香港浸會大學 HONG KONG BAPTIST UNIVERSITY

中国科学院自动化研究所 INSTITUTE OF AUTOMATION CHINESE ACADEMY OF SCIENCES

Sponsors: ICTS IAPR IEEE Biometrics Council 川大智胜 WISESOFT

IAPR/IEEE WINTER SCHOOL ON BIOMETRICS

9-13 JANUARY 2017 | HONG KONG BAPTIST UNIVERSITY, HONG KONG

Biometric Indexing

Yi Wang

alice.yi.wang@ieee.org

13/Jan/2017

Outlines

- Introduction to biometric indexing
- *Accuracy* issues: Dealing with low-quality query fingerprints
- *Efficiency* issues: Search and indexing fingerprints with compact binary codes
- *Privacy* issues: Privacy-preserving similarity search in Hamming space

Biometric Indexing

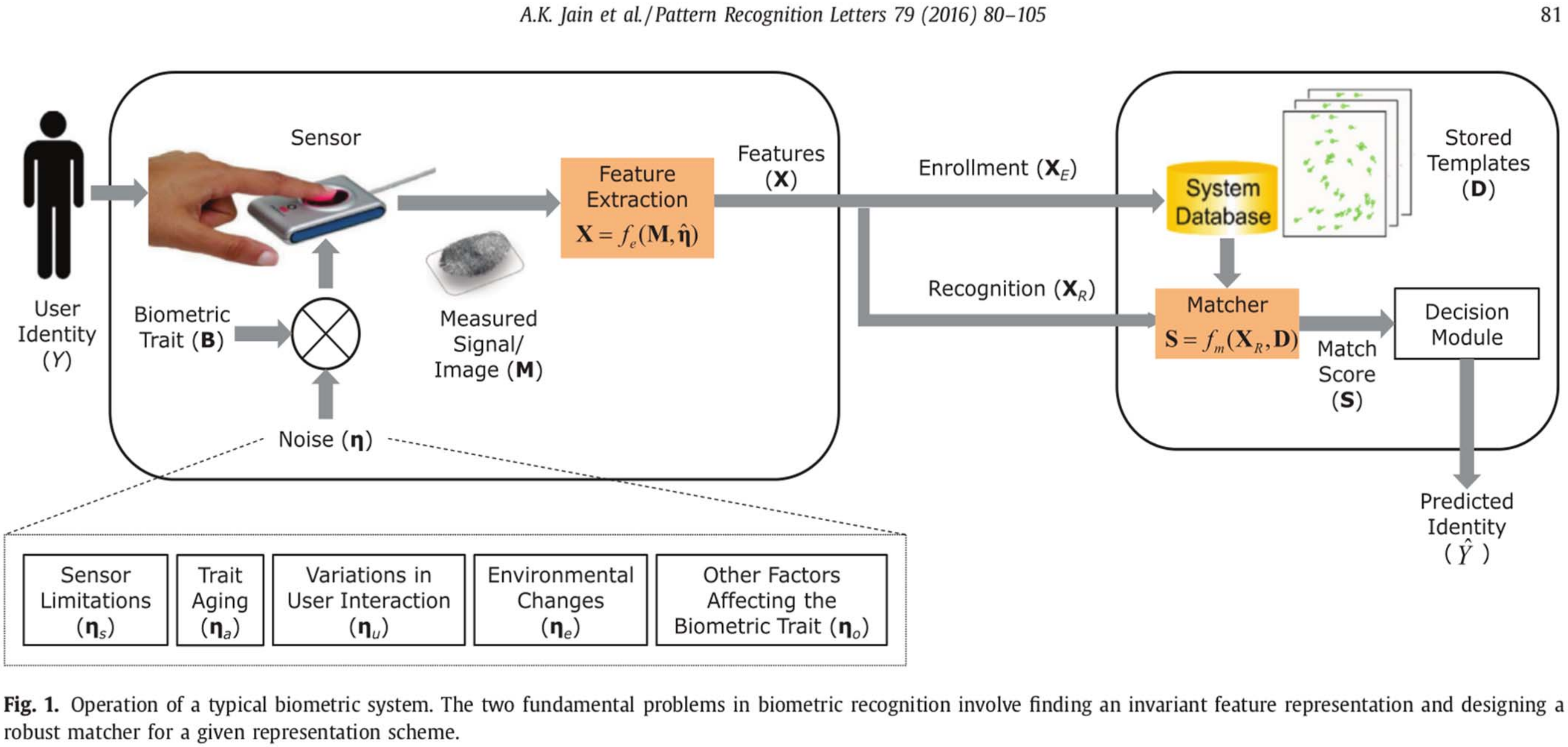
INTRODUCTION

Biometric Recognition

- Verification mode
  - Claimed identity
  - One-to-one match

- Identification mode
  - Identity to be determined
    - *Closed-set*: Output the identity
    - *Open-set*: Possibly output a nil
  - Template databases involved
  - One-to-many match

Biometric Identification System



A.K. Jain et al./Pattern Recognition Letters 79 (2016) 80–105 81

Sensor
User Identity (Y)
Biometric Trait ($\mathbf{B}$)
Noise ($\boldsymbol{\eta}$)
Measured Signal/ Image ($\mathbf{M}$)
Feature Extraction $\mathbf{X} = f_e(\mathbf{M}, \hat{\boldsymbol{\eta}})$
Features ($\mathbf{X}$)
Enrollment ($\mathbf{X}_E$)
Recognition ($\mathbf{X}_R$)
System Database
Stored Templates ($\mathbf{D}$)
Matcher $\mathbf{S} = f_m(\mathbf{X}_R, \mathbf{D})$
Match Score ($\mathbf{S}$)
Decision Module
Predicted Identity ($\hat{Y}$)
Sensor Limitations ($\boldsymbol{\eta}_s$)
Trait Aging ($\boldsymbol{\eta}_a$)
Variations in User Interaction ($\boldsymbol{\eta}_u$)
Environmental Changes ($\boldsymbol{\eta}_e$)
Other Factors Affecting the Biometric Trait ($\boldsymbol{\eta}_o$)

Fig. 1. Operation of a typical biometric system. The two fundamental problems in biometric recognition involve finding an invariant feature representation and designing a robust matcher for a given representation scheme.

Courtesy: A. K. Jain, K. Nandakumar and A. Ross, "50 years of Biometric Research: Accomplishments, Challenges, and Opportunities", *Pattern Recognition Letters*, Vol. 79, Pages 80-105, August 2016.

Fundamental Problems

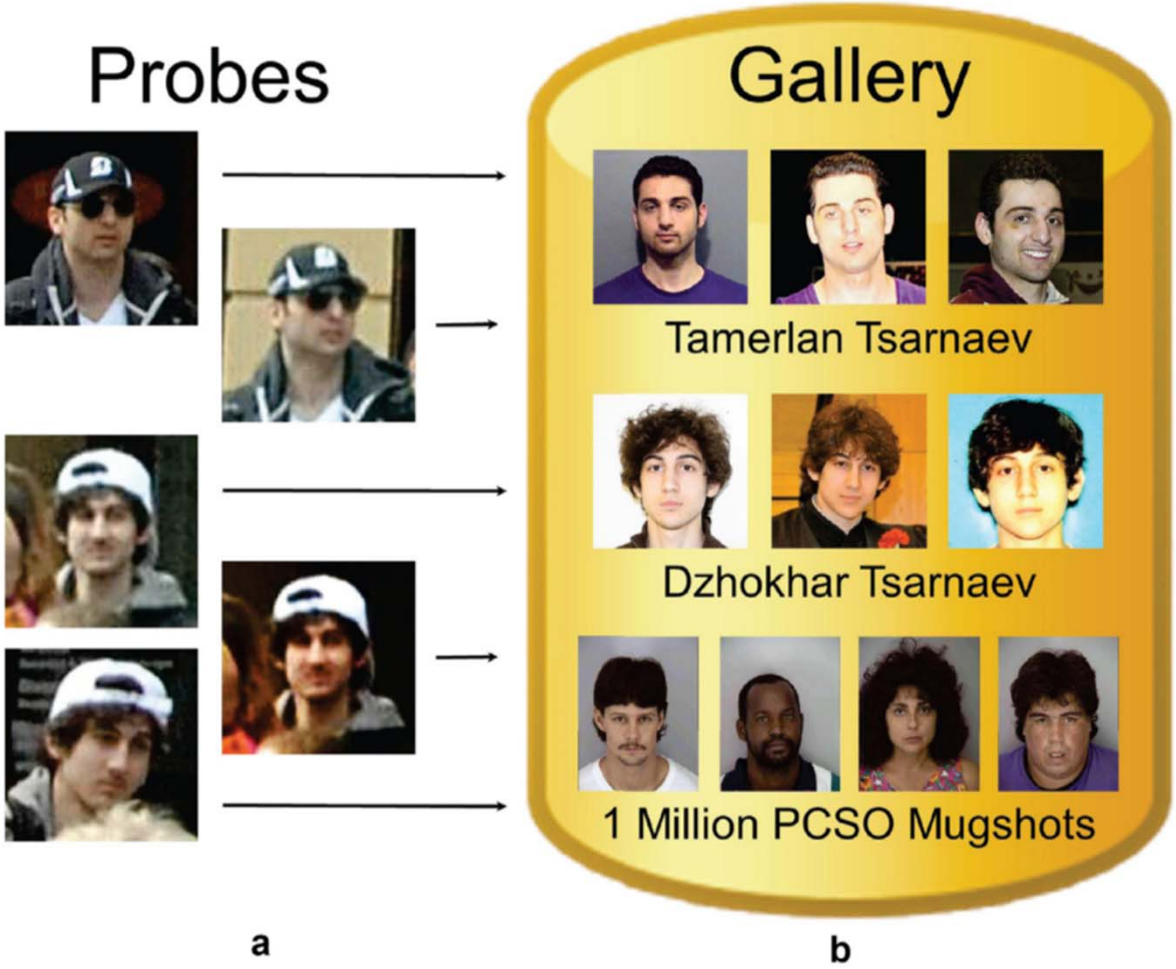
- Finding the best *feature representation* scheme for a given biometric trait
  - Retain all the discriminative information
  - Remain invariant to intra-subject variation
- Designing a *robust matcher* for a given representation scheme
  - Suitable similarity measure to minimize the recognition errors

Problems with Large Databases

- Identification by 1:N exhaustive matching does not scale well with size
- Increasing false positive identification rates with the size of database
- No established way of organizing high dimensional data
- Identification with biometric samples taken from unconstrained sensing environment

Face Identification Example

A.K. Jain et al. / Pattern Recognition Letters 79 (2016) 80–105



Results of State-of-the-Art

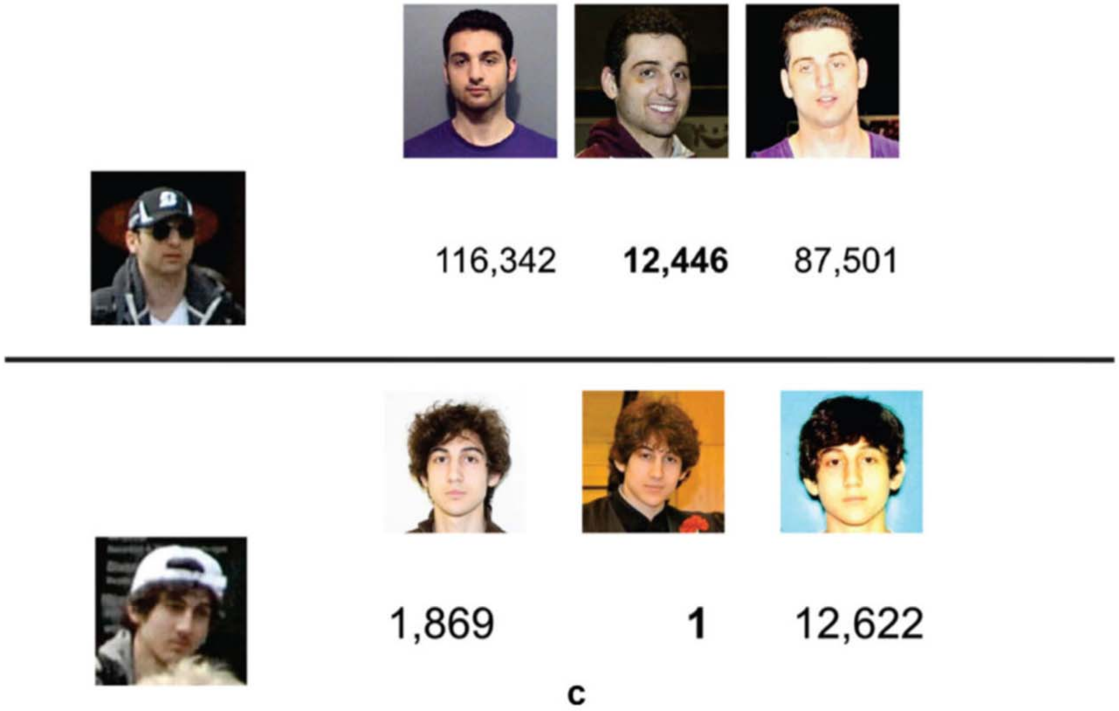
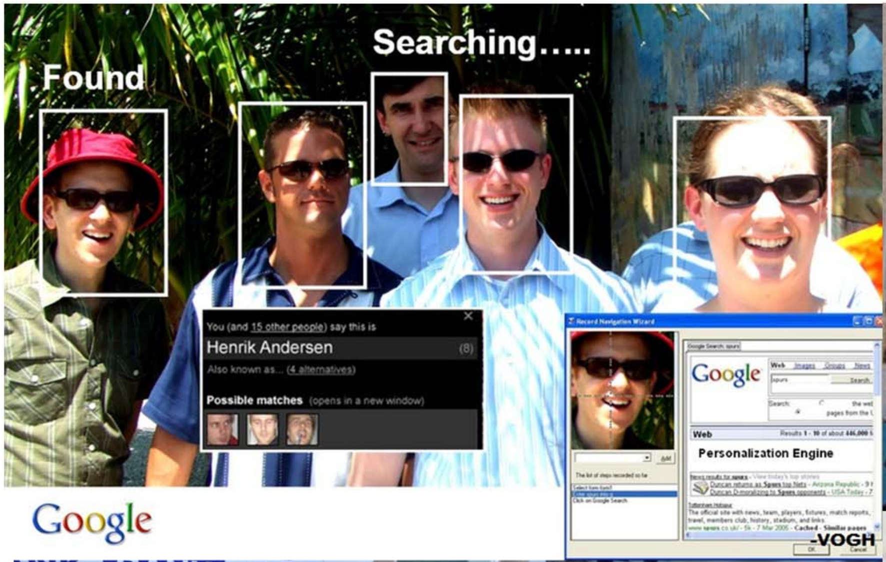


Fig. 19. A simulated example to illustrate how face recognition systems could have been used to identify the suspects in the April 2013 Boston marathon bombings [99]. (a) The five face images of the suspects obtained from surveillance videos and released by the FBI. (b) A gallery database constructed by adding three portrait images each of the two suspects (the Tsarnaev brothers) to a background database of 1 million mugshots provided by the Pinellas County Sheriff's Office (PCSO). Note that the six images added to the gallery included mugshots as well as face images of the brothers obtained from the social media. (c) The top retrieval ranks (after demographic filtering) output by a COTS face matcher when the images in (a) are used as probes to search against the gallery in (b). It was observed that one of the probe images of the younger brother (Dzhokhar Tsarnaev) matched correctly (at rank 1) with his high school graduation photograph included in the gallery.

