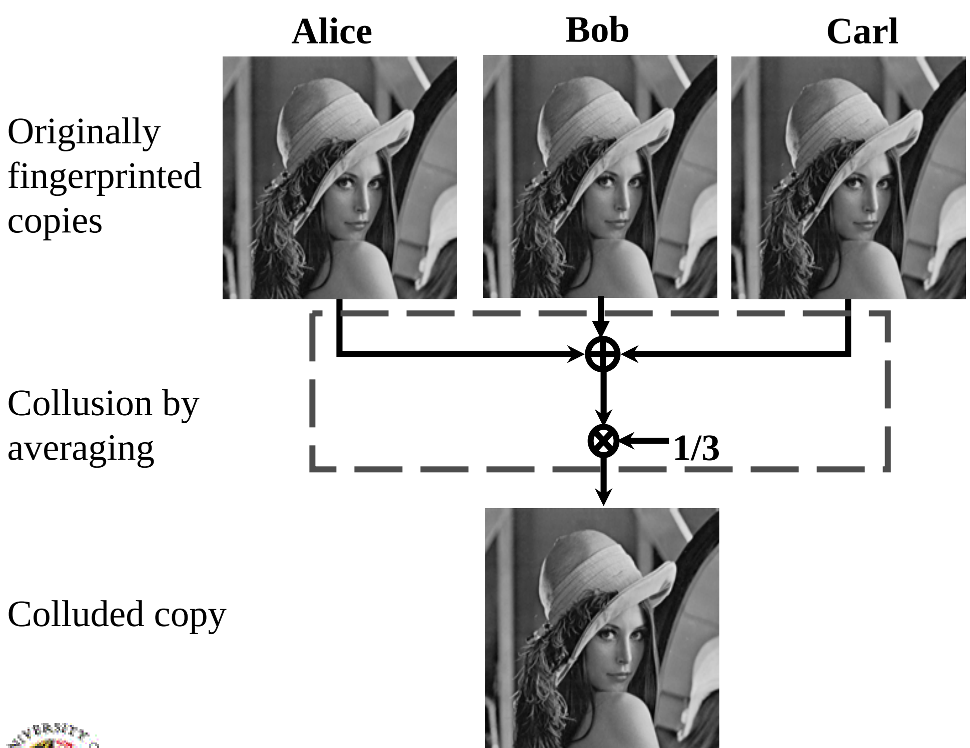
Fairness Issue in Collusion

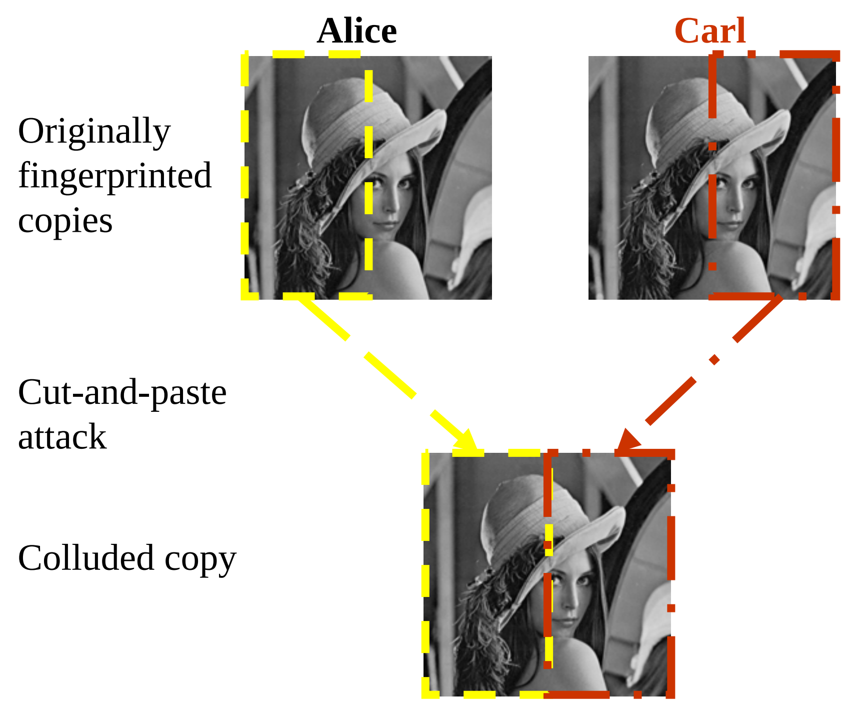
- Multi-user collusion
  - Colluders share the profit as well as the risk of being caught
- Fairness issue in collusion
  - All colluders have the same probability of being detected
- Each colluder ensures that he/she is not taking higher risk of being detected than the others

➢ **Fair-play during collusion**

Achieving the Fairness of Collusion

- Prior work: all users receive copies of the same quality
  - Examples of fair collusion: averaging, cut-and-paste
  - Reduces the energy of each contributing fingerprint by an equal ratio



