Information-Theoretical Limits of Active Content Fingerprinting in Content-based Identification Systems

Farzad Farhadzadeh [1] Frans M.J. Willems [1] Sviatoslav Voloshynovskiy[2]

[1]Electrical Engineering Department, Eindhoven University of Technology, The Netherlands

[2]Computer Science Department, Univeristy of Geneva, Switzerland

November, 2015

Workshop on Information Forensics and Security (WIFS' 15)

Outline

Motivation

Digital content/Physical objects




- Goals
  - Identification: origin, ownership, *etc.*
  - Monitoring
  - Automatic tagging

Online sharing services

Motivation

Digital content/Physical objects




Online sharing services

- Goals
  - Identification: origin, ownership, *etc.*
  - Monitoring
  - Automatic tagging
- Main concerns
  - Performance
  - Search complexity
  - Memory complexity
  - Security and Privacy

Main approaches to content identification

- Digital Watermarking (DWM)
- Passive Content FP (PCFP)
- Active Content FP (ACFP)

Main approaches to content identification

- **Digital Watermarking (DWM)**
- Passive Content FP (PCFP)
- Active Content FP (ACFP)

- Main idea
  - image identification based on host-independent mark embedding
    (ID $\rightarrow$ WM)

Main approaches to content identification

- **Digital Watermarking (DWM)**
- Passive Content FP (PCFP)
- Active Content FP (ACFP)

- Main idea
  - image identification based on host-independent mark embedding (ID $\rightarrow$ WM)
- Main properties
  - host interference cancellation
  - identification performance $\equiv$ WM power
  - structured code $\Rightarrow$ low identification complexity

Main approaches to content identification

- Digital Watermarking (DWM)
- **Passive Content FP (PCFP)**
- Active Content FP (ACFP)

- Main idea
  - identification based on content features
    (content $\rightarrow$ FP $\rightarrow$ ID)

Main approaches to content identification

- Digital Watermarking (DWM)
- **Passive Content FP (PCFP)**
- Active Content FP (ACFP)

- Main idea
  - identification based on content features
    (content $\rightarrow$ FP $\rightarrow$ ID)
- Main properties
  - no modifications
  - identification performance $\equiv$ content feature power
  - random code $\Rightarrow$ high identification complexity

Main approaches to content identification

- Digital Watermarking (DWM)
- Passive Content FP (PCFP)
- **Active Content FP (ACFP)**

- Main idea
  - similar to PCFP (content $\rightarrow$ FP $\rightarrow$ ID)
  - but modify content to
    - increase identification performance
    - reduce search complexity

[1] Voloshynovskiy et al,. Active content fingerprinting: A marriage of digital watermarking and content fingerprinting, IEEE WIFS'12.
[2] F. Farhadzadeh and S. Voloshynovskiy, Active Content Fingerpriting, IEEE Trans. TIFS'14.

Main approaches to content identification

- Digital Watermarking (DWM)
- Passive Content FP (PCFP)
- **Active Content FP (ACFP)**

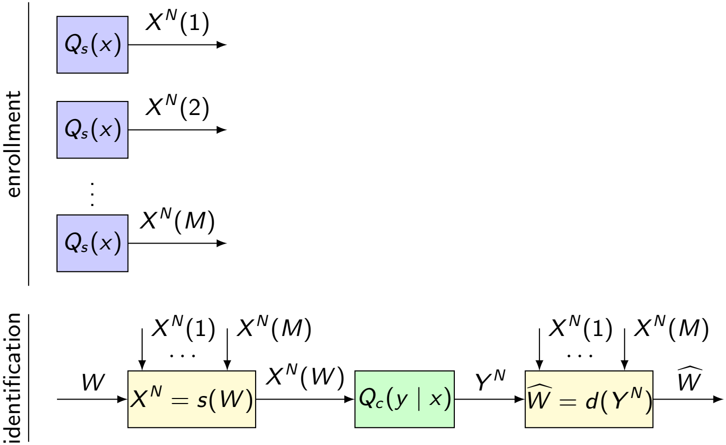
- Main idea
  - similar to PCFP (content $\rightarrow$ FP $\rightarrow$ ID)
  - but modify content to
    - increase identification performance
    - reduce search complexity
- Main properties
  - content modulation (but no need in interference cancellation)
  - modulated content $\equiv$ content feature power $\Rightarrow$ performance
  - potentially structured code $\Rightarrow$ low identification complexity

ACFP references[1] [2]

[1] Voloshynovskiy et al,. Active content fingerprinting: A marriage of digital watermarking and content fingerprinting, IEEE WIFS'12.