More Applications of Identification


Found
Searching…..
You (and 15 other people) say this is
Henrik Andersen
Also known as… (4 alternatives)
Possible matches (opens in a new window)
Google
Record Navigation Wizard
Personalization Engine
-VOGH

Biometric Indexing

- To avoid an exhaustive 1:N matching by reducing the search space
- To overcome limitations of classification
  - The class of a biometric identity may be intrinsically ambiguous
  - The distribution of identities across classes may be uneven, resulting in inefficient classification
- To facilitate a rapid retrieval in the indexing feature space

Indexing Features

- Feature points and local structures
  - MCC [Cappelli et al. 2011], local texture features [Choi et al. 2012], SIFT [Mehrotra et al. 2010], learned local face descriptors [Lei et al. 2014][Lu et al. 2015]
- Global/Holistic features
  - ridge orientation model [Wang et al. 2011], deep learning features [He et al. 2015][Kan et al. 2016] [Wang et al. 2016]
- Match scores
  - match score vector [Paliwal et al. 2010], reference scores [Gyaourova et al. 2012]

Retrieval Strategies

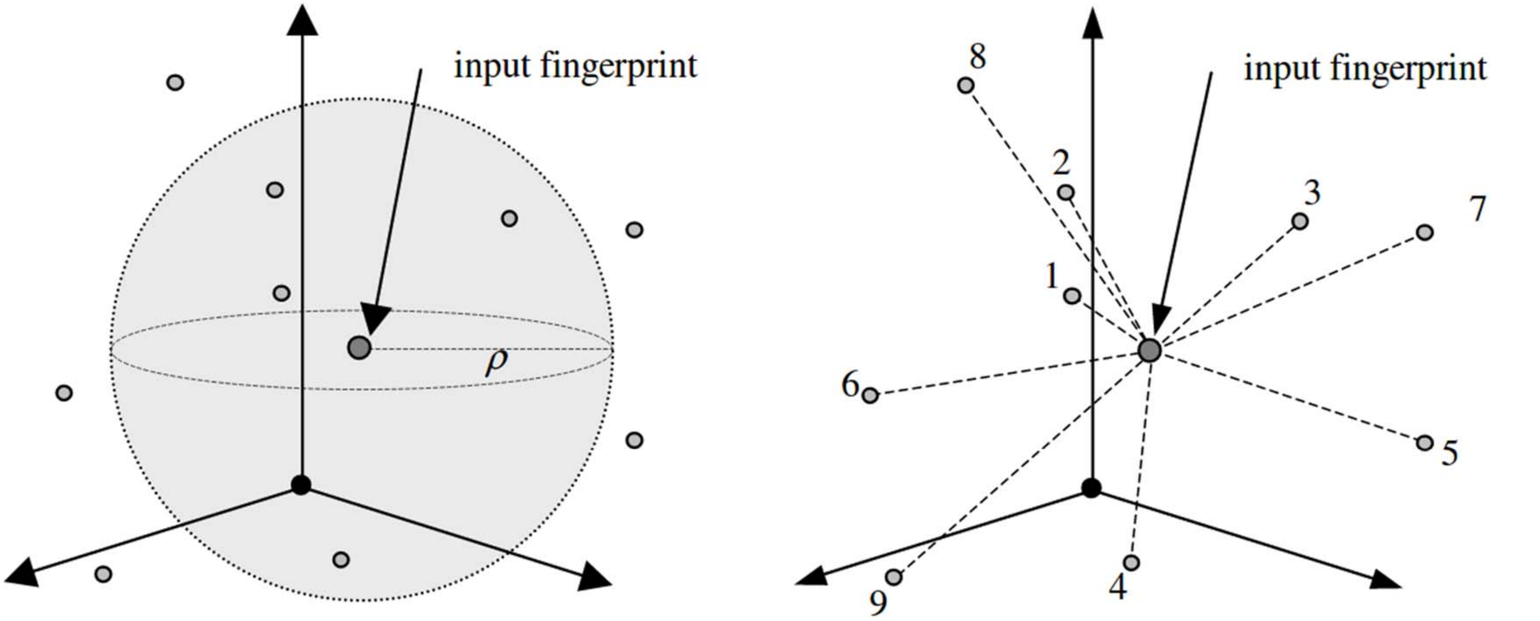


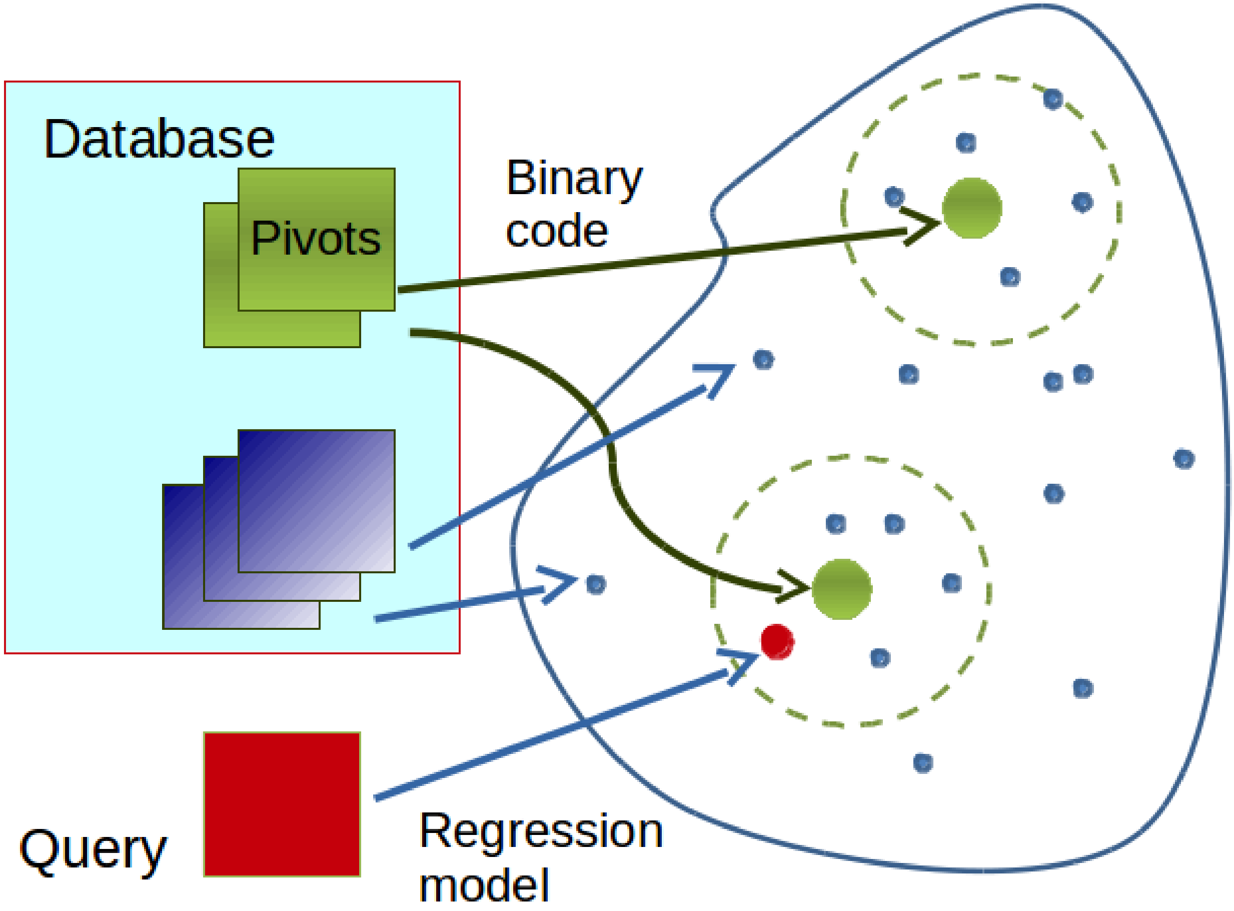
Figure 5.15. Retrieval strategies for continuous classification. On the left: the fingerprints whose corresponding vectors are inside the hypersphere are considered (*fixed radius*); on the right: the fingerprints are incrementally retrieved according to the distance of the corresponding vectors from the input point (*incremental search*).

Courtesy: D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed. Springer-Verlag, 2009, Ch. 5, pp. 264.

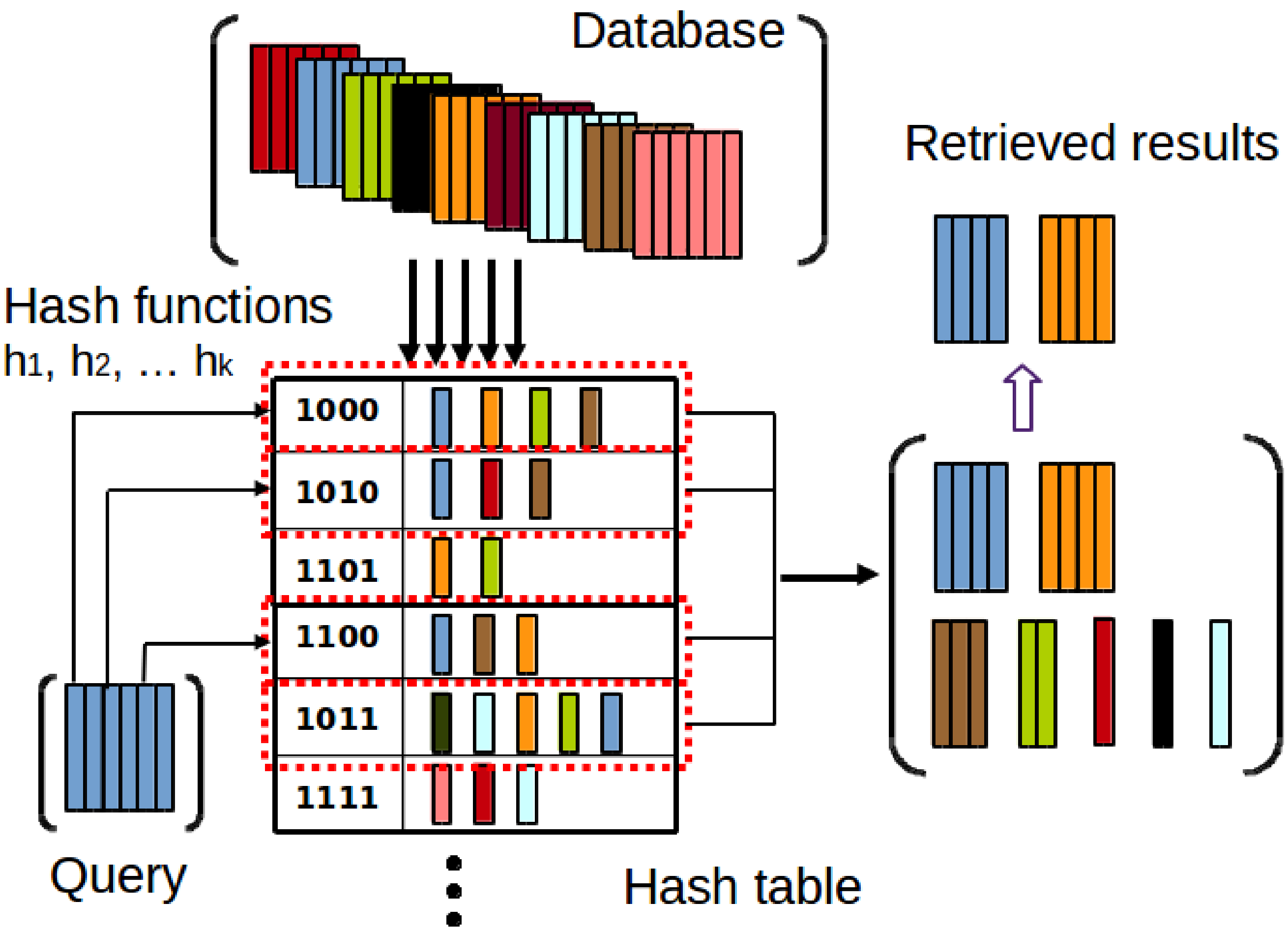
Organizing into Data Structures

- Tree-like structures [Rathgeb et al. 2015] [Procena 2013][Gyaourova et al. 2012]
  - Partitioning the feature space
  - To identify the pivots
- Hash tables [Wang et al. 2015] [Yue et al. 2013][Hao et al.2008]
  - Collision-based search by hashing similar items to the same "buckets", e.g., locality sensitive hashing (LSH)
  - To define and covert the similarity measure into collision probabilities

Partitioning-Based Search



Collision-Based Search



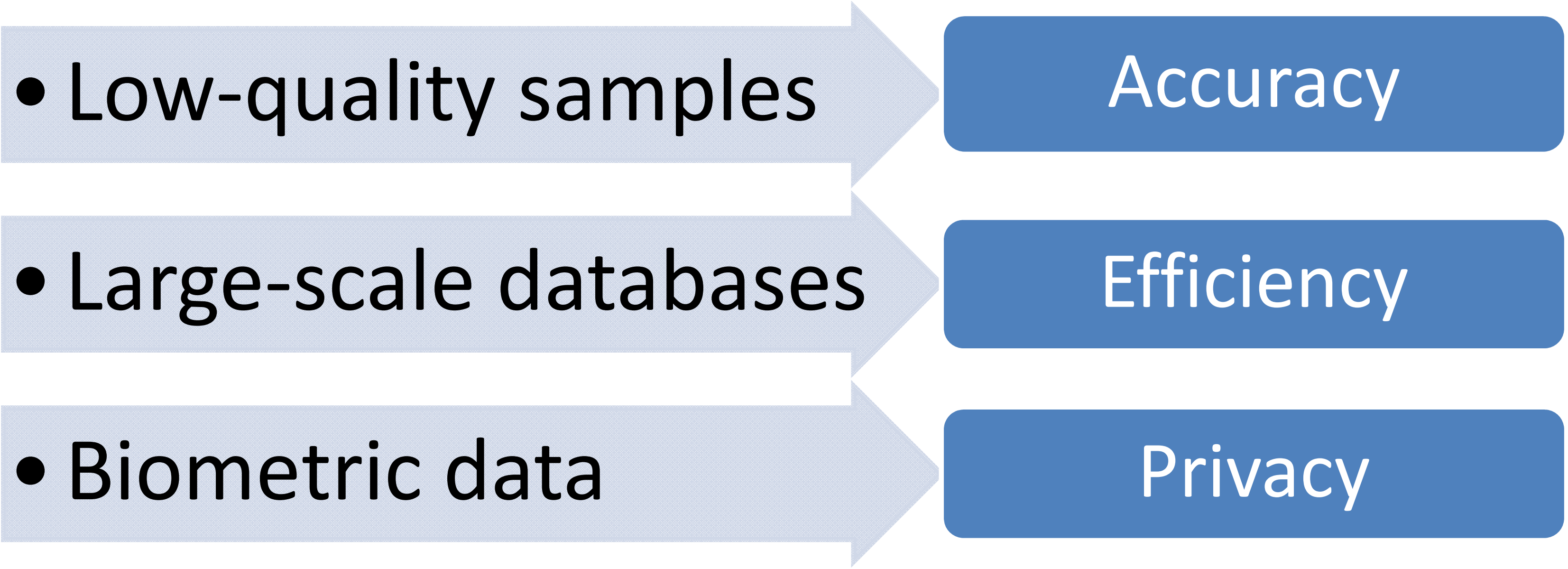
Performance Objectives

- Accuracy
  - Hit rate = $\frac{\#queries\ found\ with\ correct\ identities}{\#\ Totoal\ queries}$
- Efficiency
  - Reducing the number of comparisons
  - Reducing the cost of a single comparison
  - Penetration rate = $\frac{\#\ \ gallery\ entries\ to\ be\ retrieved}{\#\ Total\ gallery\ entries}$
- Privacy
  - Revocable for segregation and privacy
  - Safe against forgery and spoofing attacks