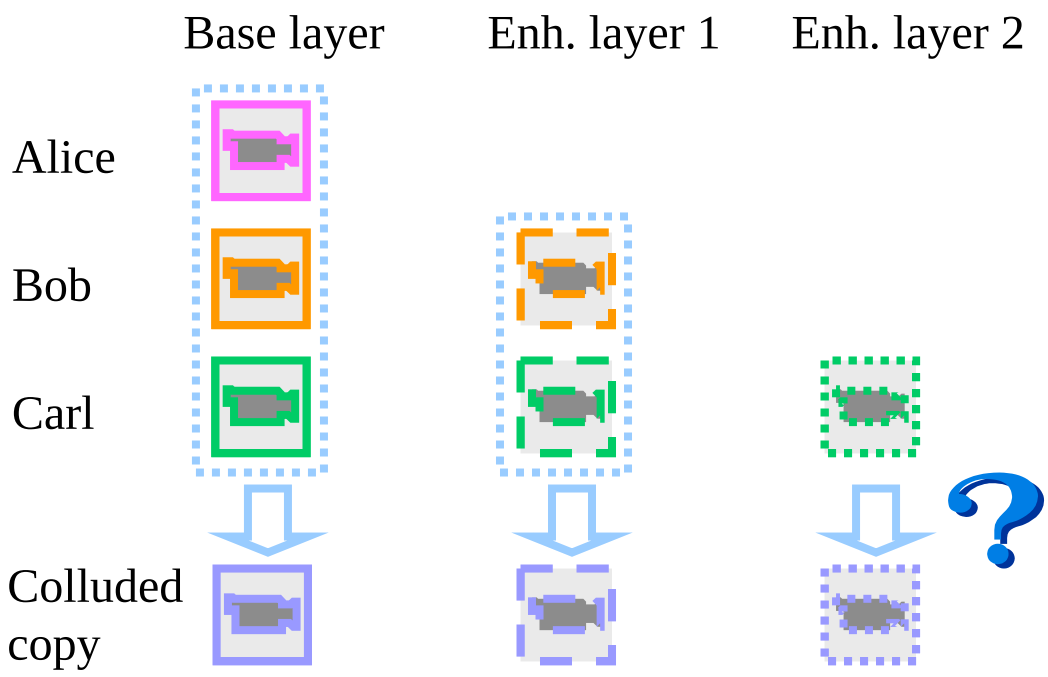


Achieving the Fairness of Collusion (cont'd)

- Scalable multimedia coding: network and device heterogeneity
  - Users receive copies of different quality
  - Temporal scalability: multiple versions of the same video with different frame rates
  - Layered coding: decompose the video into non-overlapping bit streams of different priorities

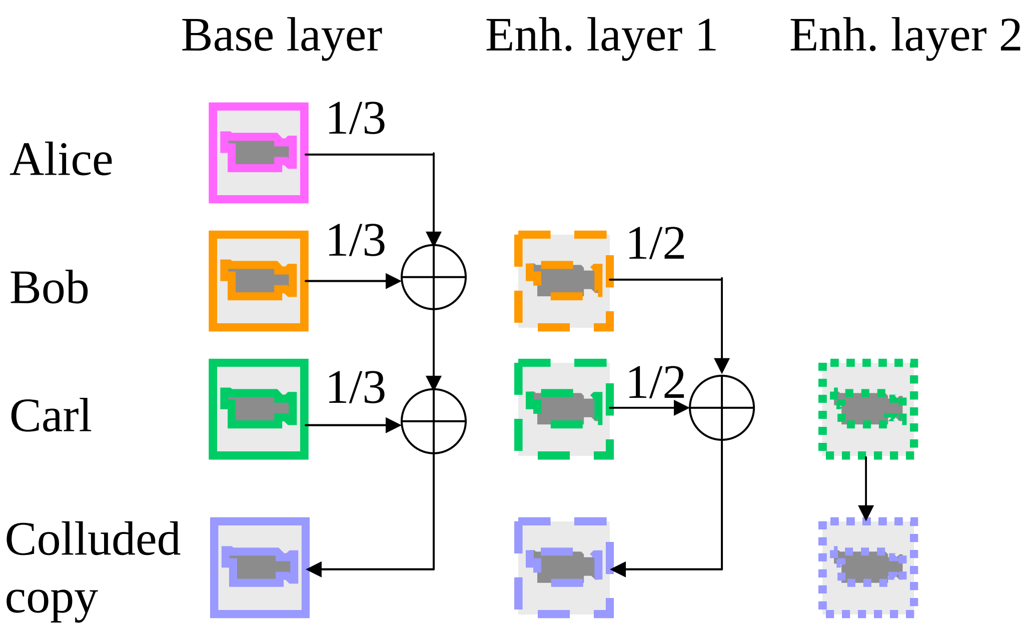
Original Video	1	2	3	4	5	6	7	8	• • •
Base layer	1				5				• • •
Enh. layer 1			3-1				7-5		• • •
Enh. layer 2		2-1		4-3		6-5		8-7	• • •

Achieving the Fairness of Collusion (cont'd)



Problem: how to achieve the fairness of collusion in scalable fingerprinting systems?

