Secure Sketch for Set Distance on Noisy Data

KMS Annual Meeting 2014

Jung Hee Cheon and Yongsoo Song

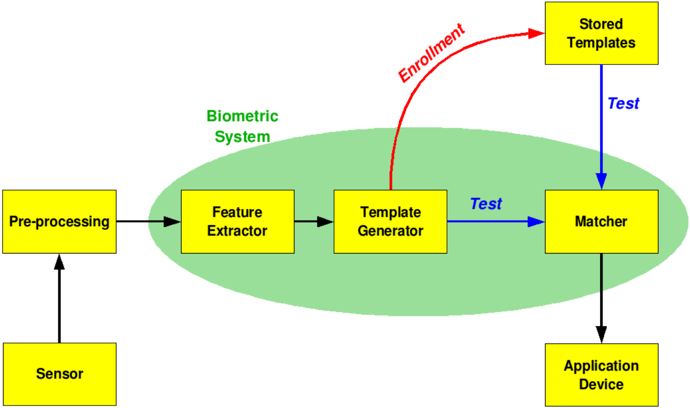
Seoul National University

Oct 25, 2014

Noisy information in cryptography

- Classical cryptographic applications
  - Lack of error-tolerance
  - Key arrangement problem: storing, reliably reproducing
- Noisy information (biometric)
  - More plentiful (higher entropy) and convenient
  - Small noises are introduced during acquisition and processing
  - Cannot be reproduced exactly

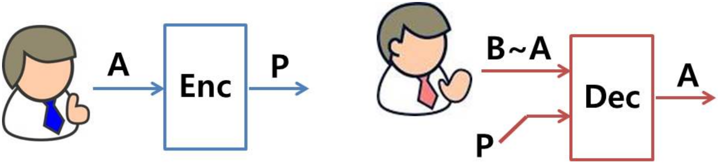
Biometric security system



- Biometric templates are elements of a metric space $(\mathcal{M}, \mathrm{DIST})$
  - For an enrollment A, a query B is accepted whenever $\mathrm{DIST}(A, B) \leq \tau$
- Performance indicators: FRR, FAR

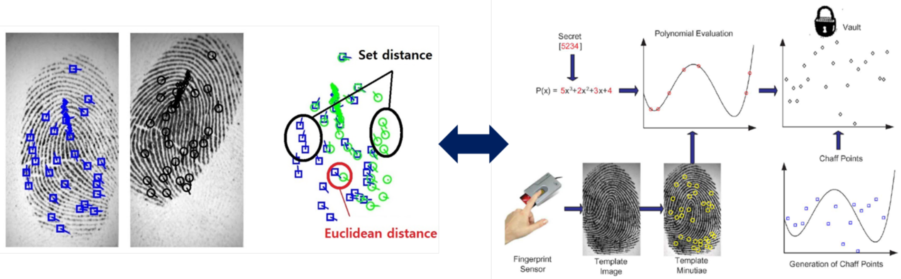
Theoretic primitive

- Secure sketch on a metric space $(\mathcal{M}, \mathsf{DIST})$ with parameter $(\tau, \mathcal{L})$
  - Additional helper data is made public
  - Consisting of $\mathsf{Enc} : \mathcal{M} \to \{0,1\}^*$ and $\mathsf{Dec} : \mathcal{M} \times \{0,1\}^* \to \mathcal{M}$ satisfying $\mathsf{Dec}(B, \mathsf{Enc}(A)) = A$ if $\mathsf{DIST}(A, B) \le \tau$
  - Can be reduced to many cryptographic applications such as secure authentication, key binding, key extraction
  - Security: bound the entropy loss $\mathcal{L} = \mathbf{H}_\infty(X) - \tilde{\mathbf{H}}_\infty(X|\mathsf{Enc}(X))$
  - Reusability: multi-templates attack
  - Set distance: $(A, B) \mapsto |A \triangle B|$ for $A \triangle B = (A \backslash B) \cup (B \backslash A)$
  - Fuzzy vault [JS06], Improved JS [DORS08]



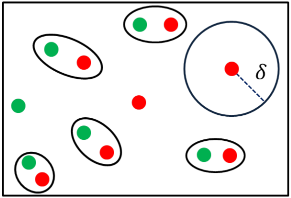
Two phases

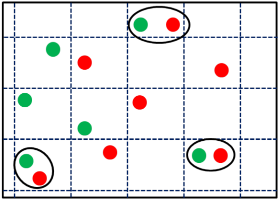
- Biometric system
  - Express practical algorithms as a metric function
- Cryptographic application
  - Construct a secure sketch scheme for a given distance function