Key Issues

- Intra-subject variations
  - No identical match in the biometric database
  - Low-quality biometric samples for query
  - Retrieval of the *most likely* candidate(s)
- No natural order of biometric templates
  - Direct sorting of biometric data is not possible
- Indexing multi-biometric traits
  - To increase population coverage
  - To attained the desired level of performance

Performance Considerations



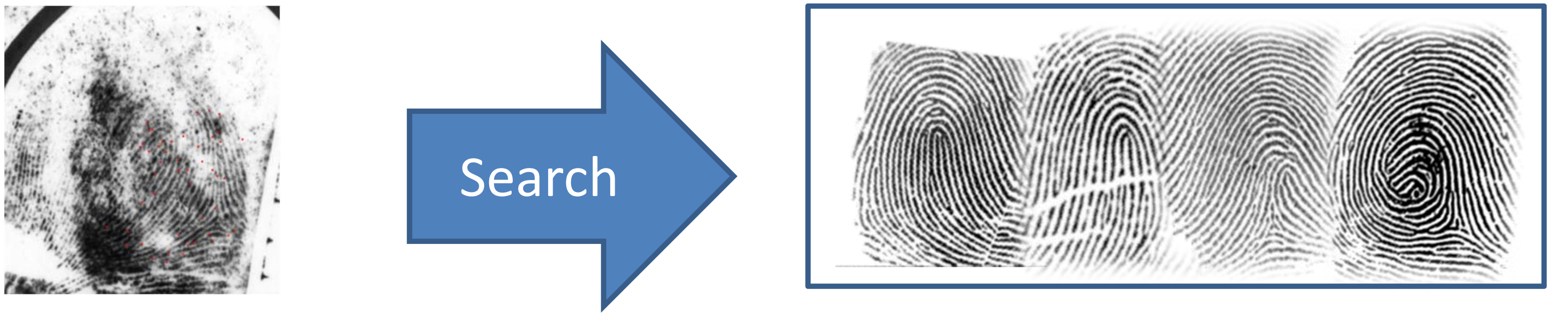
- Low-quality samples → Accuracy
- Large-scale databases → Efficiency
- Biometric data → Privacy

Biometric Indexing

DEALING WITH LOW-QUALITY QUERY FINGERPRINTS

Fingerprint Recognition Accuracy

- NIST evaluations and the various editions of FVC tests show that [Jain et al. 2016]
  - Plain-to-plain matching is of 99.4% accuracy
  - Latent-to-plain matching is of 64.4% accuracy



Search

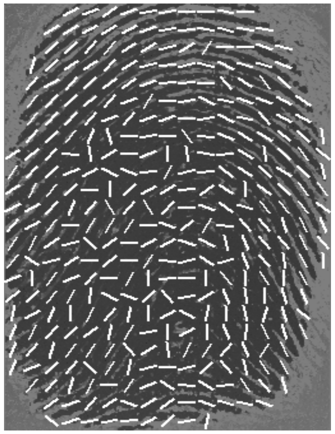
Latent fingerprint

Rolled/Plain fingerprint database

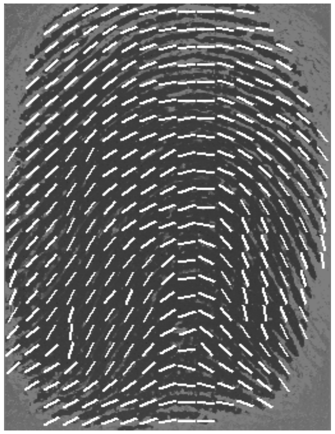
Ridge Orientation Modelling

- Ridge orientation estimation

Gray-scale image



Coarse estimates



Reconstructed ROF

- Use mathematical functions to describe the ridge orientation field (ROF)
  - Enhancing fingerprint image quality with refined ROF
  - Typically require prior knowledge of singular points for which the detection process is often error-prone

Fingerprint Orientation Model based on 2D Fourier Expansions (FOMFE)

- Models the transformed ROF as a phase portrait of an *unknown* dynamic system $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$
- Singular points are modeled as critical points of the dynamic system
- A functional repr $\mathbf{f}(\mathbf{x}_o) = 0$ n enables more uses
  - Singular point detection and feature analysis
  - Model-based fingerprint indexing

Y. Wang, J. Hu and D. Phillips, "A fingerprint orientation model based on 2D Fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing", *IEEE Trans. Pattern Analysis and Machine Intelligence, Special Issue on Biometrics: Progress and Directions*, vol. 29, no. 4, pp. 573-585, April 2007.

Model-Based Fingerprint Indexing

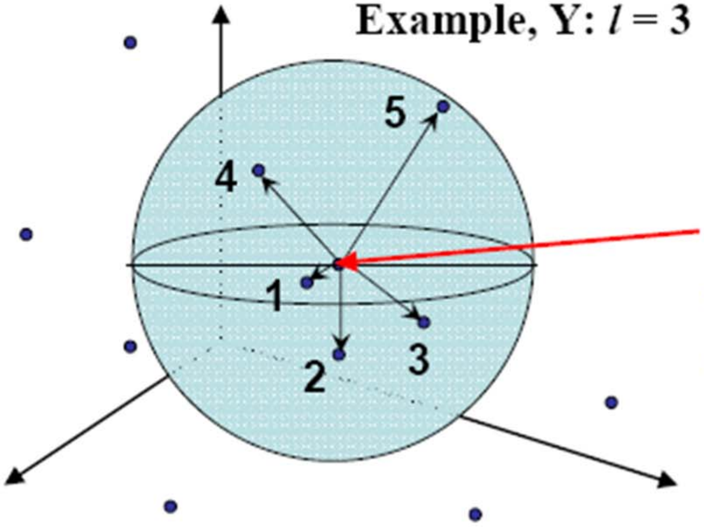
Step 1. Training the Indexing Feature Space

$$\mathbf{x}_i = [\beta_c; \beta_s] \Rightarrow \mathbf{X} = \underbrace{\left[\mathbf{x}_1,\ \mathbf{x}_2,\ \ldots,\ \mathbf{x}_N\right]}_{\text{Original feature space}} \Rightarrow \Phi_l = PCA(\mathbf{X}, l)$$

$$\mathbf{y}_i = \Phi_l^T \times \mathbf{x}_i$$

$$\mathbf{Y} = \underbrace{\left[\mathbf{y}_1, \mathbf{y}_2,\ \ldots,\ \mathbf{y}_N\right]}_{\text{Indexing feature space}}$$

Step 2. Candidate Retrieval



Query projection

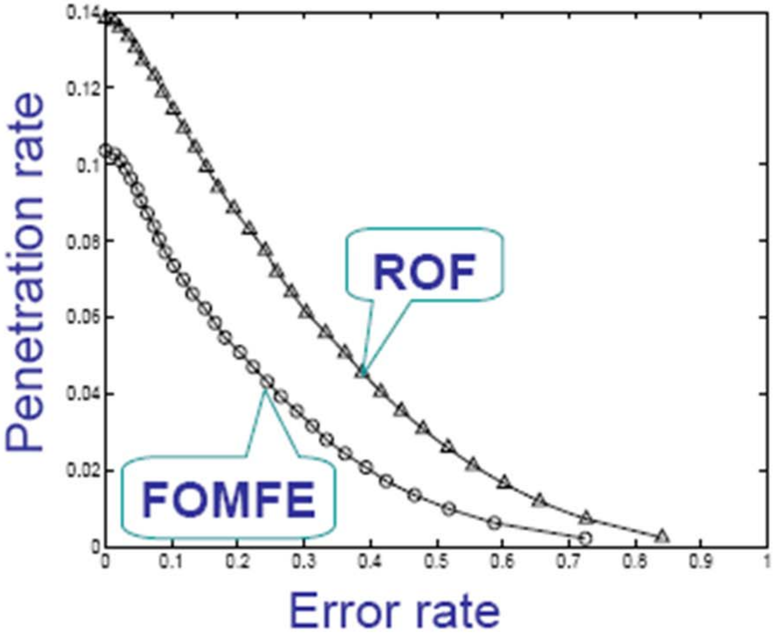
$$\mathbf{y}_q = \Phi_l^T \times \mathbf{x}_q$$

Visiting list: 1, 2, 3, …
(until a match is found)

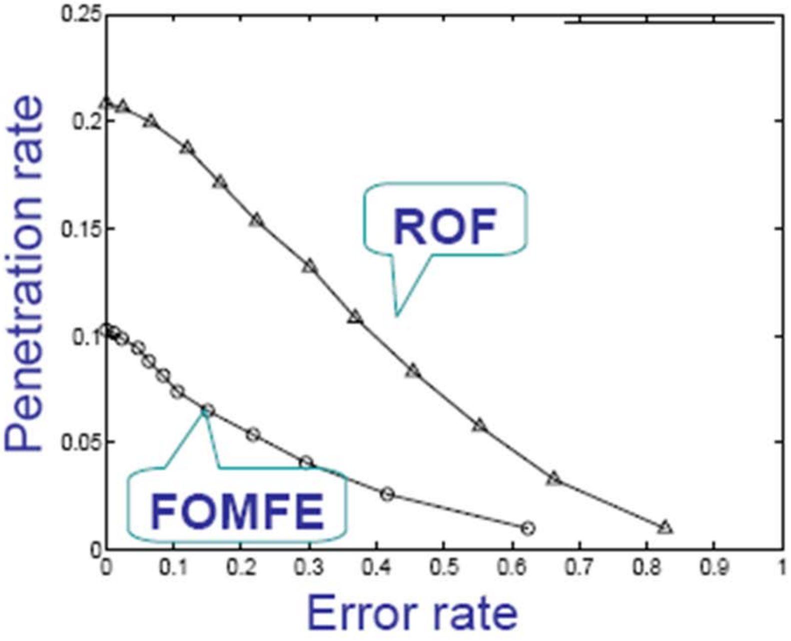
Performance Evaluation

Feature vector length: 162 (FOMFE) vs. 1,920 (ROF)

CPU time: 0.78 sec (FOMFE) vs. 1103.22 sec (ROF) to generate the indexing feature space on 2, 700 gallery prints



5, 400 ink-rolled prints from NIST Special DB 14



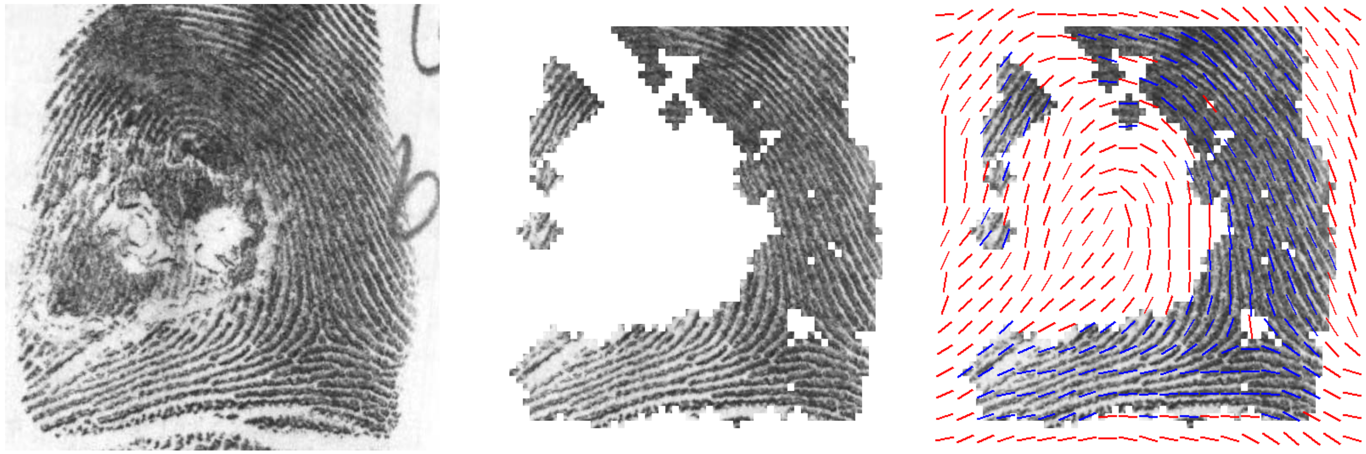
800 optical-scanned prints from FVC2002 DB1a

Partial fingerprint Identification

- Matching with partial fingerprint is a critical challenge
- Identifying them from large databases is even more difficult
- Manual inspection is still indispensible

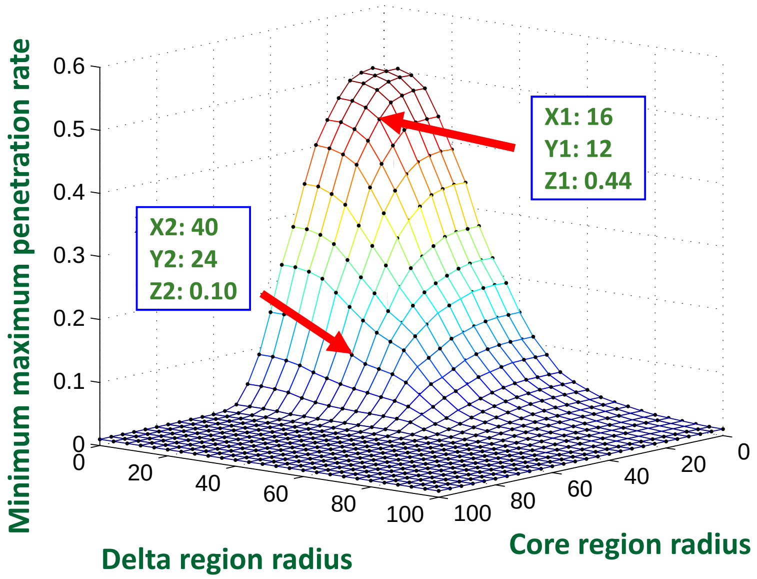
Partial Fingerprint Reconstruction

- We proposed to reconstruct the topological structure of ridge patterns to facilitate indexing with partial fingerprints

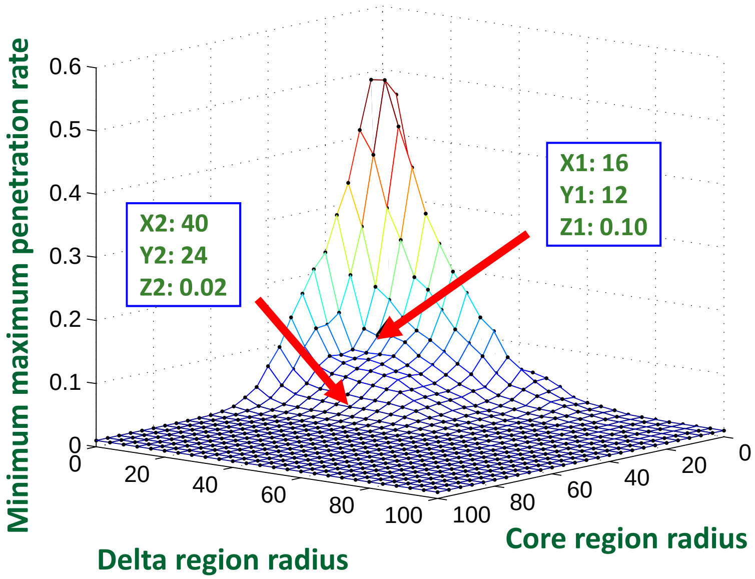


Y. Wang and J. Hu, Global ridge orientation modeling for partial fingerprint identification, *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 33, no.1, pp.72-87, Jan. 2011.

