



# Modeling an Anonymous Identification System

**Brian DeCann and Arun Ross**  
**March 8th, 2012**

**Integrated Pattern Recognition and Biometrics (i-PRoBe) Lab**  
**Lane Department of Computer Science and Electrical Engineering**  
**West Virginia University, Morgantown, West Virginia**



# Motivation

Suppose a biometric system encounters some number of individuals\*.



Encountered Individual

- Presume **no prior information** about any of these individuals / identities.
- The actual **identity** of the individual **observed is unknown** to the system (identification).
- The **system** is also **not acquiring** information pertaining to the **identity** of encountered individuals.

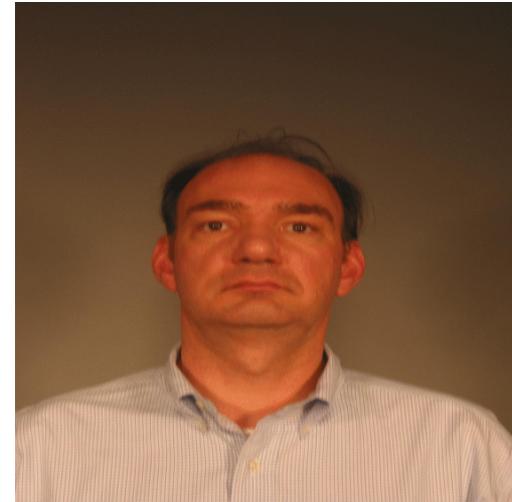


# Motivation

Suppose all we wish to know is **has this person been encountered previously** by the system.



Has this person  
been encountered?



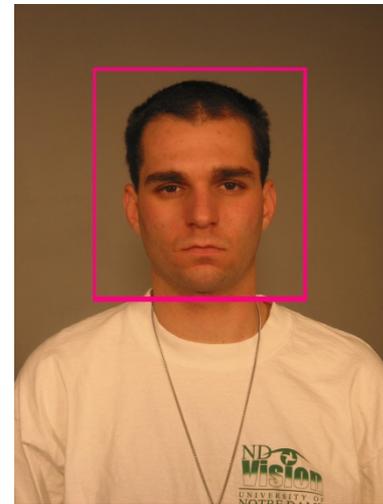
Encountered Individual

# Motivation

Suppose all we wish to know is **has this person been encountered previously** by the system.



Has this person  
been encountered?



Encountered Individual

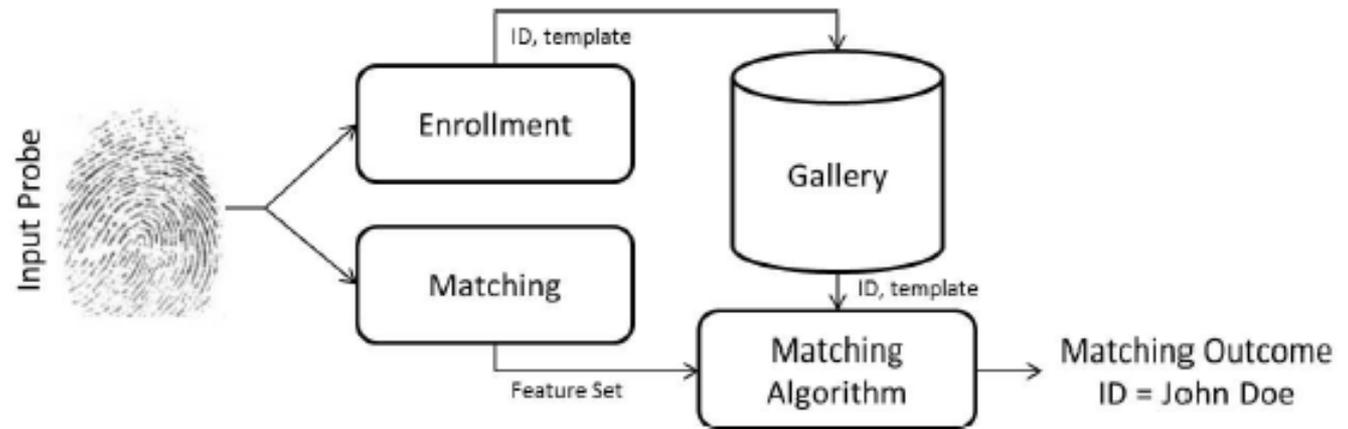
Yes, this person has been previously  
encountered.