Set distance on noisy data

- Motivation
  - Many biometric templates are represented in a general form: The original A is a set of s feature points of a metric space $(\mathcal{U}, \mathrm{dist})$
  - Each point is perturbed by a distance less than δ (point-wise error) and some points can be replaced (set distance) under permissible noise
- Previous work
  - Count the number of pairs $(a, b) \in A \times B$ such that $\mathrm{dist}(a, b) < \delta$: $A \backslash_\delta B = \{a \in A : \mathrm{dist}(a, B) \geq \delta\}, A \triangle_\delta B = (A \backslash_\delta B) \cup (B \backslash_\delta A)$
  - Approximate set distance $\mathrm{ASD}(A, B) = |A \triangle_\delta B|$: Hard to construct a (reusable) secure sketch scheme
  - Quantized set distance $\mathrm{QSD}(A, B) = \mathrm{SD}(\mathcal{Q}(A), \mathcal{Q}(B))$: Errors on the boundary of quantization



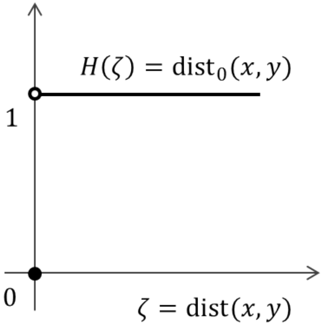


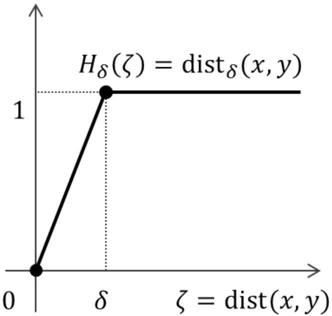
Our contributions

- Propose a new metric function
  - More reasonable measure for biometric matching than previous methods
  - Biometric system based on this metric achieves better performance indicators
- Construct a secure sketch scheme for this metric
  - Lower entropy loss independent to the size of biometric templates
  - Achieve the reusability

Indiscrete set distance

- Generalization of set distance
  - $\mathsf{SD}(A,B) = \sum_{a\in A} \mathsf{dist}_0(a,B) + \sum_{b\in B} \mathsf{dist}_0(b,A)$
    for $\mathsf{dist}_0(x,y) = \begin{cases} 0, & \text{if } x = y \\ 1, & \text{if } x \neq y \end{cases}$
  - Local distance $\mathsf{dist}_\delta(x,y) := \min\{1, \delta^{-1} \cdot \mathsf{dist}(x,y)\}$
  - $\mathsf{ISD}_\delta(A,B) := \sum_{a\in A} \mathsf{dist}_\delta(a,B) + \sum_{b\in B} \mathsf{dist}_\delta(b,A)$

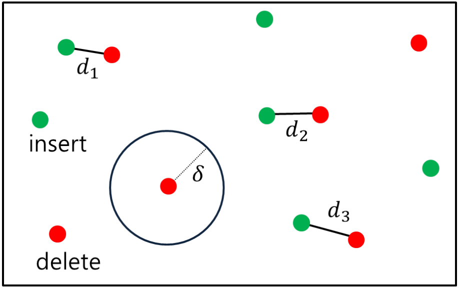




Indiscrete set distance

$$\begin{aligned}\mathrm{ISD}_\delta(A, B) &= \sum_{a\in A} \mathrm{dist}_\delta(a, B) + \sum_{b\in B} \mathrm{dist}_\delta(b, A) \\ &= \underbrace{|A \triangle_\delta B|}_{\text{insertion/deletion}} \underbrace{+\frac{2}{\delta} \cdot \sum_{\mathrm{dist}(a,b)<\delta} \mathrm{dist}(a, b)}_{\text{point-wise error}}\end{aligned}$$

- Consider both the set distance and the point-wise error
- Much more resemble a practical standard of biometric recognition



Performance indicators

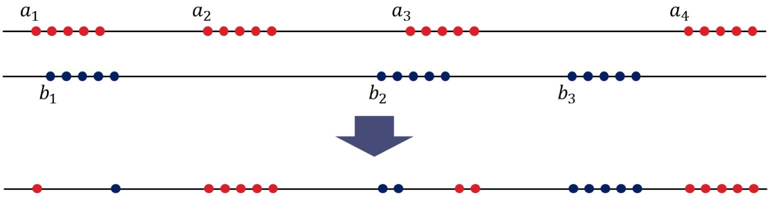
- $\mathcal{D}, \mathcal{R}$: distributions of biometric templates of genuine, random data
  τ: threshold (upper bound of tolerable error size)
- Performance indicators of a biometric system

$$\begin{aligned} \mathsf{FRR}_{\mathsf{DIST}} &= \Pr_{A,B \leftarrow \mathcal{D}}[\mathsf{DIST}(A,B) > \tau] \\ \mathsf{FAR}_{\mathsf{DIST}} &= \Pr_{A \leftarrow \mathcal{D}, R \leftarrow \mathcal{R}}[\mathsf{DIST}(A,R) \leq \tau] \end{aligned}$$