Indexing Performance



(a) Indexing without global estimation



(b) Indexing with global estimation

- Generate partial fingerprints by segmenting the core and delta regions of the gallery fingerprints with different size.
- 26x26=676 query sets, each has 100 partial fingerprint.

Biometric Indexing

SEARCH AND INDEXING FINGERPRINTS WITH COMPACT BINARY CODES

Motivations

- Vast data collections & frequent access demands
  - Border control, e.g., US-VISIT
  - National ID programs, e.g., UIDAI
- Computation intensive tasks, e.g., identity de-duplication
  - Essential in large-scale biometric systems
  - Typically involves cross-matching with $O(N^2)$
  - Bottleneck with big data volume
- At the core is the search on biometric features
  - Increasing the speed of every comparison
  - Reducing the total number of comparisons

Binary Feature Representations

- Biometric indexing methods using real-valued feature vectors focus on
  - Dimensionality reduction of biometric features
  - Similarity preserving transforms
- Binary representations of biometric features
  - Fast operations: 1 million comparisons per second
  - Typically long bit-length, e.g., 2048-bit iris code, 384-bit MCC per minutiae point
  - Typically an exhaustive search by sequential matching
  - Not all biometric features can be easily encoded into fixed-length binary string representations

NN Search in Hamming Space

- Long binary representations are problematic for large-scale searches
  - the Hamming-ball volume becoming prohibitive to explore
  - risk that many queries may not find any neighbor within the restricted volume
  - leading to a low recall because the collision probability decreases exponentially with an increasing code length

Hashing Biometric Features

- Various hash codes were developed for the similarity search of natural images, BUT
  - searching biometric identities requires higher retrieval accuracy
  - the indexing feature of a probe is not likely to be identical to that of the corresponding identity in the database
  - for fingerprints in particular, feature points are unordered and their number is unfixed

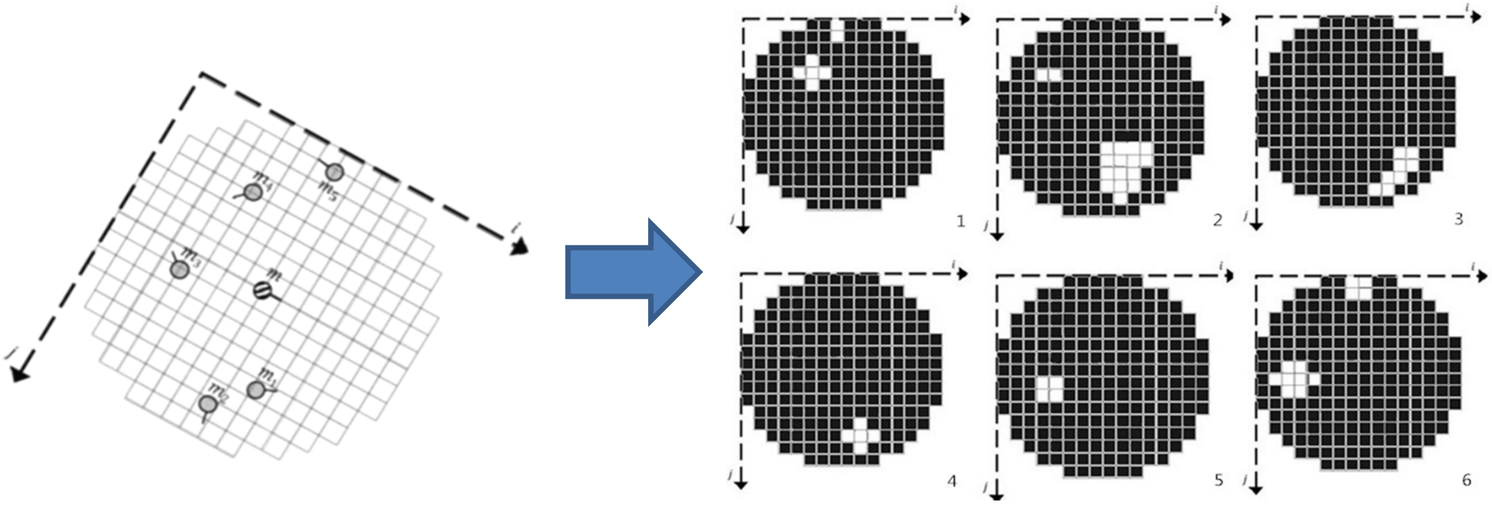
Learning Compact Binary Codes for Hash-Based Fingerprint Indexing

- How to optimally embed the input data into Hamming space heavily depends on the *data characteristic*
- Systematically learning compact binary codes in an integrated framework with nearest neighbor search procedures

Y. Wang, L. Wang, Y.-M. Cheung and P. C. Yuen, "Learning compact binary codes for hash-based fingerprint indexing", *IEEE Trans. Information Forensics and Security*, vol. 10, no. 8, pp. 1603-1616, Aug. 2015.

Minutiae Cylinder Code (MCC)

- A translation and rotation invariant local feature descriptor derived from the standard minutiae template
- Encoding the local neighborhood information of each minutiae point into a 3D data structure
- Binary implementation by thresholding the cell values into a 384-bit vector

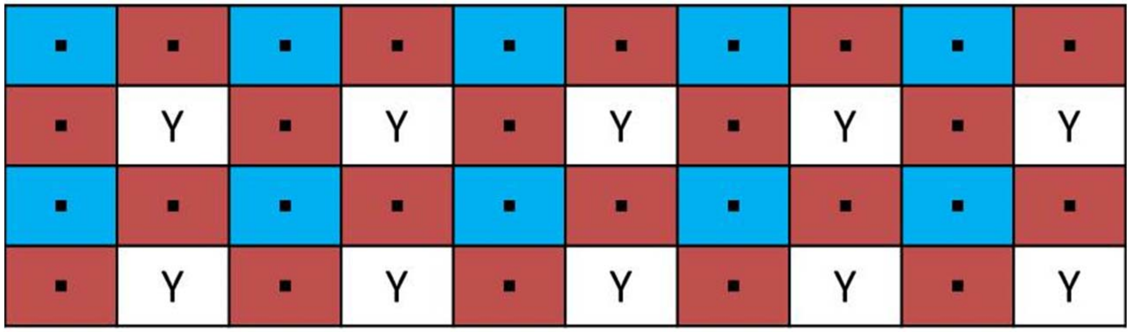


Data Characteristics of MCC

- About 95% of MCC bits are zeros on average
- The entropy per MCC bit is approximately 0.3
- There are bit dependencies in MCC
  - The cell values are obtained from accumulating contributions of minutiae in the neighborhood
  - Side lopes of the distance function extend the minutiae contributions to adjacent cells, thus correlated cell values

Modelling Bit Correlations

- Markov random field to capture bit correlations



▪	▪	▪	▪	▪	▪	▪	▪	▪	▪
▪	Y	▪	Y	▪	Y	▪	Y	▪	Y
▪	▪	▪	▪	▪	▪	▪	▪	▪	▪
▪	Y	▪	Y	▪	Y	▪	Y	▪	Y

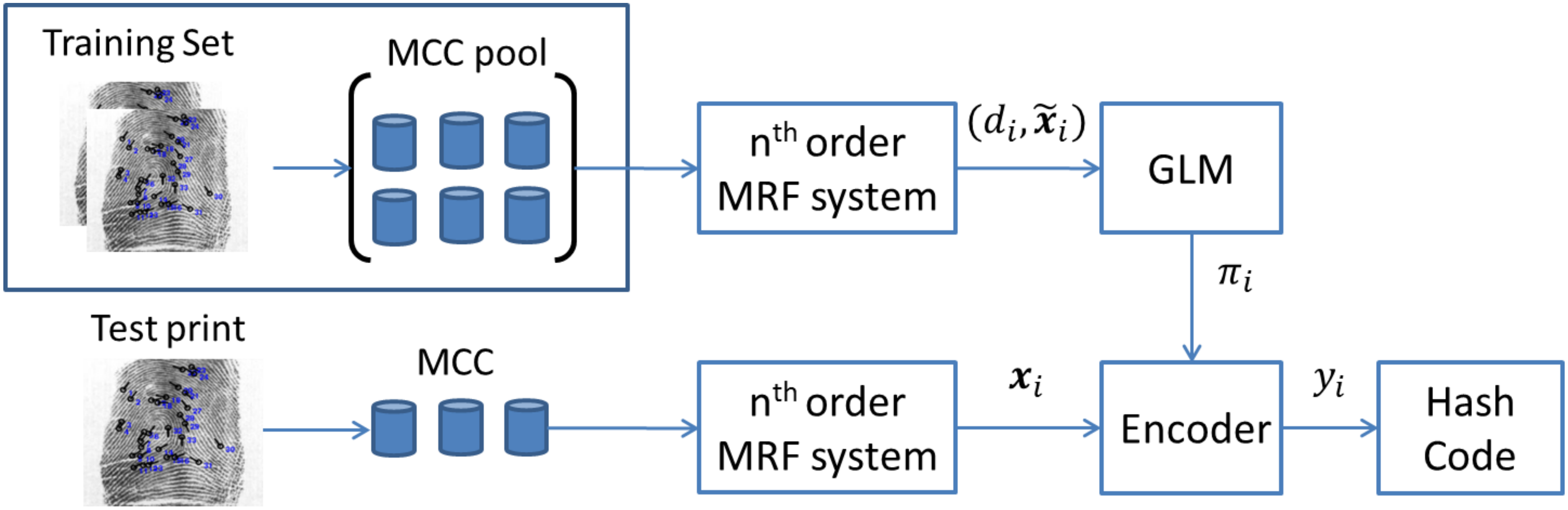
Coding of a 2nd order MRF system. The “Y” sites are mutually independent in the presence of the “.” sites

- Hashing the neighborhood information into a single bit by quantizing the expected value at each “Y” site

$$E(Y_i) = g(\mathbf{x}_{\mathcal{N}_i}|\theta),$$

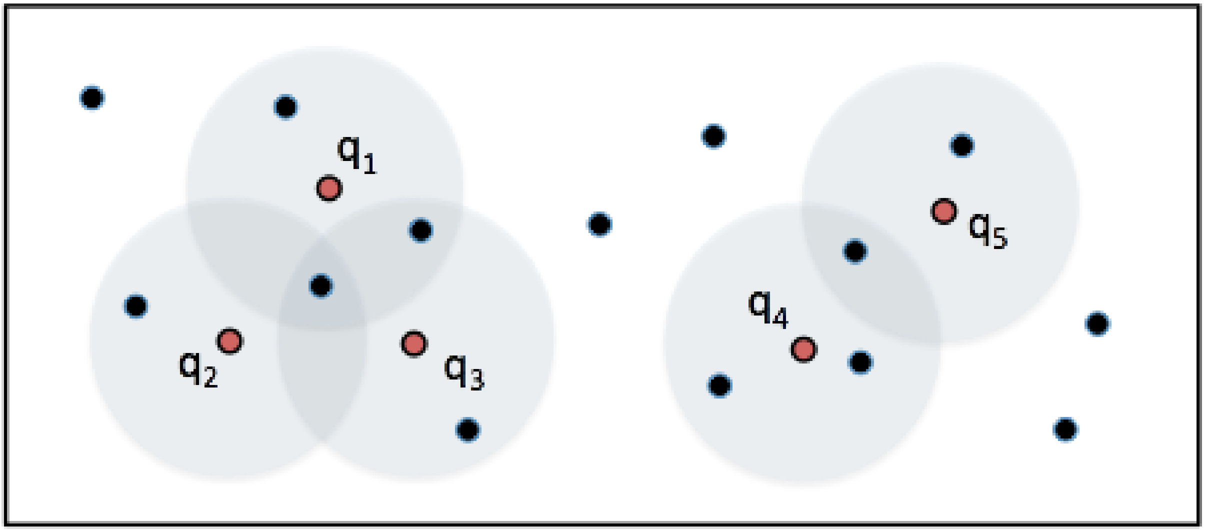
Learning Hash Bits from GLM

- Without knowing θ, a generalized linear model (GLM) links the random variables to the explanatory terms with a small set of parameters


Training Set
MCC pool
n^{th} order MRF system
$(d_i, \tilde{\boldsymbol{x}}_i)$
GLM
π_i
Test print
MCC
n^{th} order MRF system
$\boldsymbol{x}_i$
Encoder
y_i
Hash Code