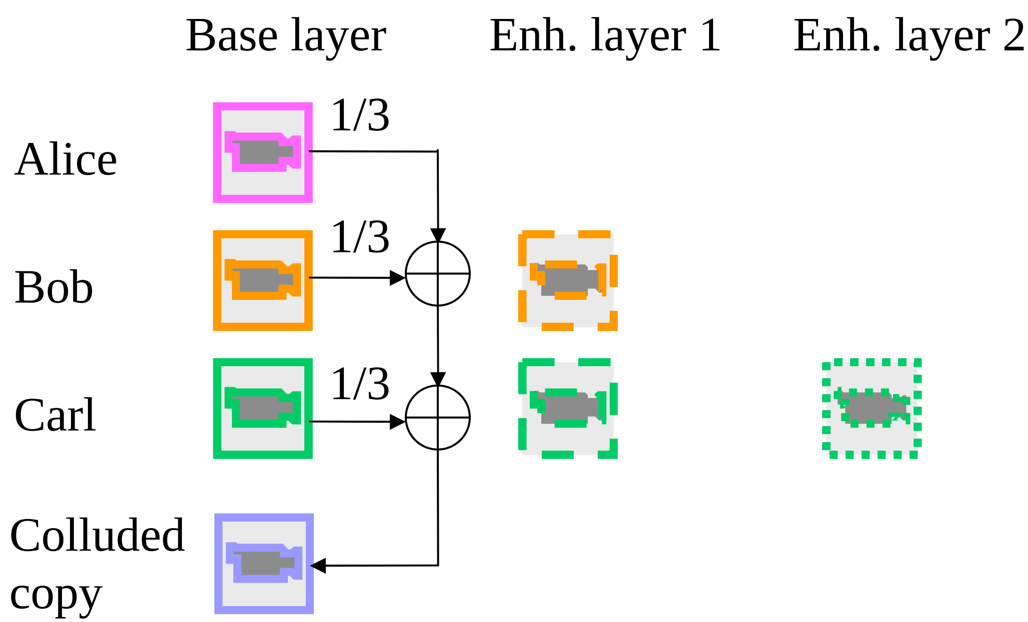
Achieving the Fairness of Collusion (cont'd)



Quality of the colluded copy High

Probability of being detected $P_{Carl} > P_{Bob} > P_{Alice}$

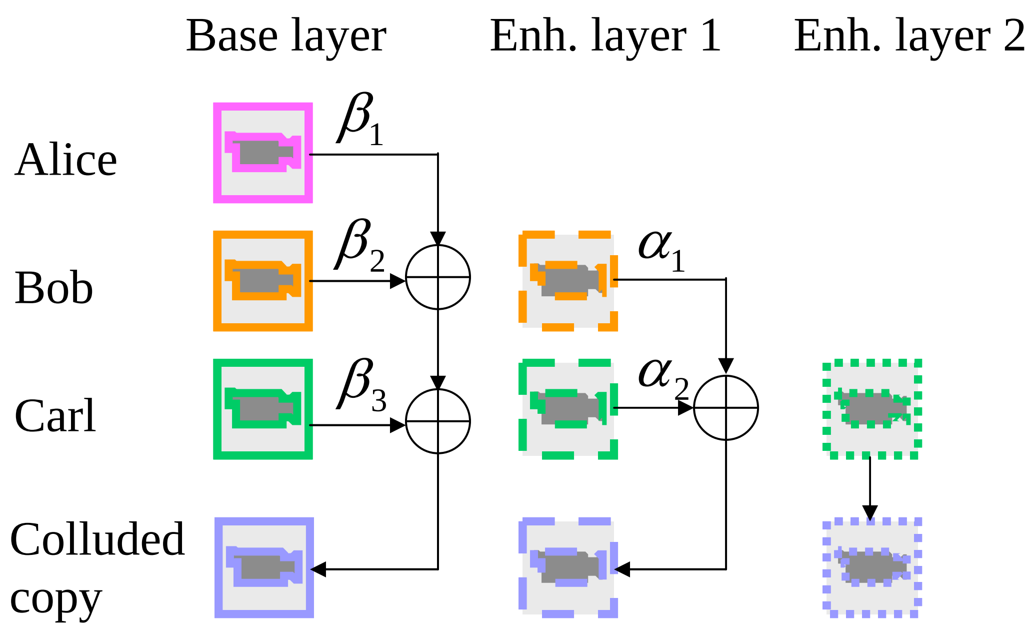
Achieving the Fairness of Collusion (cont'd)



Quality of the colluded copy **Low**

Probability of being detected $P_{Carl}=P_{Bob}=P_{Alice}$

Achieving the Fairness of Collusion (cont'd)



Quality of the colluded copy   High

Probability of being detected $P_{Carl}=P_{Bob}=P_{Alice}$

- *Choose {α,β} to guarantee the equal risk of all colluders*

Analysis of Each Colluder's Risk

- Consider a simple detector that uses fingerprints extracted from all layers collectively to identify colluder.

- The correlation based detection statistics: $T_N^{(i)} \sim N\left(\mu^{(i)}, \sigma_n^2\right)$
  - For different users, $T_N^{(i)}$ have the same variance σ_n^2 but different means $\mu^{(i)}$

- To achieve the fairness of collusion, seek $\{\beta_k\}$ and $\{\alpha_l\}$ such that $\mu^{(i)}$ are the same for all colluders.

$$\begin{aligned} & \mu^{(Alice)} = \mu^{(Bob)} = \mu^{(Carl)} \\ s.t. \quad & 0 \le \beta_1, \beta_2, \beta_3 \le 1, \beta_1 + \beta_2 + \beta_3 = 1 \\ & 0 \le \alpha_1, \alpha_2 \le 1, \alpha_1 + \alpha_2 = 1 \end{aligned}$$