[2] F. Farhadzadeh and S. Voloshynovskiy, Active Content Fingerpriting, IEEE Trans. TIFS'14.

Identification Setup (PCFP)



Identification Setup (PCFP)

Identification rate R is called achievable, if for any $\epsilon > 0$ there exist for large enough N, decoders such that

$$\frac{1}{N}\log_2 M \geq R - \epsilon,$$
$$P_{\mathcal{E}} \leq \epsilon.$$

Error probability:

$$P_{\mathcal{E}} \triangleq \frac{1}{M}\sum_{w=1}^{M}\Pr\{\widehat{W} \neq w | W = w\}$$

Theorem

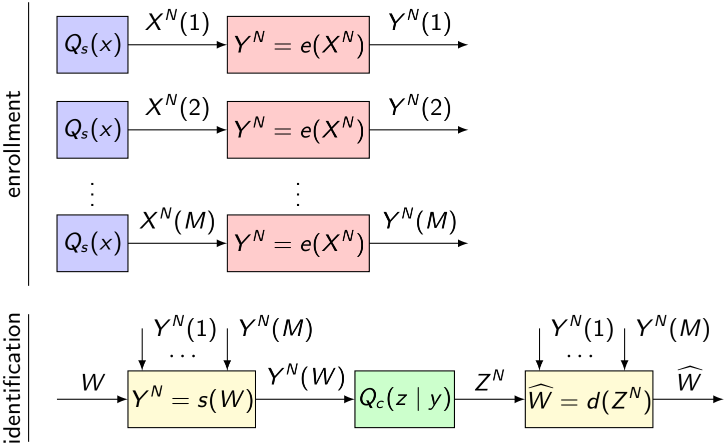
Capacity of an identification system C_{id}, supremum of all achievable rates, is given by [3]

$$C_{id} = I(X;Y),$$

where $P(x,y) = Q_s(x)Q_c(y|x)$ for all $x \in \mathcal{X}, y \in \mathcal{Y}$.

[3] Willems et al, On the capacity of a biometrical identification system, IEEE ISIT'03.

Model Description (ACFP)



Model Description (ACFP)

Identification rate-distortion pair (R, Δ) is called achievable, if for any $\epsilon > 0$ there exist for large enough N, decoders such that

$$\frac{1}{N}\log_2 M \geq R - \epsilon,$$
$$\overline{D_{xy}} \leq \Delta + \epsilon,$$
$$P_{\mathcal{E}} \leq \epsilon.$$

Modification distortion:

$$\overline{D_{xy}} = \frac{1}{N} E\left[\sum_{n=1}^{N} D_{xy}(X_n, Y_n)\right]$$

Statement of Result

Theorem

The region of achievable rate-distortion pair (R, Δ) for the identification system using ACFP is given by [4]

$$\Big\{(R, \Delta) : R \leq I(Y; Z), \quad \Delta \geq \sum_{x,y} Q_s(x) P_t(y \mid x) D_{xy}(x, y), \quad \text{for } P(x, y, z) = Q_s(x) P_t(y \mid x) Q_c(z \mid y)\Big\}$$

[4] Farhadzadeh, Willems, and Voloshynovskiy, Information theoretical analysis of identification based on active content fingerprinting, WIC'14.