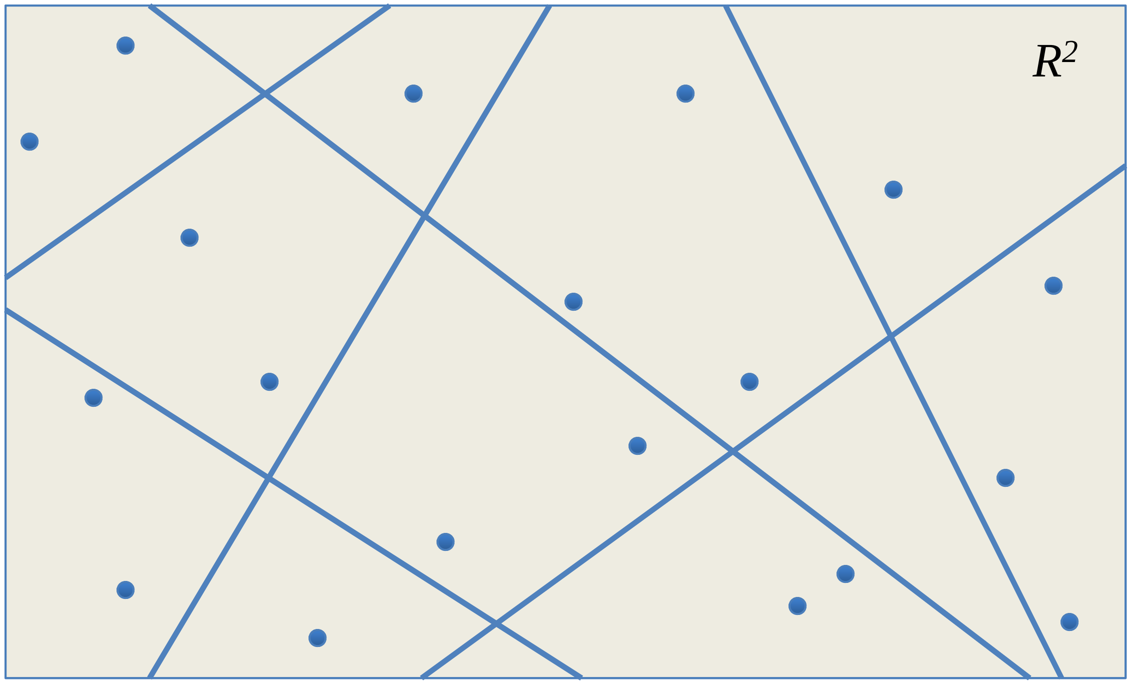
Hash-Based Fingerprint Indexing

- Fingerprint templates are indexed by an unordered set of minutiae represented in binary hash codes
- Each minutiae creates a Hamming-ball search
- Nominate the most likely match by collecting evidence from all the Hamming-ball search of a query



Locality Sensitive Hashing

- Hash similar points into the same ``buckets’’ by random projections
- Colliding segments in at least some of the buckets



LSH problems:

- Long hashes and more index tables
- Not efficient for non-uniformly distributed points

Geometric Hashing

- Recognition based on maximum collisions of similar local invariants and their geometric relations
- Previous fingerprint geometric hashing algorithms
  - Mostly based on constructing minutiae triangulations: sensitive to noise and distortion
  - Same local geometric invariants for both index creation and feature comparisons
  - Accuracy depending on more geometric invariants
  - **Real-valued** and high-dimensional feature descriptors
  - Only local information used
  - Problematic if two fingerprints have small overlaps

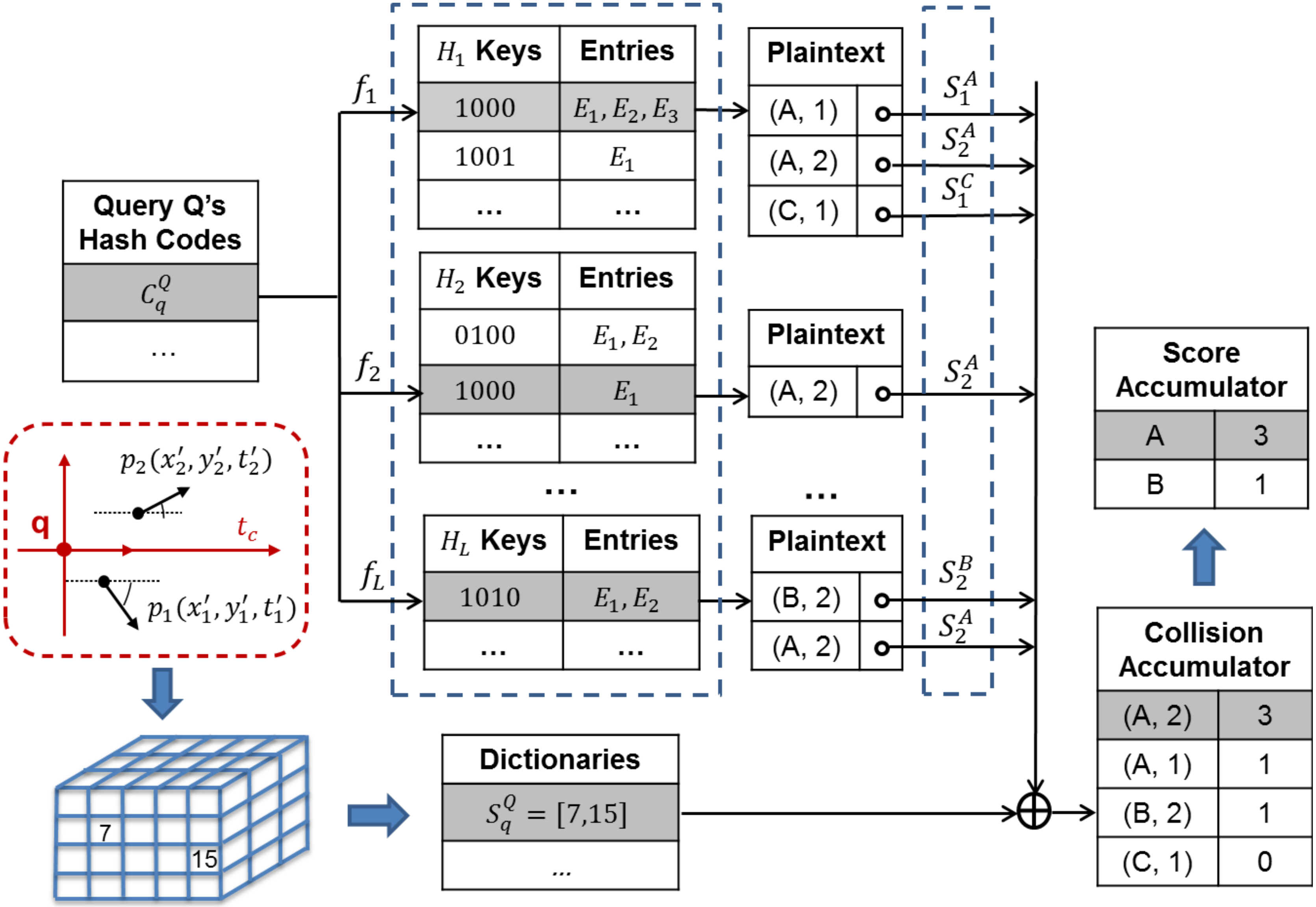
Geo-MCC

- MCC as the local invariants at each basis point
- Access keys by basis-defined triplets (x, y, θ)
  - Multiple views of the local invariants from different perspectives (i.e., access points)
  - Collectively, the access keys of a probe describe the *global* geometric configuration

Y. Wang, L. Wang, Y.-M. Cheung and P. C. Yuen, "Fingerprint geometric hashing based on binary minutiae cylinder codes", in *Proc. IEEE Intl. Conf. Pattern Recognition* (ICPR'14), Stockholm, Sweden, Aug. 20, pp. 690-695.

Geo-LSH

- Limitations of Geo-MCC:
  - An uneven distribution of database entries over a few hash bins
  - The point matching is based on MCC comparisons
- Combine the merits of LSH and geometric hashing for fingerprint indexing
  - LSH helps to distribute binary codes more evenly to buckets by random bit sampling
  - Geometric hashing incorporates relative spatial configuration of the local invariants



Query Q's Hash Codes
C_q^Q
…

H_1 Keys	Entries
1000	E_1, E_2, E_3
1001	E_1
…	…

Plaintext
(A, 1)
(A, 2)
(C, 1)

H_2 Keys	Entries
0100	E_1, E_2
1000	E_1
…	…

Plaintext
(A, 2)

H_L Keys	Entries
1010	E_1, E_2
…	…

Plaintext
(B, 2)
(A, 2)

Dictionaries
$S_q^Q = [7,15]$
…

Score Accumulator	
A	3
B	1

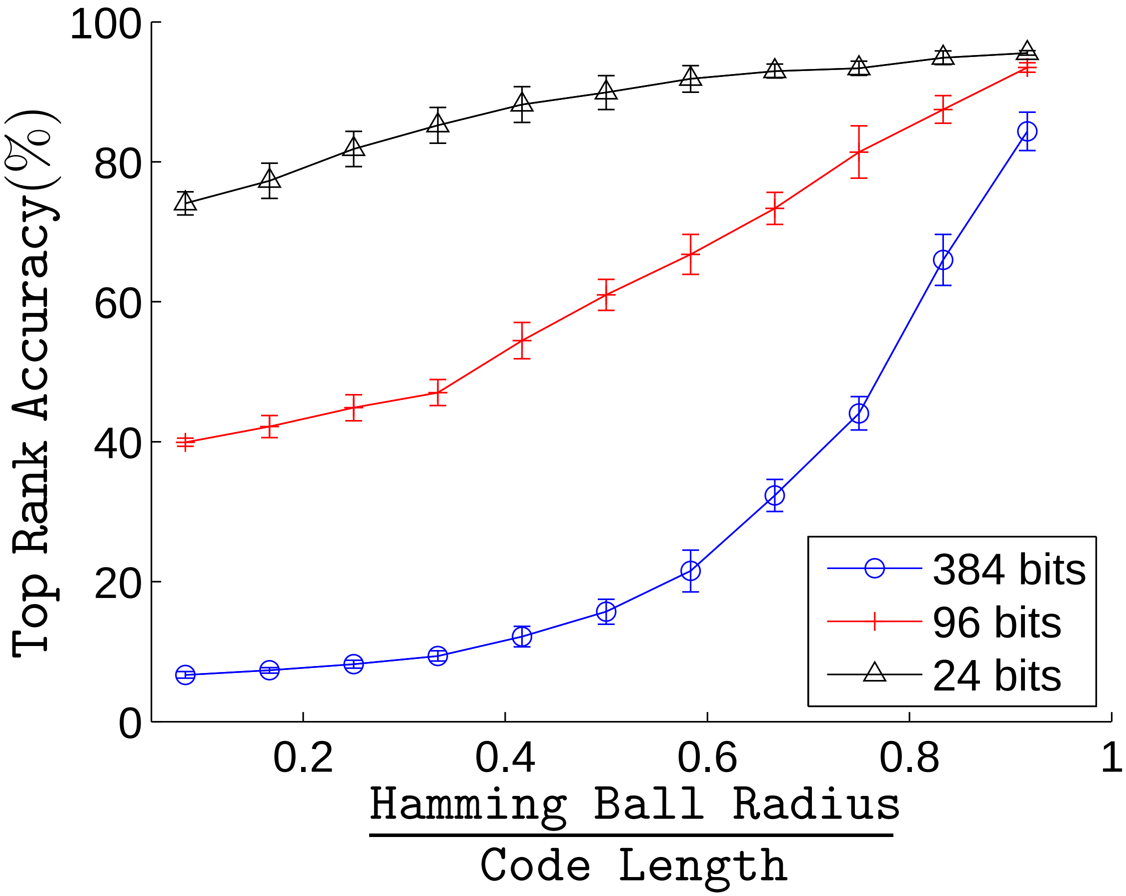
Collision Accumulator	
(A, 2)	3
(A, 1)	1
(B, 2)	1
(C, 1)	0

A hierarchical collision-based fingerprint indexing approach

Indexing Experiments

- FVC2002 DB1a and NIST DB14
  - FVC 8x100 live-scanned fingerprints
  - NIST 2x2700 ink-rolled fingerprints
- Performance measures
  - Hit rate (accuracy) vs. Penetration rate (efficiency)
- Binary MCC features
  - MCC SDK v1.3 available from http://biolab.csr.unibo.it
  - Minutiae extracted by VeriFinger v6.6

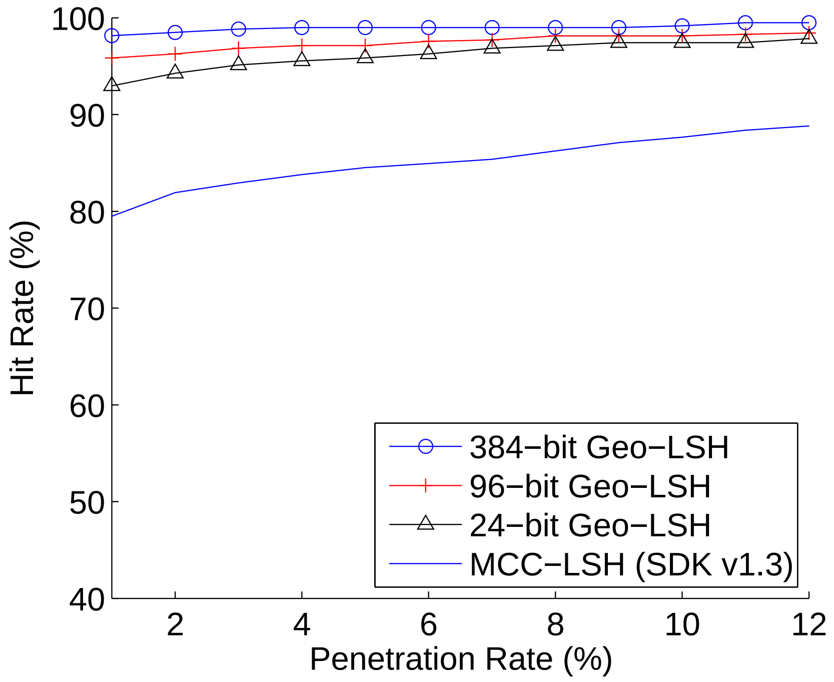
Hamming-Ball Search Accuracy



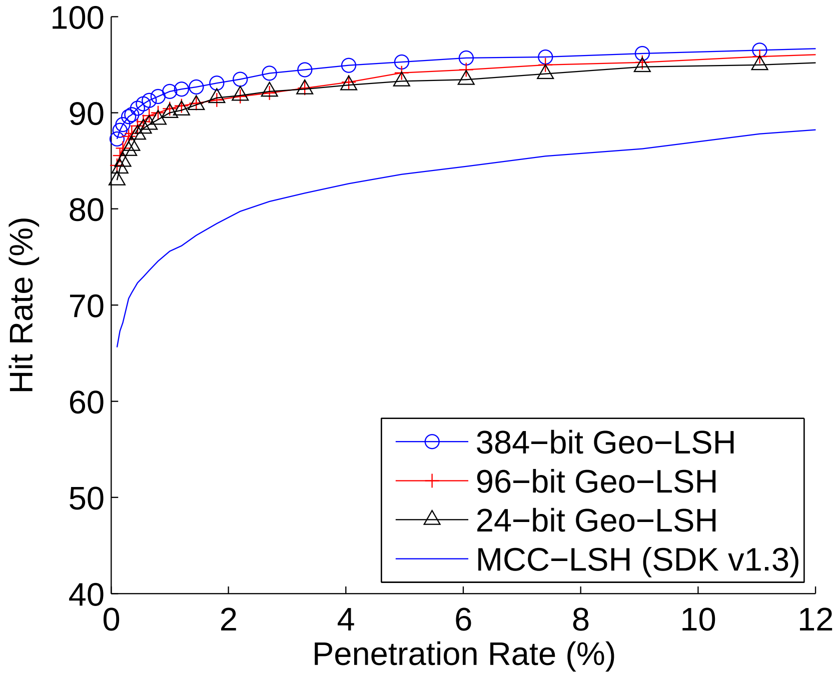
ANN search performance with respect to Hamming-ball radius for binary codes