Fairness Issue During Collusion

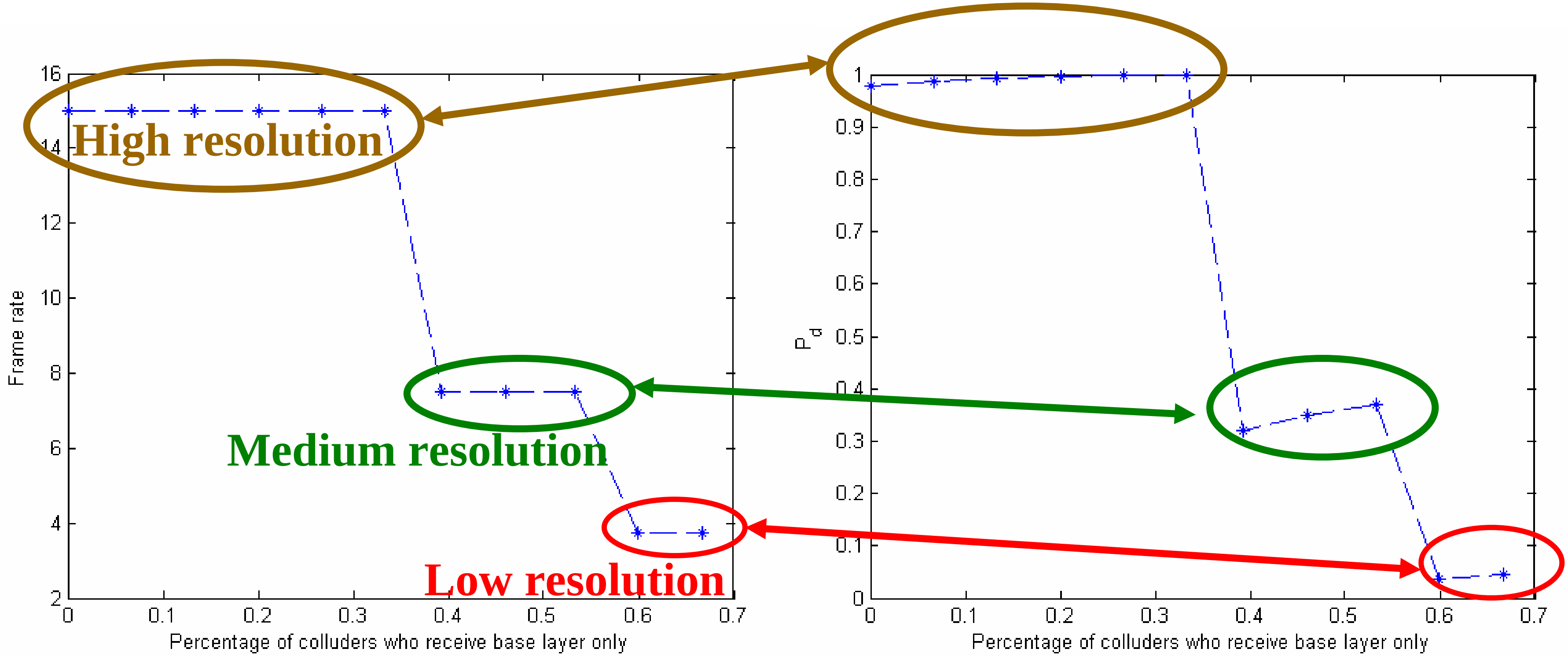
$F^c = F_b \cup F_{e1} \cup F_{e2}$ (Highest resolution)	Fairness Constraints	$\begin{cases} \frac{K^b\sqrt{N_b}}{K^b\sqrt{N_b}+K^{b,e1}\sqrt{N_b+N_{e1}}+K^{all}\sqrt{N_b+N_{e1}+N_{e2}}} \le \frac{N_b}{N_b+N_{e1}+N_{e2}}, \\ \frac{K^{all}\sqrt{N_b+N_{e1}+N_{e2}}}{K^b\sqrt{N_b}+K^{b,e1}\sqrt{N_b+N_{e1}}+K^{all}\sqrt{N_b+N_{e1}+N_{e2}}} \ge \frac{N_{e2}}{N_b+N_{e1}+N_{e2}}. \end{cases}$
	Parameter Selection	$\begin{cases} \beta_1 = \frac{N_b+N_{e1}+N_{e2}}{N_b} \frac{K^b\sqrt{N_b}}{K^b\sqrt{N_b}+K^{b,e1}\sqrt{N_b+N_{e1}}+K^{all}\sqrt{N_b+N_{e1}+N_{e2}}}, \\ \beta_2 N_b + \alpha_1 N_{e1} = \frac{(N_b+N_{e1}+N_{e2})K^{b,e1}\sqrt{N_b+N_{e1}}}{K^b\sqrt{N_b}+K^{b,e1}\sqrt{N_b+N_{e1}}+K^{all}\sqrt{N_b+N_{e1}+N_{e2}}}, \\ \beta_3 = 1-\beta_1-\beta_2,\ \alpha_2 = 1-\alpha_1. \end{cases}$
$F^c = F_b \cup F_{e1}$ (Medium resolution)	Fairness Constraints	$\frac{K^b\sqrt{N_b}}{K^b\sqrt{N_b}+(K^{b,e1}+K^{all}) \ldots} \le \frac{N_b}{\ldots}$
		$\alpha_1 = \frac{\ldots^{b,e1}}{K^{b,e1}+K^{all}},\ \alpha_2 = 1-\alpha_1.$
$F^c = F_b$ (Lowest resolution)	Fairness Constraints	No constraints on $(K^b, K^{b,e1}, K^{all})$ and (N_b, N_{e1}, N_{e2})
	Parameter Selection	$\beta_1 = \frac{K^b}{K^b+K^{b,e1}+K^{all}},\ \beta_2 = \frac{K^{b,e1}}{K^b+K^{b,e1}+K^{all}},\ \beta_3 = \frac{K^{all}}{K^b+K^{b,e1}+K^{all}}.$