Statement of Result

Theorem

The region of achievable rate-distortion pair (R, Δ) for the identification system using ACFP is given by [4]

$$\Big\{(R,\Delta) : R \leq I(Y;Z),\quad \Delta \geq \sum_{x,y} Q_s(x)P_t(y \mid x)D_{xy}(x,y),\quad \text{for } P(x,y,z) = Q_s(x)P_t(y \mid x)Q_c(z \mid y)\Big\}$$

Capacity of an identification system using ACFP, supremum of all achievable rates for a given Δ, is given by

$$C_{ACFP}(\Delta) = \max_{P_t(y|x): \sum_{x,y} Q_s(x)P_t(y|x)D_{xy}(x,y) \leq \Delta} I(Y;Z)$$

[4] Farhadzadeh, Willems, and Voloshynovskiy, Information theoretical analysis of identification based on active content fingerprinting, WIC'14.

Gaussian Setup

Let's X^N be distributed i.i.d. according to a Gaussian with variance V_X and mean zero, and $Q_c(z|y)$ be AWGN with variance V_Z.

Gaussian Setup

Let's X^N be distributed i.i.d. according to a Gaussian with variance V_X and mean zero, and $Q_c(z|y)$ be AWGN with variance V_Z.

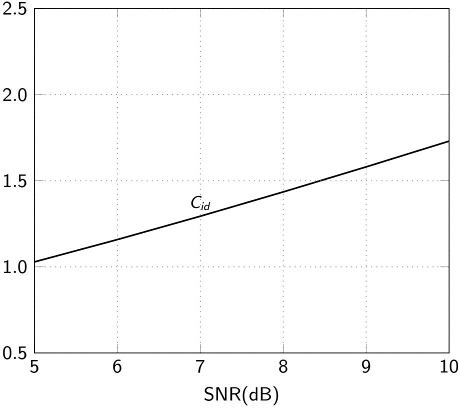
Theorem

Considering distortion as the mean-squared error, the capacity of identification using ACFP is given by

$$\boxed{C_{ACFP}(\Delta) = \frac{1}{2}\log_2\left(1 + \frac{(\sqrt{V_X}+\sqrt{\Delta})^2}{V_N}\right)}$$

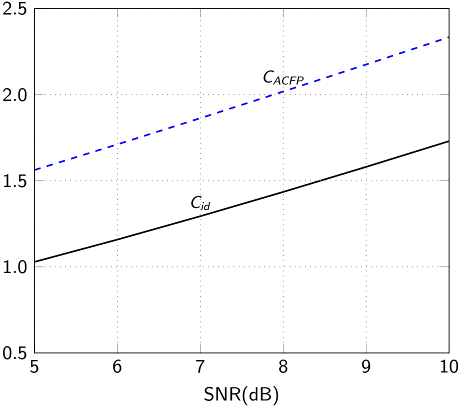
achieved by $Y^N = fX^N$*, such that* $(f-1)^2 V_X = \Delta$*.*

Gaussian Setup



$$C_{id} = \frac{1}{2}\log_2\left(1 + \frac{V_X}{V_N}\right)$$

Gaussian Setup

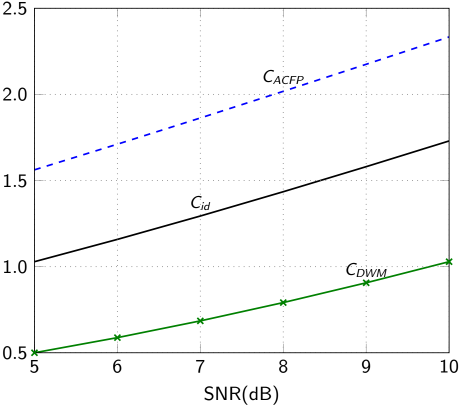


$$C_{id} = \frac{1}{2}\log_2\left(1 + \frac{V_X}{V_N}\right)$$

$$C_{ACFP} = \frac{1}{2}\log_2\left(1 + \frac{(\sqrt{\Delta}+\sqrt{V_X})^2}{V_N}\right)$$

Signal-to-Distortion Ratio (SDR)=5dB

Gaussian Setup



$$C_{id} = \frac{1}{2}\log_2\left(1 + \frac{V_X}{V_N}\right)$$

$$C_{ACFP} = \frac{1}{2}\log_2\left(1 + \frac{(\sqrt{\Delta}+\sqrt{V_X})^2}{V_N}\right)$$

$$C_{DWM} = \frac{1}{2}\log_2\left(1 + \frac{\Delta}{V_N}\right)^5$$

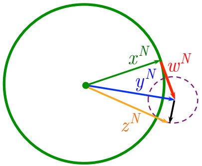
Signal-to-Distortion Ratio (SDR)=5dB

[6] Costa, Writing on dirty paper, IEEE Trans. Information Theory , 1983.