Indexing Performance

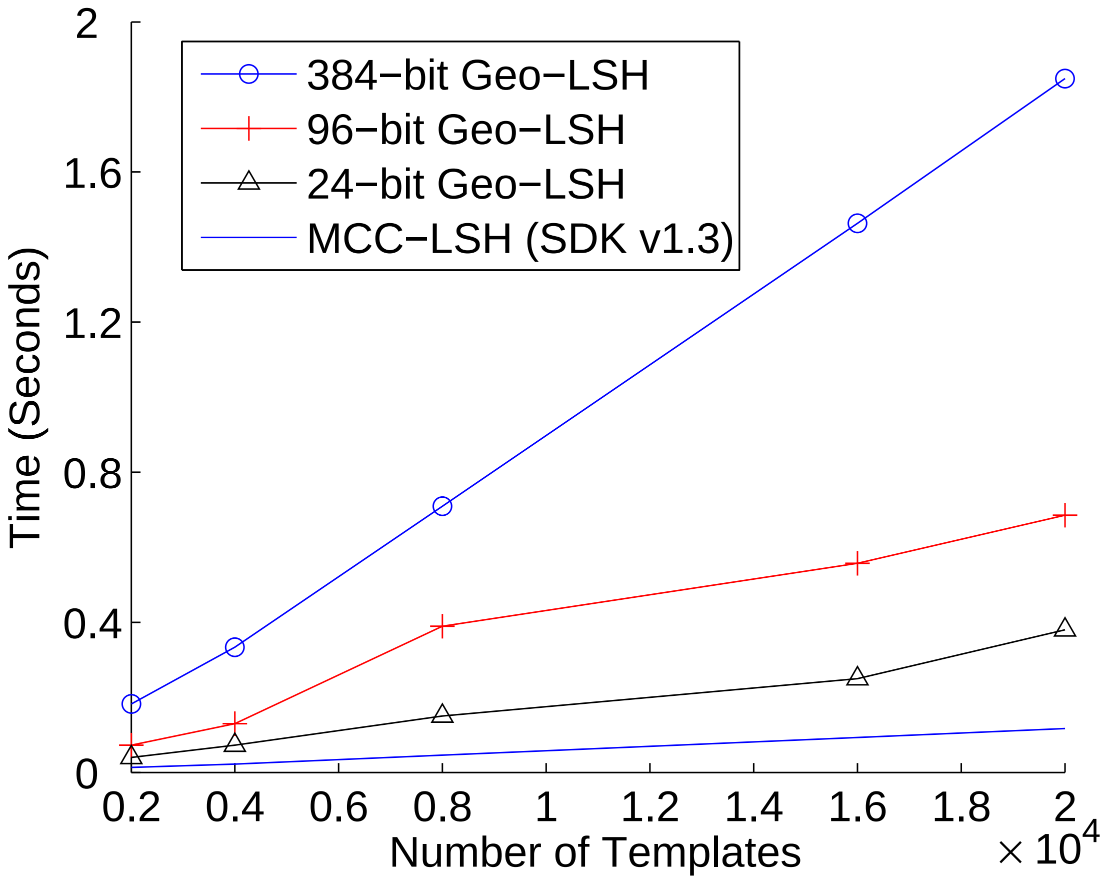
FVC2002 DB1



NIST SD14



Scalability and Time Efficiency



Average time of searching one query against an increasing data set

Biometric Indexing

PRIVACY-PRESERVING SIMILARITY SEARCH IN HAMMING SPACE

Motivations

- NN methods reduce the matching complexity by using data structures
- Two vulnerabilities that can lead to privacy infringements:
  - Statistical information, e.g., clustering patterns and feature similarity information, may be derived by analyzing search indexes in the data structures
  - Similarity distribution of the genuine users may enable adversarial learning of biometric features and lead to severe security attacks

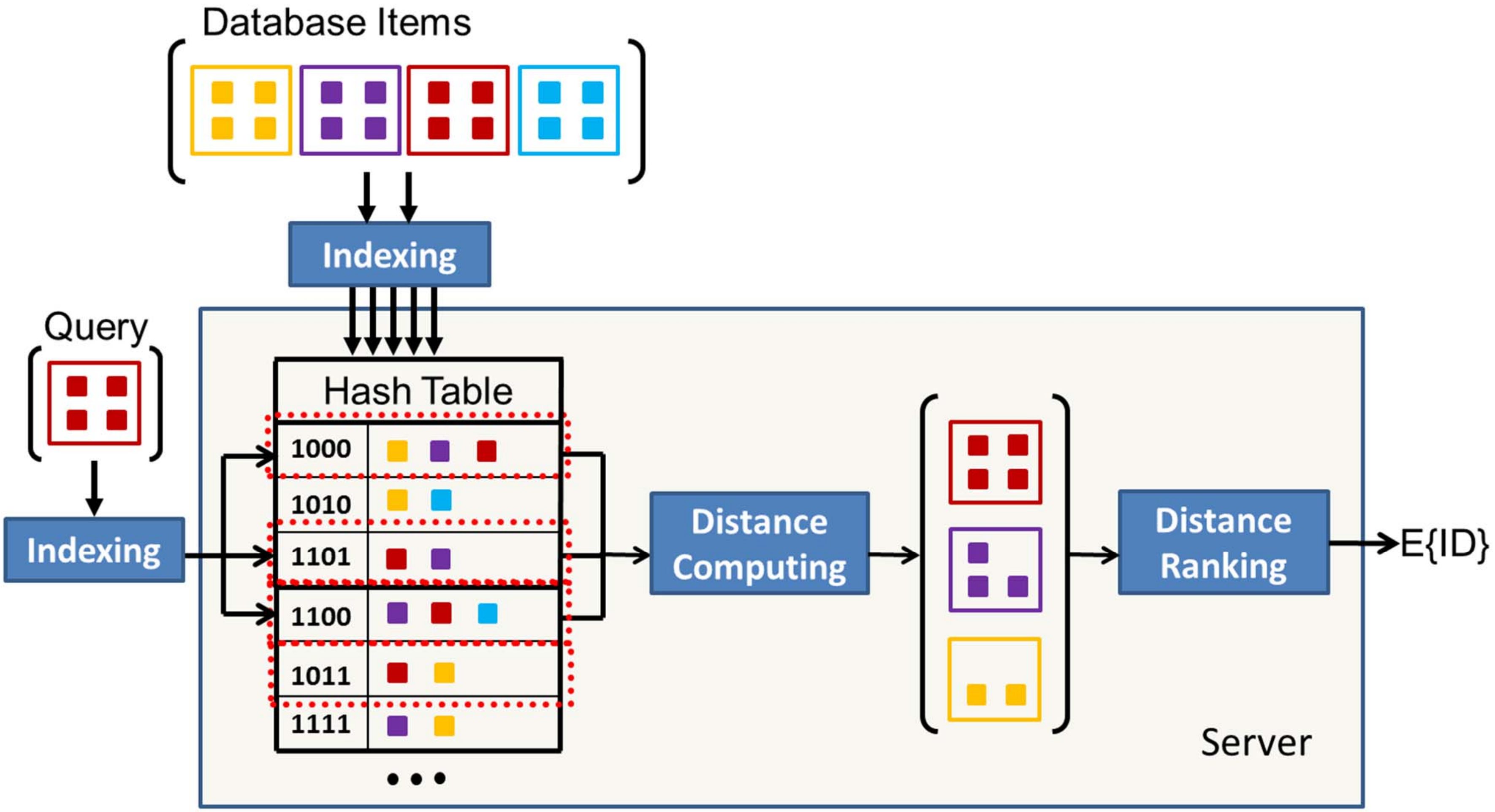
Adversarial Biometric Recognition

- The genuine biometric similarity information may be exploited to compromise system operations[Biggio et al. 2015]
  - Hill-climbing attacks: Effective spoofing with a fabricated reference can be constructed from similarity scores
  - Presentation attacks: Multi-biometric systems may be evaded by spoofing a single biometric trait, if $p(S_F) = p(S_G)$

Challenges

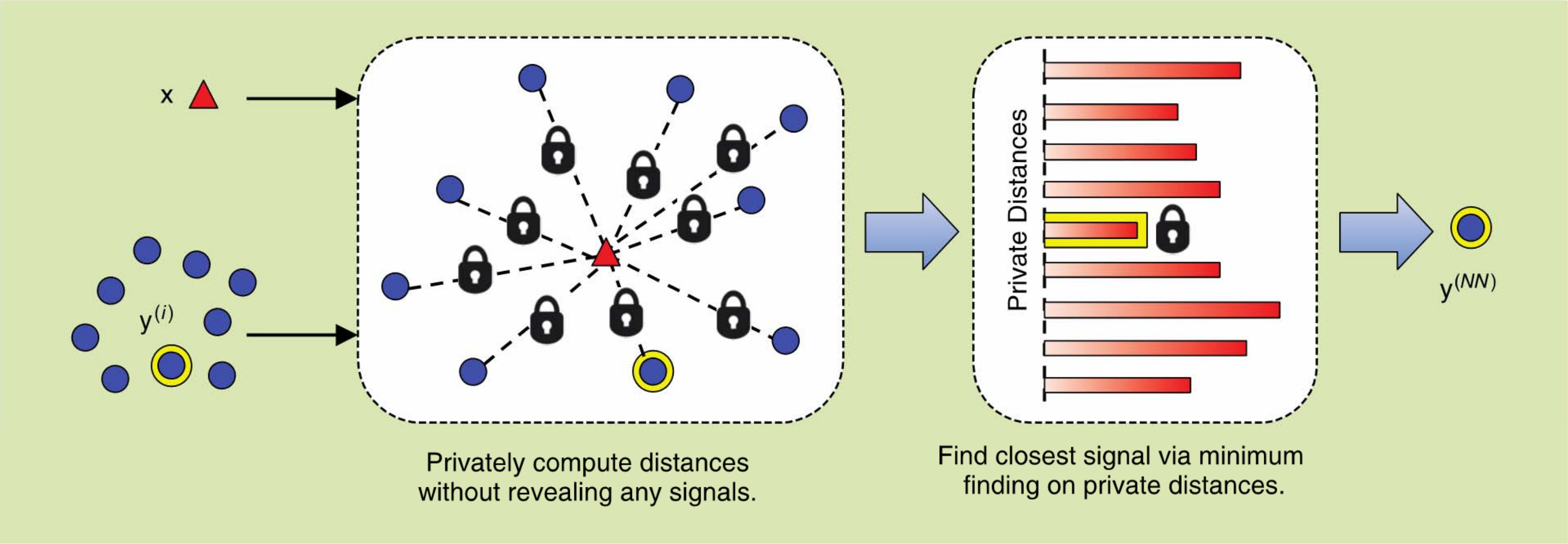
- Efficiency and privacy also become increasingly important considerations for the design of large-scale biometric identification systems
- Binary feature representations can provide fast matching in Hamming space but
  - High-dimensional binary feature representations with large search radius in Hamming space
  - The retrieval of biometric identities must be rank-ordered due to large-intra class variations

Hash-Based Similarity Search



Privacy-Preserving Similarity Search

- Perform NN searches without knowing explicitly the distance values [Rane et al. 2013]
  - Distance computation + Minimum distance finding



Privately compute distances without revealing any signals.

Find closest signal via minimum finding on private distances.

Courtesy: S. Rane and P. Boufounos, “Privacy-preserving nearest neighbor methods: Comparing signals without revealing them,” IEEE Signal Process. Mag., vol. 30, no. 2, pp. 18–28, Mar. 2013.

Template Protection

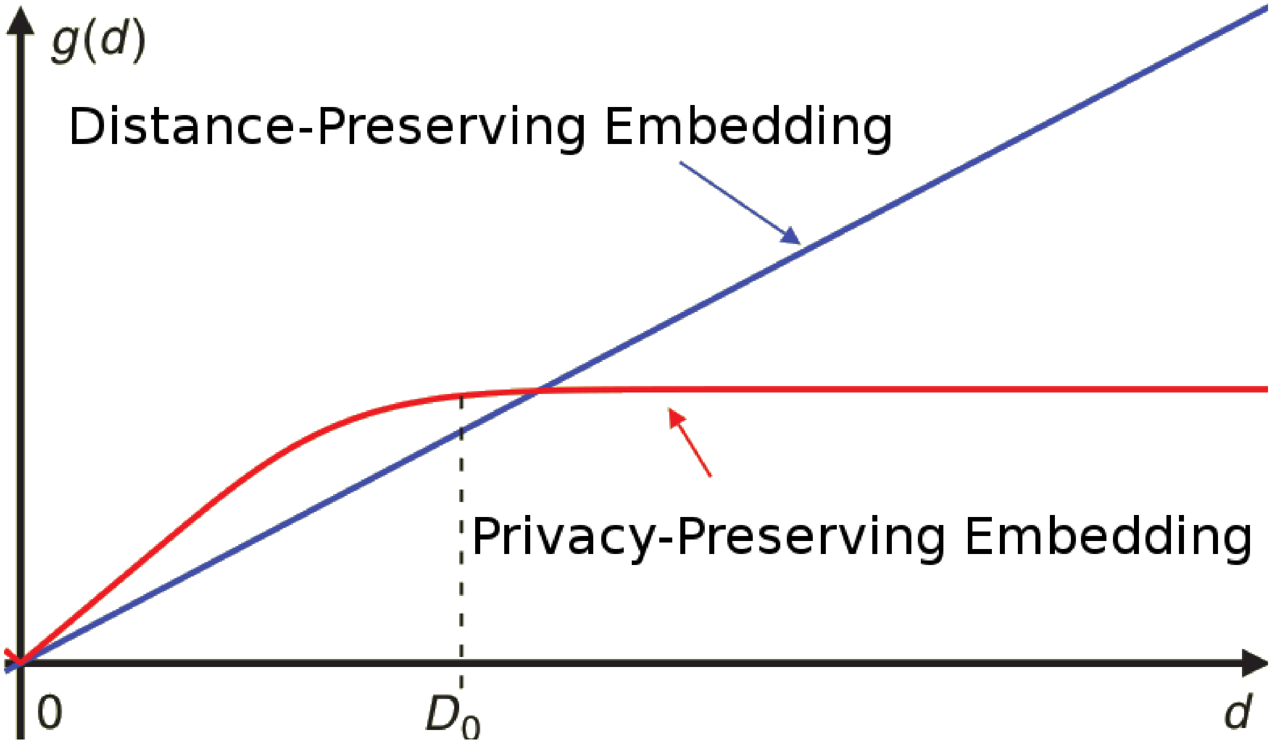
- Mostly designed for *one-to-one* matching without disclosing the feature contents
- Bio-cryptosystems
  - Validity checks (yes/no)
  - Not suitable for similarity comparisons
- Feature transformations
  - Apply non-invertible functions
  - Distance-preserving