Number of colluders in different subgroups

Length of fingerprints embedded in different layers

- **A copy of higher resolution → more severe constraints on collusion**

Effectiveness of Collusion



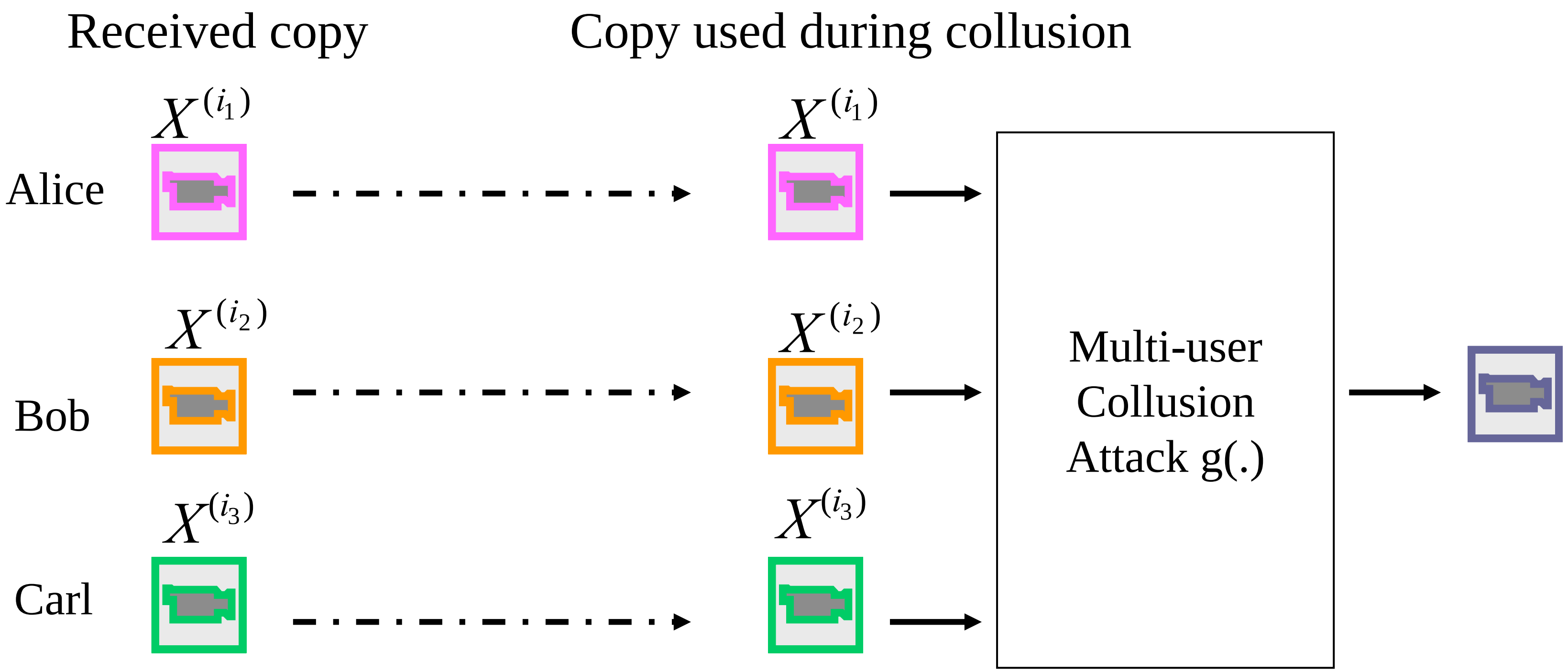
Perceptual quality of the colluded copy **Effectiveness of fair collusion**

➢**A colluded copy of higher resolution → larger risk to be detected**

Traitors within Traitors in Multimedia Forensic Systems

Assumptions in Prior Work

- Assumptions of fair-play during collusion in prior work
  - All colluders keep their agreement of fair collusion
  - Everyone tells the truth of his fingerprinted copy during collusion