Comparison of identification methods

Chain: $X \rightarrow Y \rightarrow Z$

$$C_{DWM} = \frac{1}{2}\log_2\left(1 + \frac{\Delta}{V_N}\right)$$

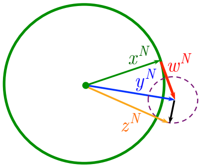


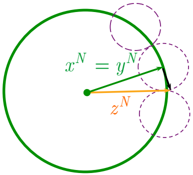
Comparison of identification methods

Chain: $X \rightarrow Y \rightarrow Z$

$$C_{DWM} = \frac{1}{2} \log_2 \left(1 + \frac{\Delta}{V_N}\right)$$

$$C_{id} = \frac{1}{2} \log_2 \left(1 + \frac{V_X}{V_N}\right)$$





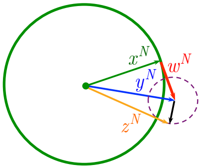
Comparison of identification methods

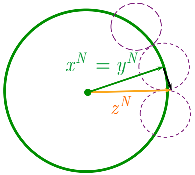
Chain: $X \to Y \to Z$

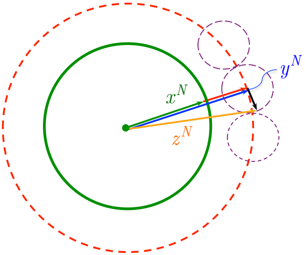
$$C_{DWM} = \frac{1}{2}\log_2\left(1 + \frac{\Delta}{V_N}\right)$$

$$C_{id} = \frac{1}{2}\log_2\left(1 + \frac{V_X}{V_N}\right)$$

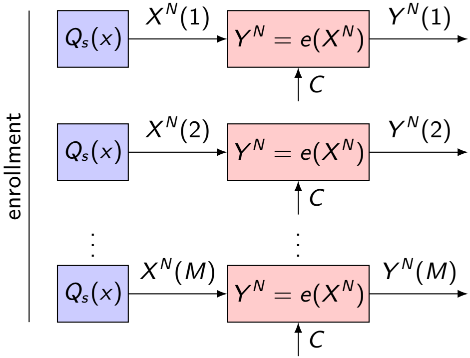
$$C_{ACFP} = \frac{1}{2}\log_2\left(1 + \frac{(\sqrt{\Delta}+\sqrt{V_X})^2}{V_N}\right)$$



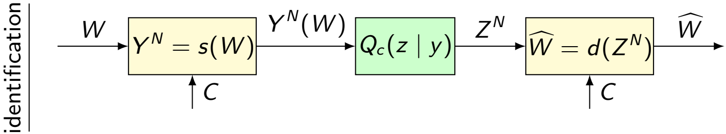




Code-based ACFP



$$C = \{Y^N(1), Y^N(2), \ldots, Y^N(M_C)\}$$



Code-based ACFP

Theorem

The region of achievable rate-distortion pair (R, Δ) for the identification system using code-based ACFP is given by

$$\Big\{(R, \Delta) : R \leq I(Y; Z),$$
$$I(X, Y) \leq I(Y; Z),$$
$$\Delta \geq \sum_{x,y} Q_s(x) P_t(y \mid x) D_{xy}(x, y),$$
$$\textit{for } P(x, y, z) = Q_s(x) P_t(y \mid x) Q_c(z \mid y)\Big\}.$$

Gaussian Setup

Let's X^N be distributed i.i.d. according to a Gaussian with variance V_X and mean zero, and $Q_c(z \mid y)$ be AWGN with variance V_Z.

Gaussian Setup

Let's X^N be distributed i.i.d. according to a Gaussian with variance V_X and mean zero, and $Q_c(z \mid y)$ be AWGN with variance V_Z.