Cryptography-Based Approach

- Processing in the encrypted domain without decrypting the data, e.g.,
  - Homomorphic encryption, garbled circuits, multi-party computation protocols, etc.
  - Excessive computation and communication overheads
  - Inherent difficulties in scaling up and meeting the efficiency requirements

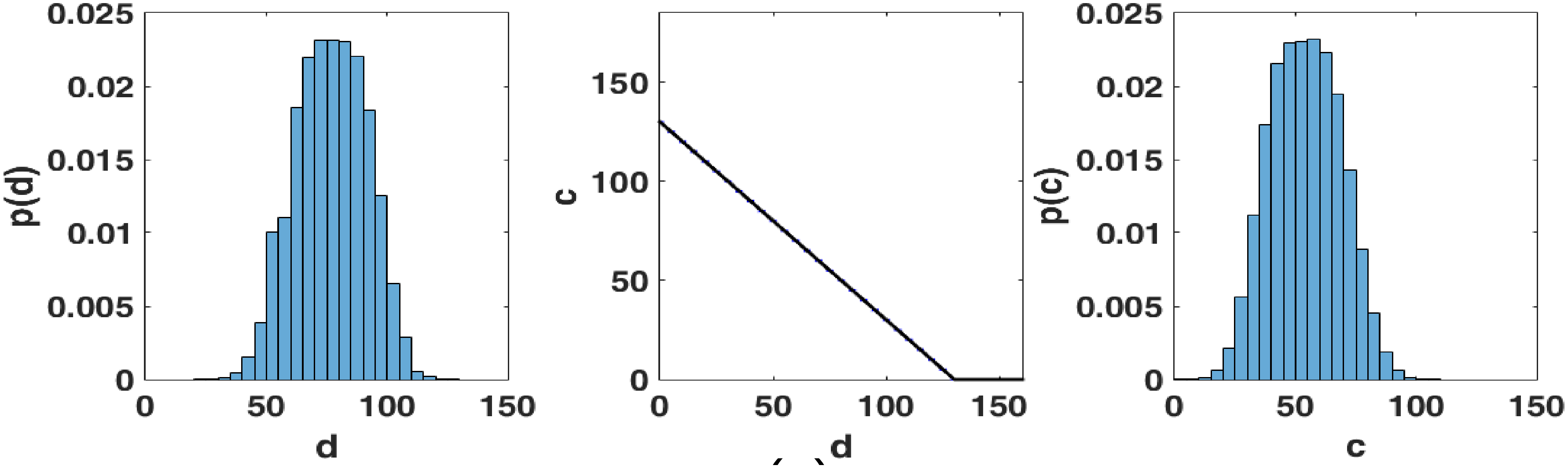
Information-Theoretic Approach

- Secure binary embedding [Rane et al. 2013]



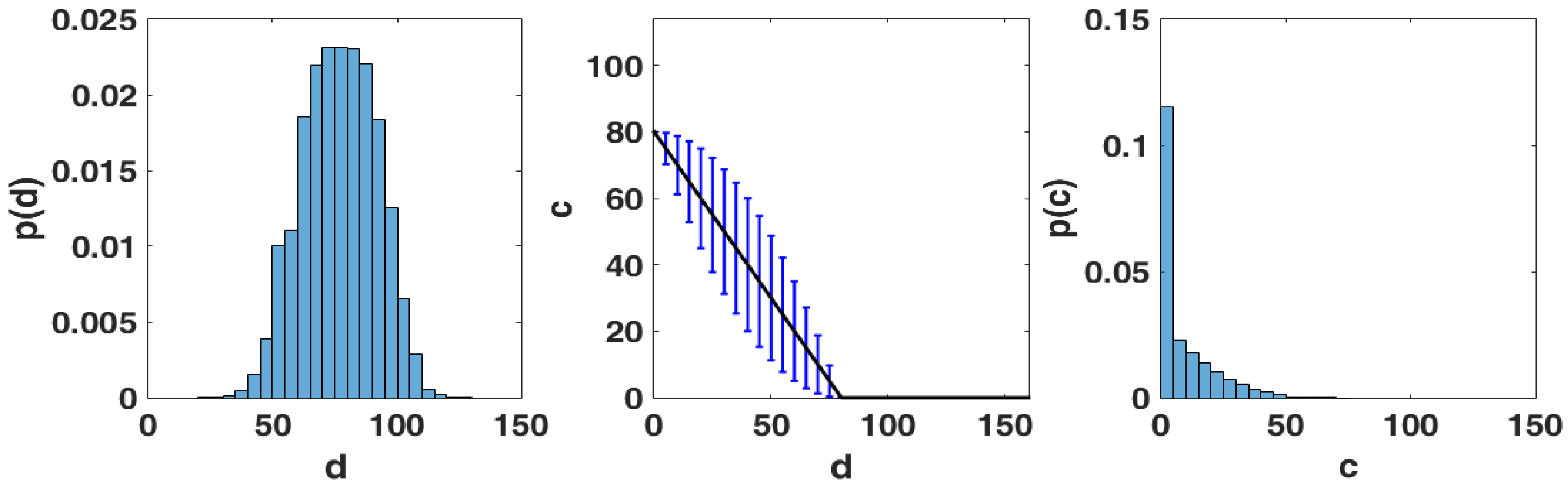
Linear Mapping

- Preserves the similarity information

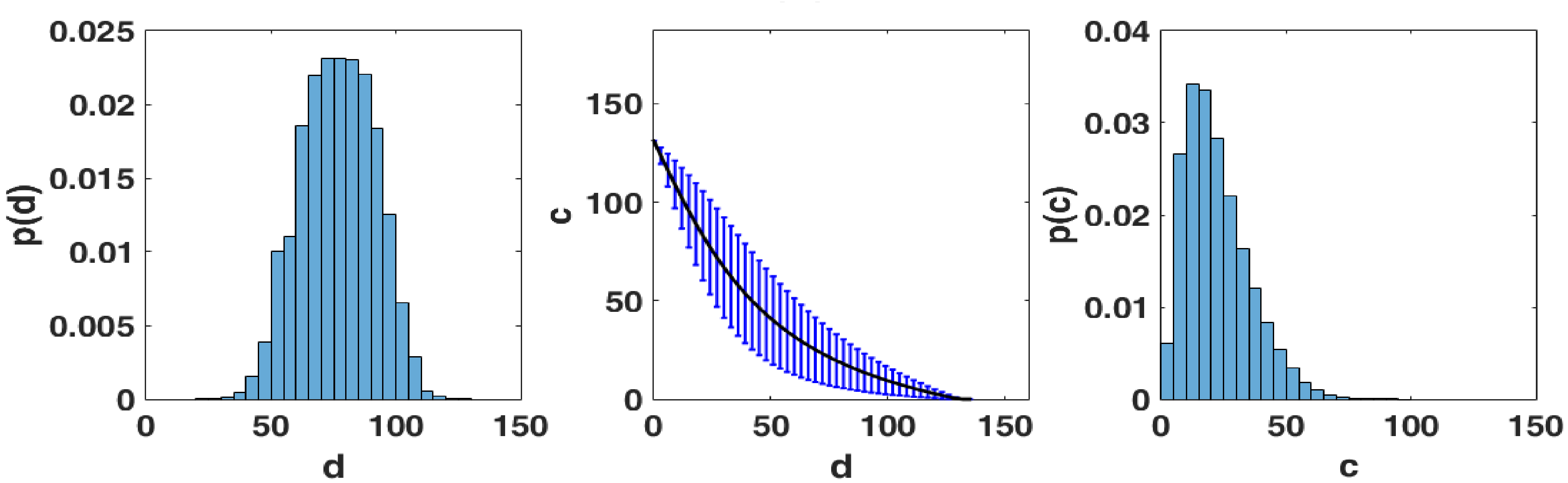


Distance Obfuscation

- Introducing variable intervals (anonymization)
- The projected value c is selected uniformly from a mapping interval at d



Anonymized Non-Linear Mapping



Revisit Hamming-Ball Search

- Consider a query string q and a data set

$$\Omega = \{\mathbf{p}_1, \mathbf{p}_2, ..., \mathbf{p}_N\}$$

Find all $\mathbf{p} \in \Omega$ satisfy

$$H(\mathbf{p}, \mathbf{q}) \leq r$$

which constitute a NN subset of query q with radius r, denoted by $\mathcal{B}_{\mathbf{q}}(\Omega, r)$.

Anonymized Distance Filter

- Explore the Hamming ball volume without explicitly evaluate the distance values
- Randomized similarity test algorithms in Hamming space
- Anonymized distance filter by designing a thresholding function

Y. Wang, J. Wan, Y.-M. Cheung and P. C. Yuen, “Anonymized Distance Filter in Hamming Space ”, *Chinese Conference on Biometric Recognition,* Chengdu, China, Oct. 2016.

Randomized Similarity Test

- Piecewise matching binary sub-hash codes

  Two binary strings p and q of D bits have $H(p, q) \leq r$. Divide p and q into $L > r$ non-overlapping substring segments in the same way. There must be $m \leq r$ unmatched substring pairs between p and q.

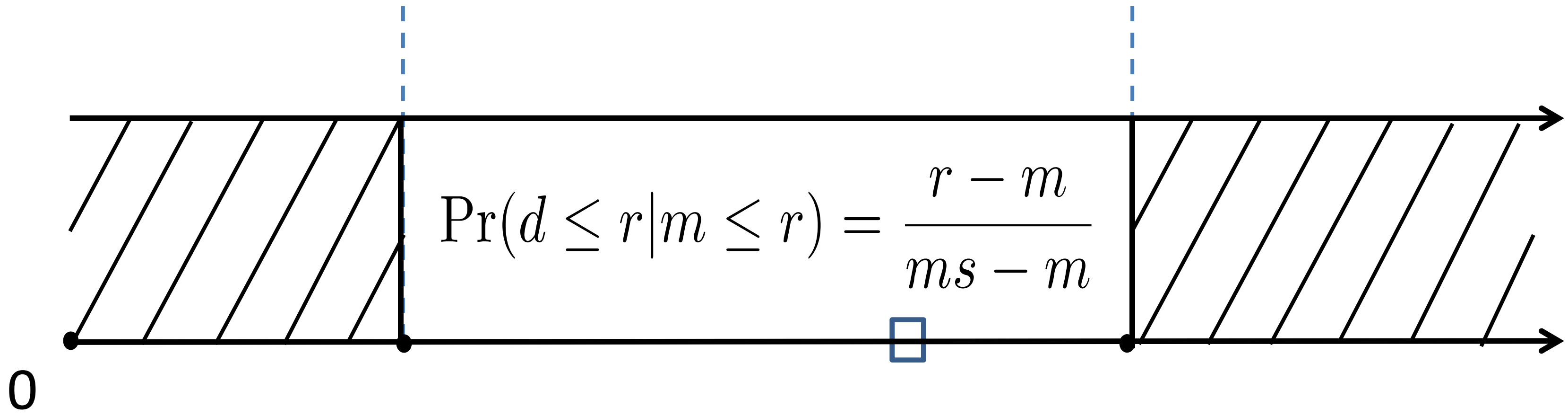
- A randomized protocol for testing if two binary strings are equal

The Drawer Principle

- Suppose $H(\mathbf{p},\mathbf{q}) \leq r$. Divide p and q into $L > r$ non-overlapping substring segments.
- There must be $m \leq r$ unmatched substring pairs between p and q.
- For every $\mathbf{p} \in \mathit{\Omega}$, find the value of m by testing L substring pairs with q
  - If $m > r$, p is not in $\mathcal{B}_{\mathbf{q}}(\mathit{\Omega}, r)$
  - If $m \leq r$, test p on a finer scale

A Variable Thresholding Function

- To avoid iterative substring division over p
- Since $m \leq d \leq ms$



$$\Pr(d \leq r | m \leq r) = \frac{r - m}{ms - m}$$

- Introduce m_ϵ for some $\epsilon \in [0,1]$Then,

$$m < m_\epsilon = \frac{r}{1 + \epsilon(s-1)}$$

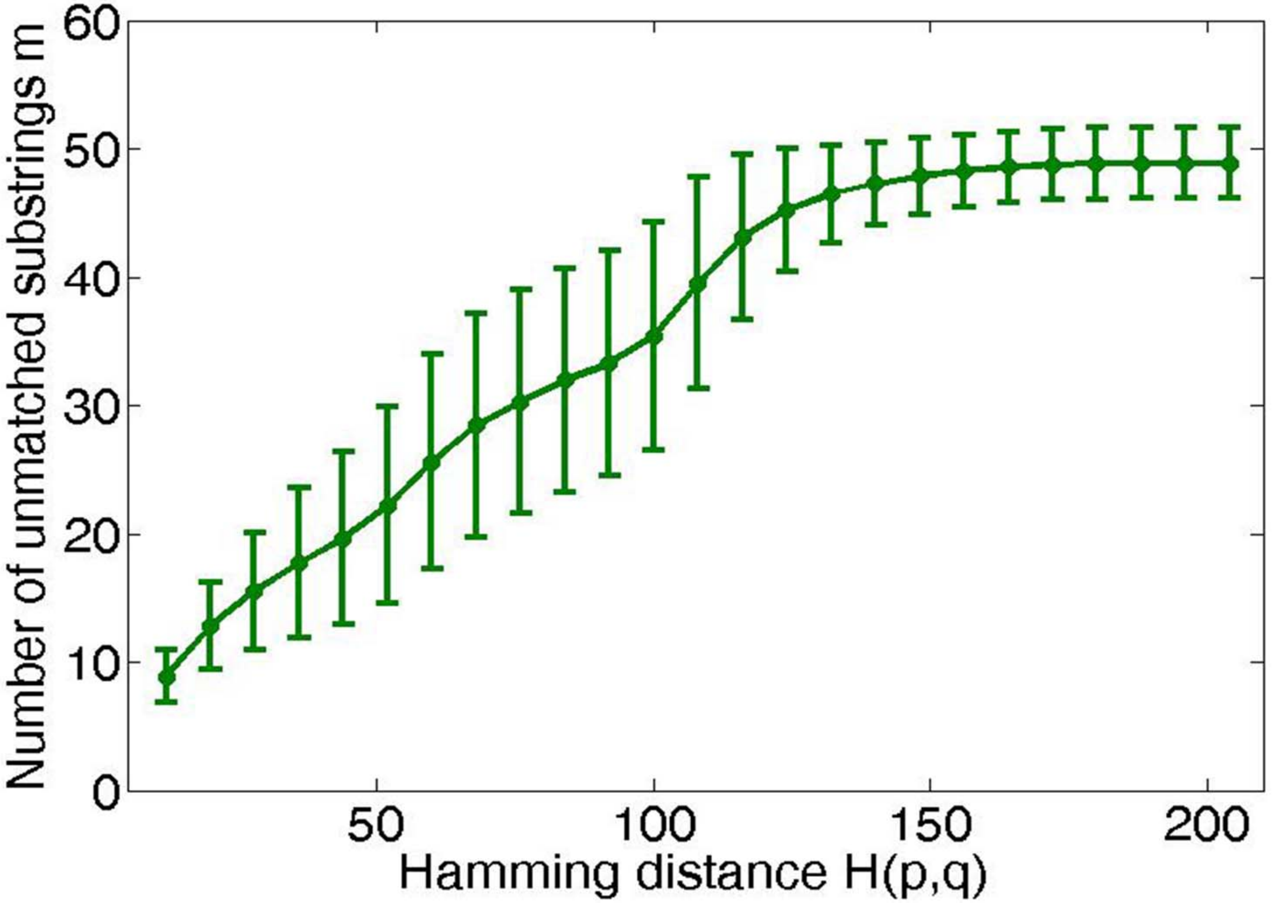
can be used to make decisions by varying ϵ