Traitors within Traitors

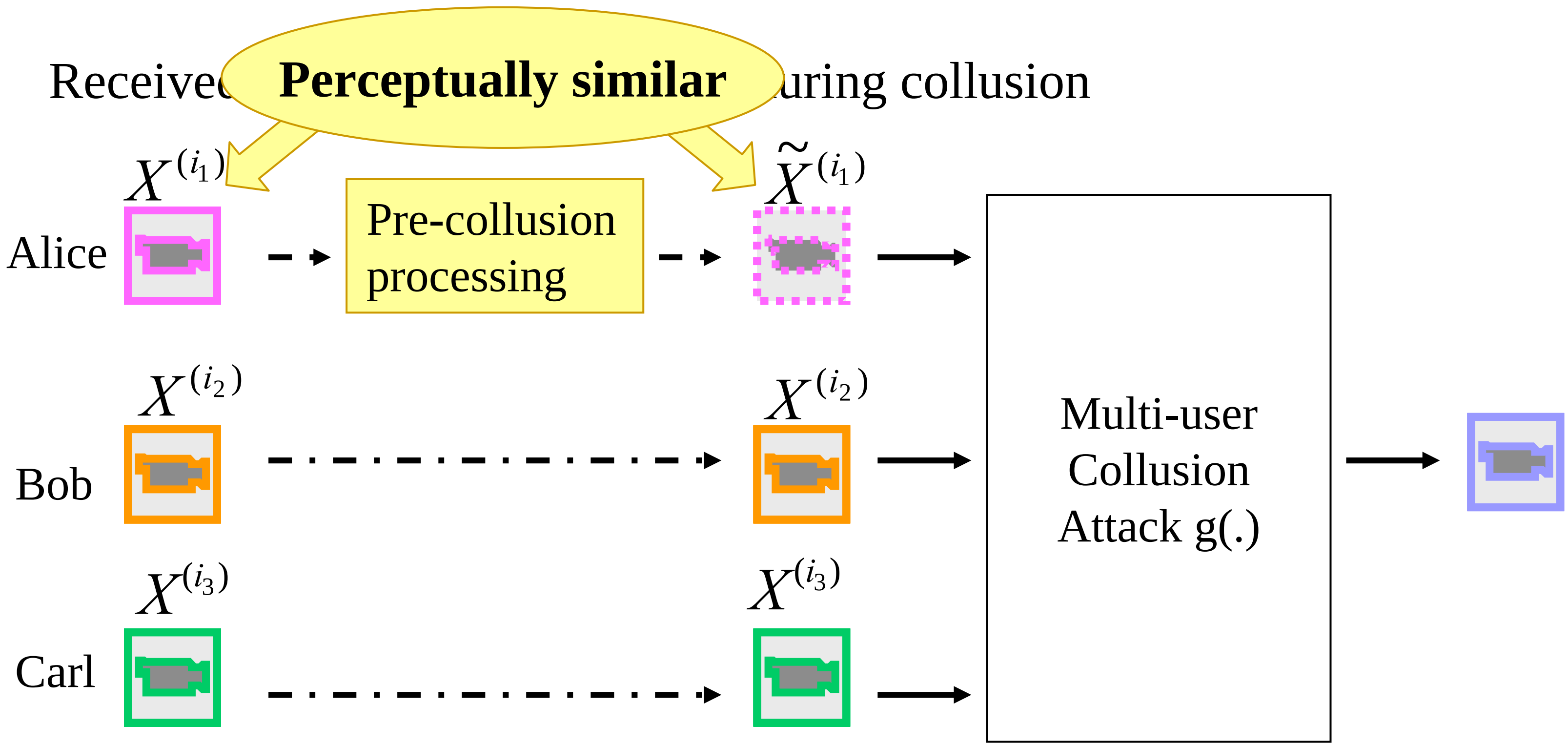
- The assumption of fair-play during collusion may not always hold

- Dynamics among attackers during collusion
  - **Selfish colluders** : wish to minimize their own risk of being caught
  - **Other colluders** : wish to protect their own interests

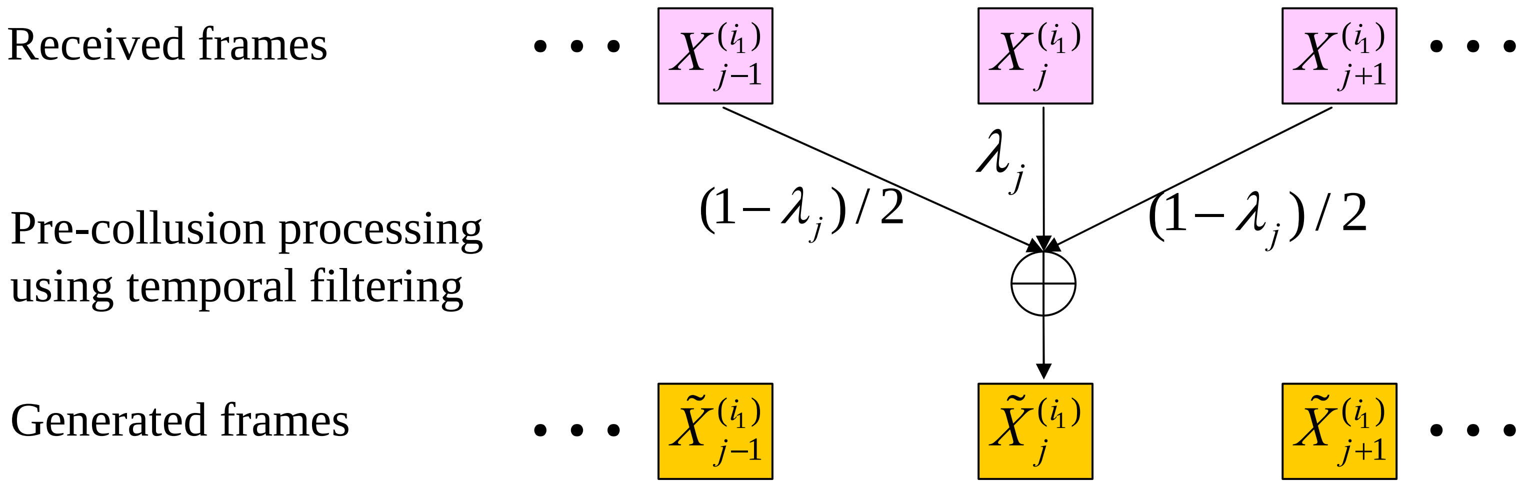
- Formulation and analysis of the dynamics among colluders:
  - Understand the attackers' behavior
  - Build a complete model of multi-user collusion