Theorem

Considering distortion as the mean-squared error, the maximum identification rate using code-based ACFP is given by

$$R^*_{ACFP(CB)}(\Delta) = \frac{1}{2}\log_2\left(\frac{1}{1-\rho^2}\right)$$

where $\rho = E[XY]/\sqrt{V_X V_Y}$ *and* $(1 - \Delta/V_X) \leq \rho^2 < 1$ *is a solution of*

$$2\rho^2 + 2\rho\sqrt{\rho^2 - \left(1 - \frac{\Delta}{V_X}\right)} - \left(1 - \frac{\Delta}{V_X}\right) = \frac{V_N}{V_X}\left(\frac{\rho^2}{1-\rho^2}\right).$$

Gaussian Setup

Let's X^N be distributed i.i.d. according to a Gaussian with variance V_X and mean zero, and $Q_c(z \mid y)$ be AWGN with variance V_Z.

Theorem

Considering distortion as the mean-squared error, the maximum identification rate using code-based ACFP is given by

$$\boxed{R^*_{ACFP(CB)}(\Delta) = \frac{1}{2}\log_2\left(\frac{1}{1-\rho^2}\right)}$$

where $\rho = E[XY]/\sqrt{V_X V_Y}$ *and* $(1 - \Delta/V_X) \leq \rho^2 < 1$ *is a solution of*

$$2\rho^2 + 2\rho\sqrt{\rho^2 - \left(1 - \frac{\Delta}{V_X}\right)} - \left(1 - \frac{\Delta}{V_X}\right) = \frac{V_N}{V_X}\left(\frac{\rho^2}{1-\rho^2}\right).$$

Remark

Contrary to General setup, $\rho = 1$ is not attainable.

Proof Outline

Any $R \leq I(Y;Z)$ subject to $I(X;Y) \leq I(Y;Z)$ is achievable with Gaussian assignment.

Remark

$I(Y;Z) \leq \frac{1}{2}\log_2\left(1+\frac{V_Y}{V_N}\right)$ for Gaussian $p(y \mid x)$ and arbitrarily $p(y)$.

Proof Outline

Any $R \leq I(Y;Z)$ subject to $I(X;Y) \leq I(Y;Z)$ is achievable with Gaussian assignment.

Remark

$I(Y;Z) \leq \frac{1}{2}\log_2\left(1+\frac{V_Y}{V_N}\right)$ for Gaussian $p(y \mid x)$ and arbitrarily $p(y)$.

$$R \leq I(Y;Z) \leq \frac{1}{2}\log_2\left(1+\frac{V_Y}{V_N}\right)$$

$$\frac{1}{2}\log_2\left(\frac{1}{1-\rho^2}\right) \leq I(X;Y) \leq I(Y;Z) \leq \frac{1}{2}\log_2\left(1+\frac{V_Y}{V_N}\right)$$

Proof Outline

Any $R \leq I(Y;Z)$ subject to $I(X;Y) \leq I(Y;Z)$ is achievable with Gaussian assignment.

Remark

$I(Y;Z) \leq \frac{1}{2}\log_2\left(1+\frac{V_Y}{V_N}\right)$ for Gaussian $p(y \mid x)$ and arbitrarily $p(y)$.

$$R \leq I(Y;Z) \leq \frac{1}{2}\log_2\left(1+\frac{V_Y}{V_N}\right)$$

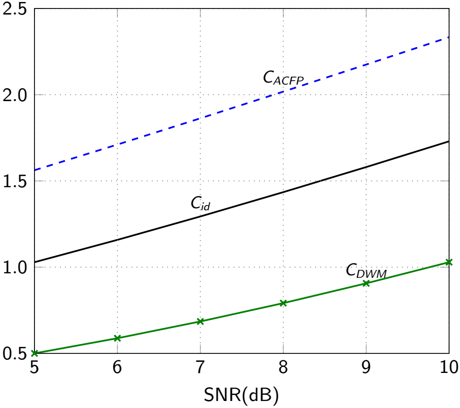
$$\frac{1}{2}\log_2\left(\frac{1}{1-\rho^2}\right) \leq I(X;Y) \leq I(Y;Z) \leq \frac{1}{2}\log_2\left(1+\frac{V_Y}{V_N}\right)$$