- $A \leftarrow \mathcal{D} : A = \{a_i + e_i : 1 \leq i \leq s\}, a_i \leftarrow S \subseteq \mathcal{U}, e_i \leftarrow \mathcal{E}$
  $\mathsf{FAR}_{\mathsf{DIST}} = \Theta\left(|\{R \subseteq \mathcal{U} : \mathsf{DIST}(A,R) \leq \tau\}|\right)$
- $\mathsf{FRR}_{\mathsf{ISD}_\delta}, \mathsf{FRR}_{\mathsf{ASD}} < \mathsf{FRR}_{\mathsf{QSD}}$
- $\mathsf{FAR}_{\mathsf{ASD}} = \mathsf{FAR}_{\mathsf{QSD}}$, $\log(\mathsf{FAR}_{\mathsf{QSD}}) - \log(\mathsf{FAR}_{\mathsf{ISD}_\delta}) \geq (s - \tau/2) \cdot \log \delta$

Construction of secure sketch scheme (1)

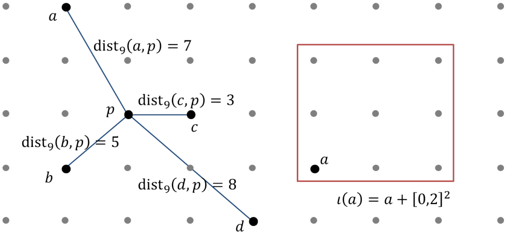
- Convert the indiscrete set distance into the set distance
  - ι is called a discretizer if $|\iota(a)| = \delta$ and $\mathrm{SD}(\iota(a), \iota(b)) = \delta \cdot \mathrm{dist}_\delta(a, b)$ for all $a, b \in \mathcal{U}$
  - $\hat{\iota}(A) := \bigcup_{a \in A} \iota(a)$
    $\mathrm{SD}(\hat{\iota}(A), \hat{\iota}(B)) = \delta \cdot |A \triangle_\delta B| + 2 \cdot \sum_{\mathrm{dist}(a,b)<\delta} \mathrm{dist}(a, b) = \delta \cdot \mathrm{ISD}_\delta(A, B)$
  - $\hat{\iota}$ is an isometry from $\delta \cdot \mathrm{ISD}_\delta(\cdot, \cdot)$ to $\mathrm{SD}(\cdot, \cdot)$



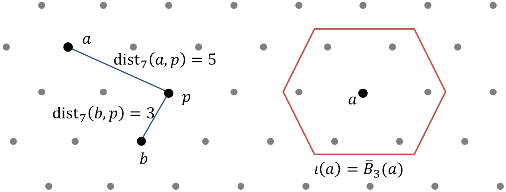
$A\Delta_\delta B = \{a_2, a_4, b_3\}$, $\mathrm{dist}(a_1, b_1) = 1$, $\mathrm{dist}(a_3, b_2) = 2$

Construction of secure sketch scheme (2)

- Square lattice



- Honeycombed lattice



- Can be generalized to higher dimensional cases

Construction of secure sketch scheme (3)

- Recall that a $(\tau, \mathcal{L})$-secure sketch scheme $(\mathsf{Enc}, \mathsf{Dec})$ on a metric space $(\mathcal{M}, \mathsf{DIST})$ satisfies the following properties:
  - $\mathsf{Dec}(B, \mathsf{Enc}(A)) = A$ if $\mathsf{DIST}(A, B) \leq \tau$
  - $\mathbf{H}_\infty(X) - \tilde{\mathbf{H}}_\infty(X|\mathsf{Enc}(X)) \leq \mathcal{L}$ for any X

Theorem

Let $(\mathsf{Enc}(\cdot), \mathsf{Dec}(\cdot,\cdot))$ be a $(\delta\tau, \mathcal{L})$-secure sketch scheme for the set distance. If ι is a discretizer, then $\left(\mathsf{Enc} \circ \hat{\iota}(\cdot), \hat{\iota}^{-1} \circ \mathsf{Dec}(\hat{\iota}(\cdot), \cdot)\right)$ is a $(\tau, \mathcal{L})$-secure sketch scheme for the indiscrete set distance.

- We also suggest a reusable secure sketch scheme for the set distance with asymptotically minimal entropy loss

Corollary

There is a reusable $(\tau, \mathcal{L} = \delta\tau \cdot \log n^d)$-secure sketch for the indiscrete set distance ISD_δ on $\mathcal{U} = [0, n)^d \cap \mathbb{Z}^d$.

Conclusion

Metric	Quantized SD	Approximate SD	Indiscrete SD
FRR	High	Low	Low
FAR	High	High	Low
Reusability	Yes	No	Yes
Entropy loss	$\tau \log n + s \log \delta$	$\tau \log n + s(1 + \log(2\delta))$	$\delta\tau \log n$

- Proposed a new metric function
  - Consider both the set distance and the point-wise error
  - Biometric security system based on this metric has better performance
- Constructed a secure sketch scheme for this metric
  - Suggested a reusable secure sketch scheme for the set distance
  - Proposed a general method using the notion of discretizer
  - Reduced entropy loss independent to the size of templates

********** THANK YOU !!!**********