Risk Minimization by Selfish Colluders

- Selfish colluders:
  - Alice processes her fingerprinted copy before multi-user collusion to further reduce her probability of being detected



Temporal Filtering of Fingerprinted Frames



- Goal: attenuate the energies of the embedded fingerprints
  - Replace each segment of the fingerprinted copy with another, seemingly similar segment from different regions of the content
- Temporal filtering of the received fingerprinted frames

$$\tilde{X}_j^{(i_1)} = \frac{1-\lambda_j}{2} X_{j-1}^{(i_1)} + \lambda_j X_j^{(i_1)} + \frac{1-\lambda_j}{2} X_{j+1}^{(i_1)}, \quad 0 \le \lambda_j \le 1$$

Performance Analysis

- Perceptual quality of the newly generated frames:

$$MSE_j = \left\| \tilde{X}_j^{(i_1)} - X_j^{(i_1)} \right\|^2 = (1-\lambda_j)^2 \phi_j / 4$$

  - ϕ_j is a constant of λ_j
  - A larger λ_j is preferred to minimize the perceptual distortion

- The selfish colluder's probability of being detected:

$$T_N^{(i_1)} = N\left(\mu^{(i_1)}, \sigma_n^2\right), \text{ where } \mu^{(i_1)} = \theta_1 + \sum_j \lambda_j \theta_2(j)$$

  - θ_1 and $\theta_2(j)$ are constants of λ_j, $\theta_2(j) \geq 0$
  - A smaller λ_j is preferred to minimize the probability of being detected

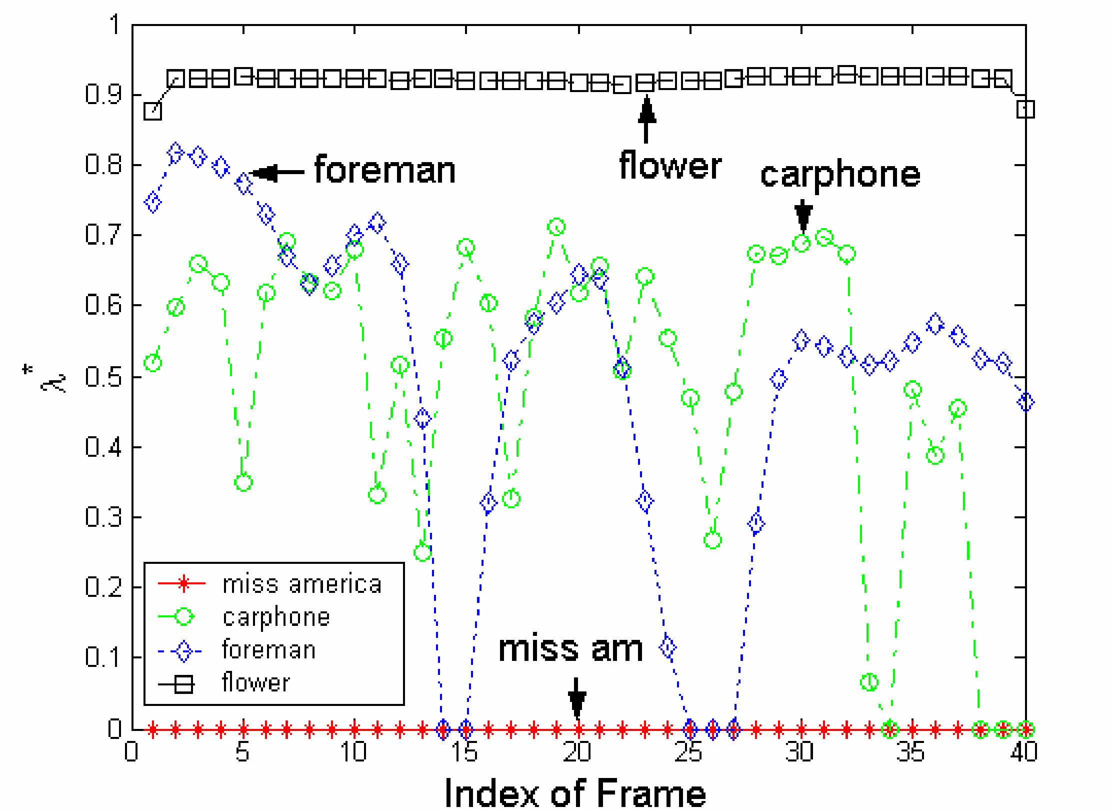
Selection of the Optimum Filter

- Selfish colluders:
  - tradeoff between the probability of being detected and the perceptual quality of the newly generated copy
- Selection of the optim