Optimization:

$$\begin{aligned} \underset{V_Y}{\text{maximize}} \quad & \frac{1}{2}\log_2\left(1+\frac{V_Y}{V_N}\right) \\ \text{subject to} \quad & \frac{1}{2}\log_2\left(\frac{1}{1-\rho^2}\right) \leq \frac{1}{2}\log_2\left(1+\frac{V_Y}{V_N}\right) \\ & V_Y + V_X - 2\rho\sqrt{V_X V_Y} \leq \Delta \end{aligned}$$

maximum occurs for such a ρ that satisfies the constraints with equality.

Gaussian Setup



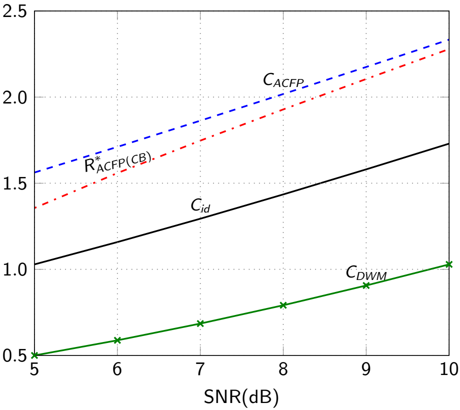
SDR=5dB

$$C_{id} = \frac{1}{2}\log_2\left(1 + \frac{V_X}{V_N}\right)$$

$$C_{ACFP} = \frac{1}{2}\log_2\left(1 + \frac{(\sqrt{\Delta}+\sqrt{V_X})^2}{V_N}\right)$$

$$C_{DWM} = \frac{1}{2}\log_2\left(1 + \frac{\Delta}{V_N}\right)$$

Gaussian Setup



SDR=5dB

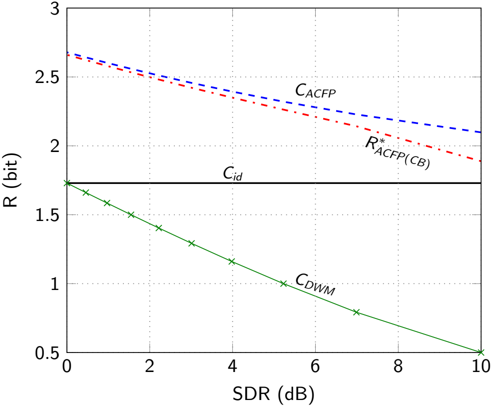
$$C_{id} = \frac{1}{2}\log_2\left(1 + \frac{V_X}{V_N}\right)$$

$$C_{ACFP} = \frac{1}{2}\log_2\left(1 + \frac{(\sqrt{\Delta}+\sqrt{V_X})^2}{V_N}\right)$$

$$C_{DWM} = \frac{1}{2}\log_2\left(1 + \frac{\Delta}{V_N}\right)$$

$$R^*_{ACFP(CB)} = \frac{1}{2}\log_2\left(1 + \frac{1}{1-\rho^2}\right)$$

Gaussian Setup



$$C_{id} = \frac{1}{2}\log_2\left(1 + \frac{V_X}{V_N}\right)$$

$$C_{ACFP} = \frac{1}{2}\log_2\left(1 + \frac{(\sqrt{\Delta}+\sqrt{V_X})^2}{V_N}\right)$$

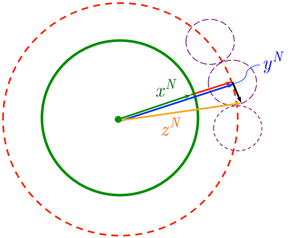
$$C_{DWM} = \frac{1}{2}\log_2\left(1 + \frac{\Delta}{V_N}\right)$$

$$R^*_{ACFP(CB)} = \frac{1}{2}\log_2\left(1 + \frac{1}{1-\rho^2}\right)$$

SNR=10dB

ACFP: random vs coded

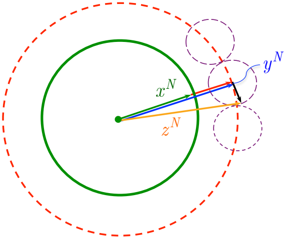
$$C_{ACFP} = \frac{1}{2}\log_2\left(1 + \frac{(\sqrt{\Delta}+\sqrt{V_X})^2}{V_N}\right)$$