Anonymized Distance Filter

- Project $d = H(\mathbf{p}, \mathbf{q})$ into an interval $[m, ms]$ defined by m and s
  - Analogous to *anonymization* that attempts to classify data into fixed or variable intervals
- Filtering decision made on m which can be regarded as an obfuscated measure of d

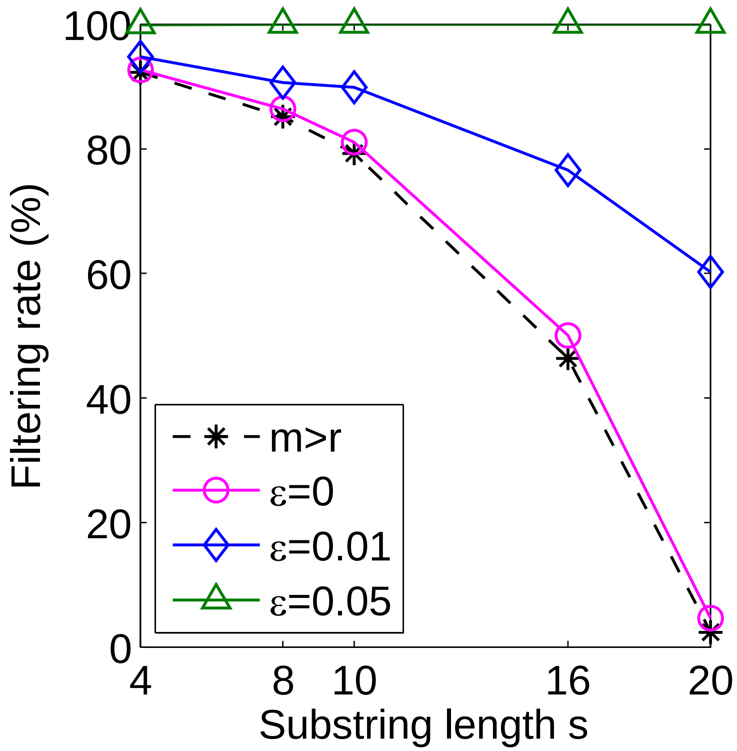
$$\begin{cases} \frac{d}{s} \le m \le d, & \text{if } 0 \le d \le L \\ \frac{d}{s} \le m \le L, & \text{otherwise} \end{cases}$$

Obfuscated Distance Measure

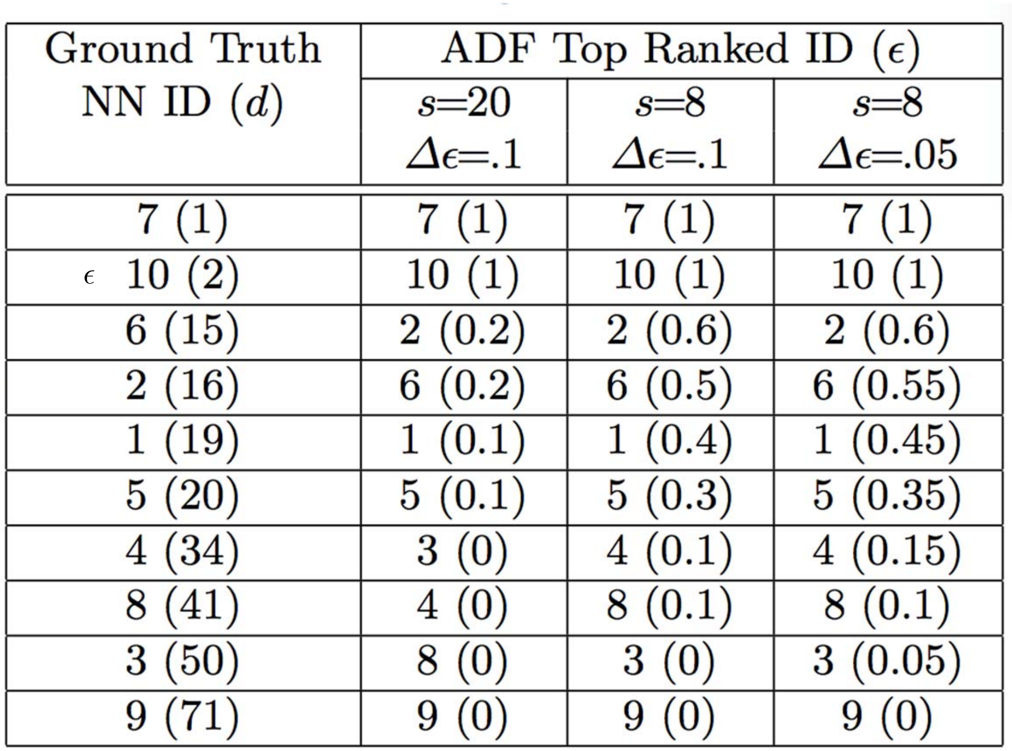


Hamming-Ball Simulation

Filtering rates by varying ϵ

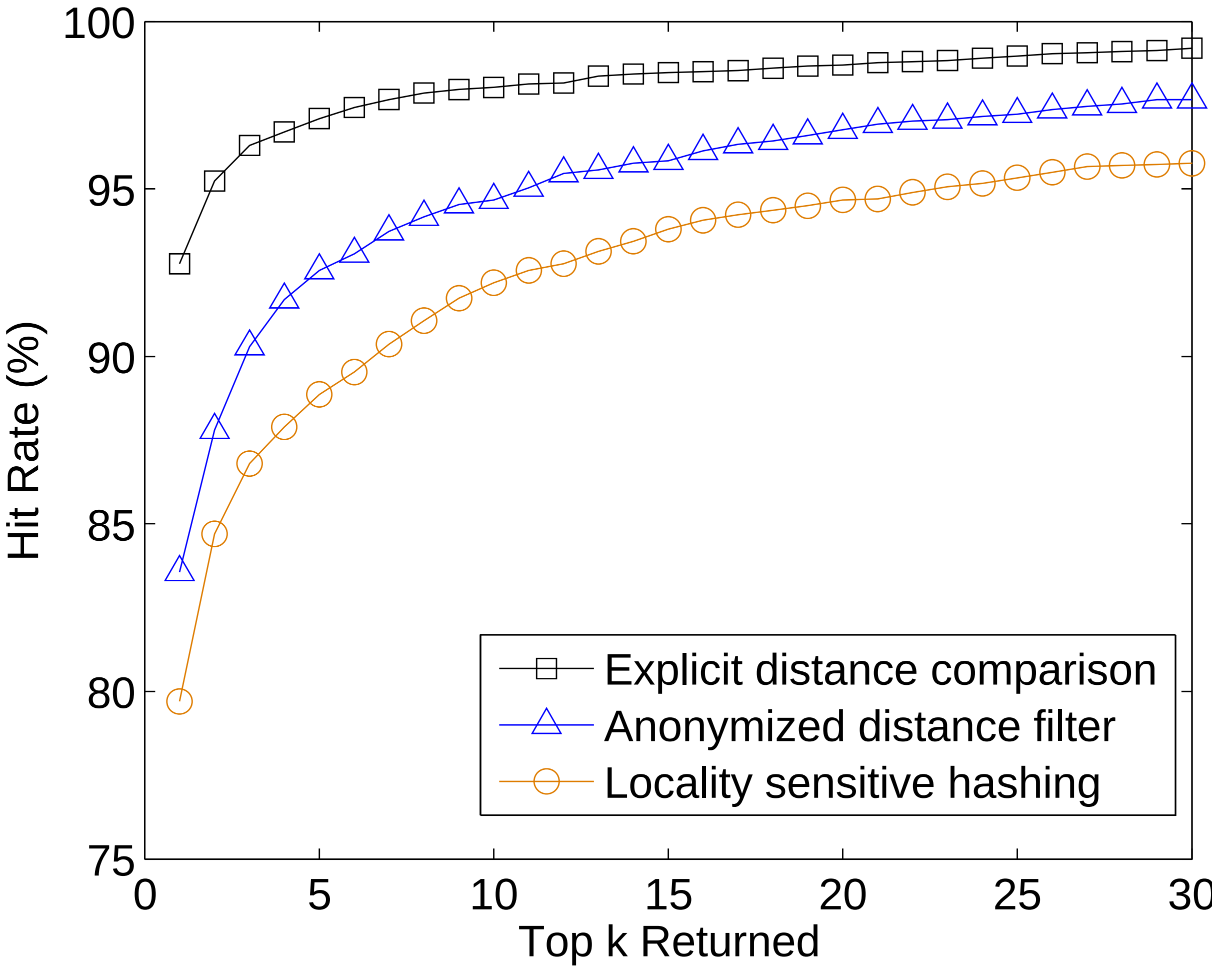


Top 10 ranked ID example



Ground Truth NN ID (d)	ADF Top Ranked ID (ϵ)		
	s=20 $\Delta\epsilon$=.1	s=8 $\Delta\epsilon$=.1	s=8 $\Delta\epsilon$=.05
7 (1)	7 (1)	7 (1)	7 (1)
ϵ 10 (2)	10 (1)	10 (1)	10 (1)
6 (15)	2 (0.2)	2 (0.6)	2 (0.6)
2 (16)	6 (0.2)	6 (0.5)	6 (0.55)
1 (19)	1 (0.1)	1 (0.4)	1 (0.45)
5 (20)	5 (0.1)	5 (0.3)	5 (0.35)
4 (34)	3 (0)	4 (0.1)	4 (0.15)
8 (41)	4 (0)	8 (0.1)	8 (0.1)
3 (50)	8 (0)	3 (0)	3 (0.05)
9 (71)	9 (0)	9 (0)	9 (0)

FERET Face Search Results



References

- [Jain et al. 2016] A. K. Jain, K. Nandakumar, A. Ross. “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern Recognition Letters*, 2016, 79: 80-105.
- [Cappelli et al. 2011] R. Cappelli, M. Ferrara, D. Maltoni, “Fingerprint indexing based on minutia cylinder-code,” *IEEE Trans. Pattern Anal. Mach. Intell.*, 2011, 33(5): 1051–1057.
- [Choi et al. 2012] J. Y. Choi, Y. M. Ro, K. N. Plataniotis. “Color local texture features for color face recognition,” *IEEE Trans. Image Processing*, 2012, 21(3): 1366-1380.
- [Mehrotra et al. 2010] H. Mehrotra, B. Majhi, and P. Gupta, “Robust iris indexing scheme using geometric hashing of SIFT keypoints,” *J. Netw. Comput. Appl.*, 2010, 33(3): 300–313.
- [Lei et al. 2014] Z. Lei, M. Pietikainen, S. Z. Li. “Learning discriminant face descriptor,” *IEEE Trans. Pattern Anal. Mach. Intell.*, 2014, 36(2): 289-302.
- [Lu et al. 2015] J. Lu, V. E. Liong, X. Zhou, J. Zhou. “Learning compact binary face descriptor for face recognition”, *IEEE Trans. Pattern Anal. Mach. Intell.*, 2015, 37(10): 2041-2056.

References

- [Wang et al. 2011] Y. Wang, J. Hu. “Global ridge orientation modeling for partial fingerprint identification,” *IEEE IEEE Trans. Pattern Anal. Mach. Intell.*, 2011, 33(1): 72-87.
- [He et al. 2015] Ran He, Yinghao Cai, Tieniu Tan, Larry Davis, “Learning predictable binary codes for face indexing”, *Pattern Recognition*, 2015, 48(10): 3160-3168.
- [Kan et al. 2016] M. Kan, S. Shan, X. Chen. “Multi-view deep network for cross-view classification,” *IEEE Conf. Computer Vision and Pattern Recognition* (CVPR’16), 2016: 4847-4855.
- [Wang et al. 2016] D. Wang, C. Otto, A. K. Jain. “Face search at scale,” *IEEE Trans. Pattern Anal. Mach. Intell*, to appear.
- [Paliwal et al. 2010] A. Paliwal, U. Jayaraman, P. Gupta. “A score based indexing scheme for palmprint databases,” *Intl. Conf. Image Processing* (ICIP’10), 2010: 2377-2380.
- [Gyaourova et al. 2012] A. Gyaourova, A. Ross. “Index codes for multibiometric pattern retrieval,” *IEEE Trans. Inf. Forensics Security*, 2012, 7(2): 518-529.

References

- [Rathgeb et al. 2015] C. Rathgeb, F. Breitinger, H. Baier, C. Busch. “Towards Bloom filter-based indexing of iris biometric data,” *Intl. Conf. Biometrics* (ICB’15), 2015: 422-429.
- [Proenca 2013] H. Proenca. “Iris biometrics: Indexing and retrieving heavily degraded data,” *IEEE Trans. Inf. Forensics Security*, 2013, 8(12): 1975-1985.
- [Wang et al. 2015] Y. Wang, L. Wang, Y. M. Cheung, P. C. Yuen. “Learning compact binary codes for hash-based fingerprint indexing,” *IEEE Trans. Inf. Forensics Security*, 2015, 10(8): 1603-1616.
- [Yue et al. 2010] F. Yue, B. Li, M. Yu, J. Wang, “Hashing based fast palmprint identification for large-scale databases,” *IEEE Trans. Inf. Forensics Security*, 2013, 8(5): 769–778.
- [Hao et al. 2008] F. Hao, J. Daugman, P. Zielinski, “A fast search algorithm for a large fuzzy database,” *IEEE Trans. Inf. Forensics Security*, 2008, 3(2): 203–212.
- [Biggio et al. 2015] B. Biggio, G. Fumera, P. Russu, L. Didaci, F. Roli, “Adversarial biometric recognition: A review on biometric system security from the adversarial machine-learning perspective,” *IEEE Signal Process. Mag.*, 2015, 32(5): 31—41.
- [Rane et al. 2013] S. Rane, P. Boufounos, “Privacy-preserving nearest neighbor methods: Comparing signals without revealing them,” *IEEE Signal Process. Mag.*, 2013, 30(2): 18–28.