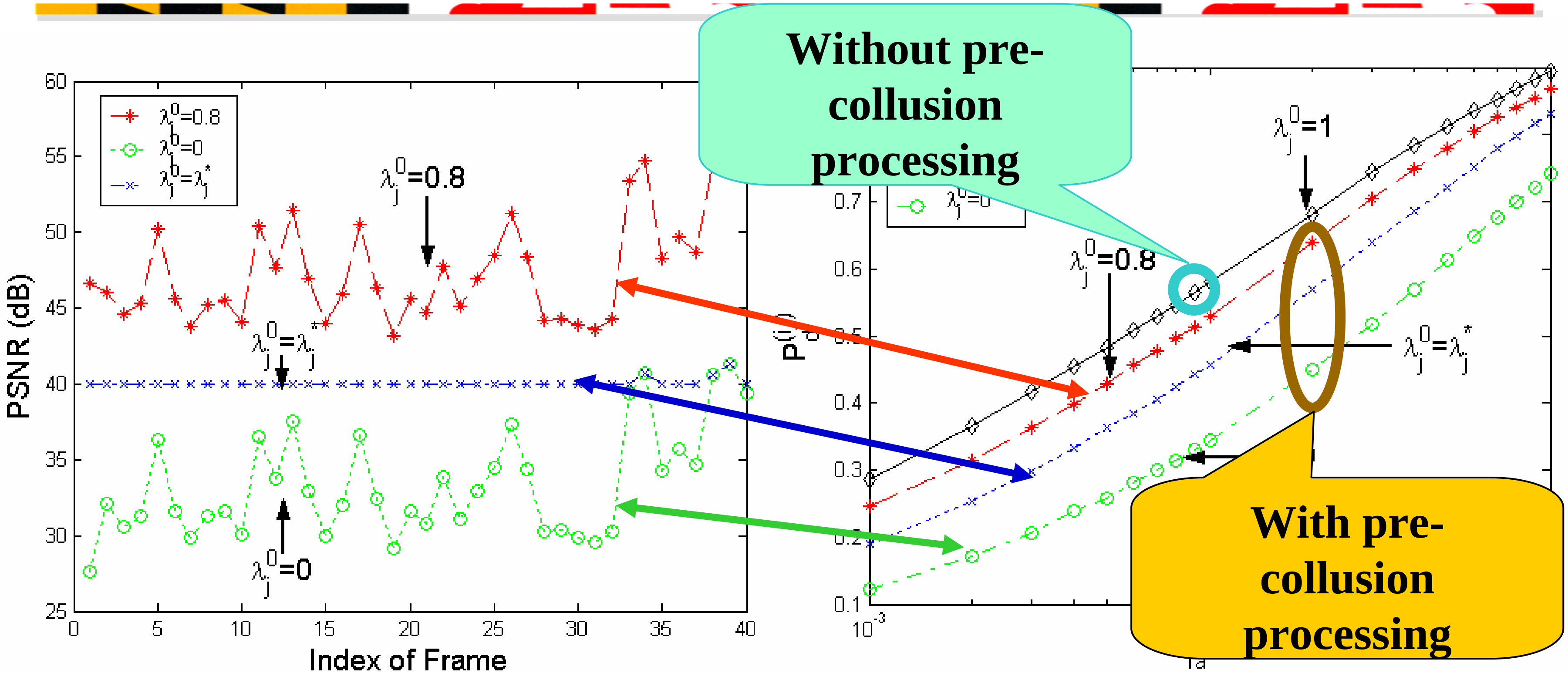
Alice's probability of being detected

Quality constraints

$$PSNR_j \geq 40dB$$



Simulation Results



Perceptual quality of the newly generated copy

The selfish colluder's probability of being detected

- **Temporal filtering can further reduce the selfish colluder's risk**
- **Smaller prob. of being detected → worse perceptual quality**

Summary on Analysis of Dynamics Among Colluders

- Important to analyze the dynamics among colluders
  - Helps to understand the attackers' behavior during collusion
  - Enables to build a complete model of multi-user collusion
- What we have known:
  - How the colluders achieve the fairness during collusion
  - How a single selfish colluder can further reduce his/her risk
- There are still a lot that we need to learn:
  - How several selfish colluders work together to minimize their risk
  - How other colluders can detect and prevent such selfish behavior during collusion
  - …
- So we have more work to do…

Related Publications

- W. Trappe, M. Wu, Z.J. Wang, K.J.R. Liu, "Anti-Collusion Fingerprinting for Multimedia", *IEEE Trans. on Signal Processing*, special issue on Signal Processing for Data Hiding in Digital Media & Secure Content Delivery, vol. 51, no. 4, pp.1069-1087, April 2003.
- Z.J. Wang, M. Wu, H. Zhao, W. Trappe, and K.J.R. Liu: "Collusion Resistance of Multimedia Fingerprinting Using Orthogonal Modulation", *IEEE Trans. on Image Proc.*, vol 14, no 6, pp. 804-821, June 2005.
- H. Zhao, M. Wu, Z.J. Wang, and K.J.R. Liu: "Nonlinear Collusion Attacks on Independent Multimedia Fingerprints", *IEEE Trans. on Image Proc.*, vol 14, no 5, pp.646-661, May 2005.
- Z.J. Wang, M. Wu, W. Trappe, and K.J.R. Liu: "Group-Oriented Fingerprinting for Multimedia Forensics", *EURASIP Journal on Applied Signal Processing*, special issue on multimedia security and rights management, 2004:14, pp. 2142-2162, Nov 2004.
- M. Wu, W. Trappe, Z.J. Wang, and K.J.R. Liu, "Collusion-Resistant Fingerprinting for Multimedia", *IEEE Signal Processing Magazine*, Special Issue on Digital Rights: Management, Protection, Standardization, vol 21, no 2, pp.15-27, March 2004.
- H.V. Zhao and K.J.R. Liu, "Risk Minimization in Traitors within Traitors in Multimedia Forensics", Proc. IEEE Int'l Conf. on Image Processing (ICIP), Genoa, Sep. 2005.
- H.V. Zhao and K.J.R. Liu, "Resistance Analysis of Scalable Video Fingerprinting under Fair Collusion Attacks", Proc. IEEE Int'l Conf. on Image Processing (ICIP), Genoa, Sep. 2005.

????

Thanks you!