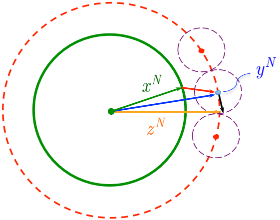


ACFP: random vs coded

$$C_{ACFP} = \frac{1}{2}\log_2\left(1 + \frac{(\sqrt{\Delta}+\sqrt{V_X})^2}{V_N}\right)$$

$$R^*_{ACFP(CB)} = \frac{1}{2}\log_2\left(1 + \frac{1}{1-\rho^2}\right)$$





Conclusions

- We investigated the capacity of identification using ACFP under arbitrarily encoding scheme (random codes)

Conclusions

- We investigated the capacity of identification using ACFP under arbitrarily encoding scheme (random codes)
  - the optimal encoding scheme under Gaussian setup

Conclusions

- We investigated the capacity of identification using ACFP under arbitrarily encoding scheme (random codes)
  - the optimal encoding scheme under Gaussian setup
- We evaluated the maximum identification rate using code-based ACFP (structured codes)

Conclusions

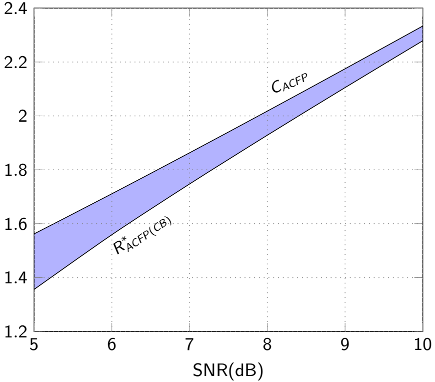
- We investigated the capacity of identification using ACFP under arbitrarily encoding scheme (random codes)
  - the optimal encoding scheme under Gaussian setup
- We evaluated the maximum identification rate using code-based ACFP (structured codes)
  - the optimal encoding scheme under Gaussian setup

Conclusions

- We investigated the capacity of identification using ACFP under arbitrarily encoding scheme (random codes)
  - the optimal encoding scheme under Gaussian setup
- We evaluated the maximum identification rate using code-based ACFP (structured codes)
  - the optimal encoding scheme under Gaussian setup
- We showed the gap between the random and code-based ACFP

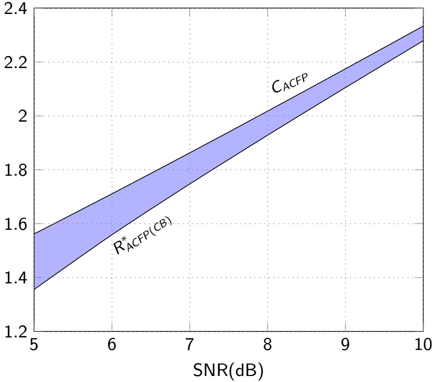
Future work

- To investigate other ACFP schemes to find optimal trade-off between complexity and performance



Future work

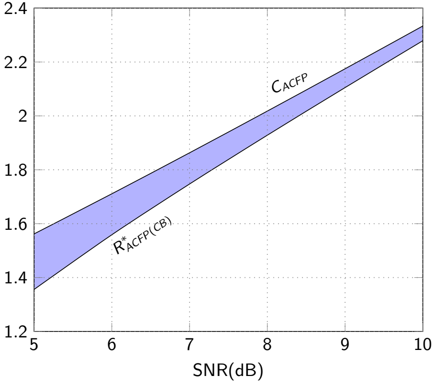
- To investigate other ACFP schemes to find optimal trade-off between complexity and performance



- To investigate ACFP in other applications like content authentication

Future work

- To investigate other ACFP schemes to find optimal trade-off between complexity and performance



- To investigate ACFP in other applications like content authentication
- To apply coded-ACFP to geometrically invariant descriptors (SPIE'16)