# Anonymous Identification

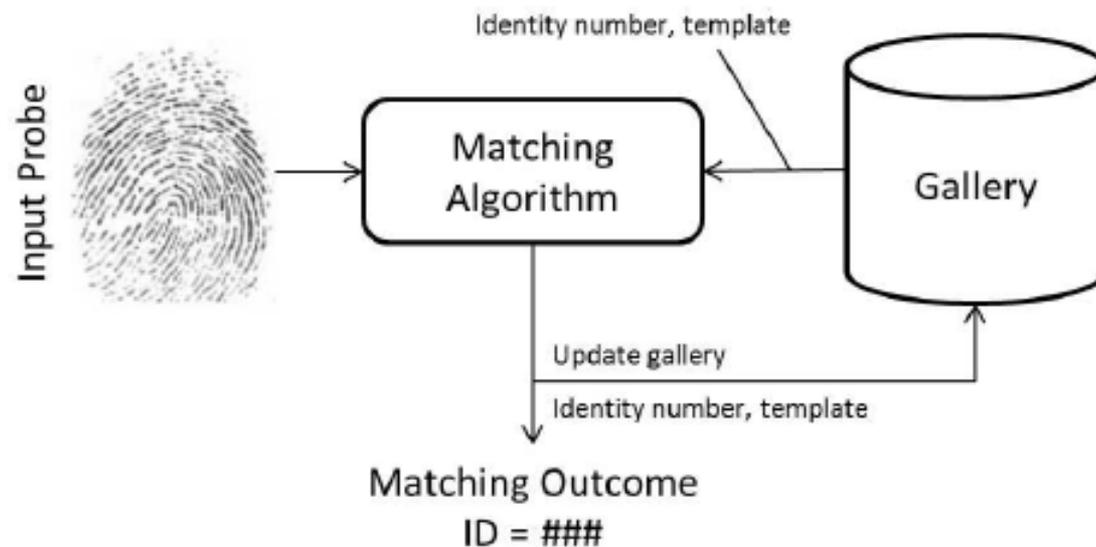
- Anonymous identification system
  - Variant of a classical biometric system.
    - No explicit **enrollment** process.
    - Biometric **templates** in the gallery are **not labeled with the identity** of individuals.
- Comparison process
  - System observes the input (probe) biometric data and **determines if a match exists** in the gallery.
  - Addresses the question: **“Has this person been encountered before?”**

# Visual Comparison

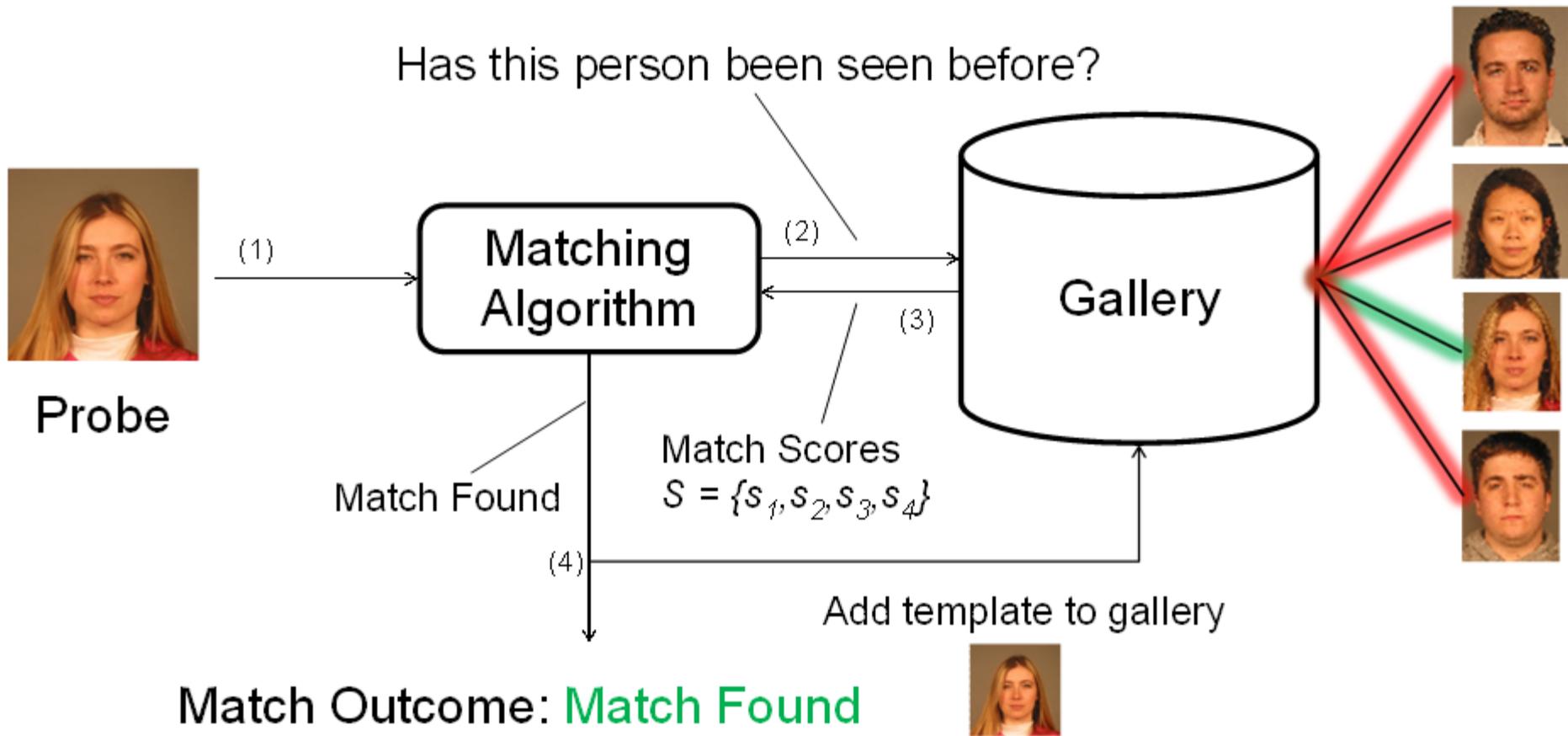
## Traditional Biometric System



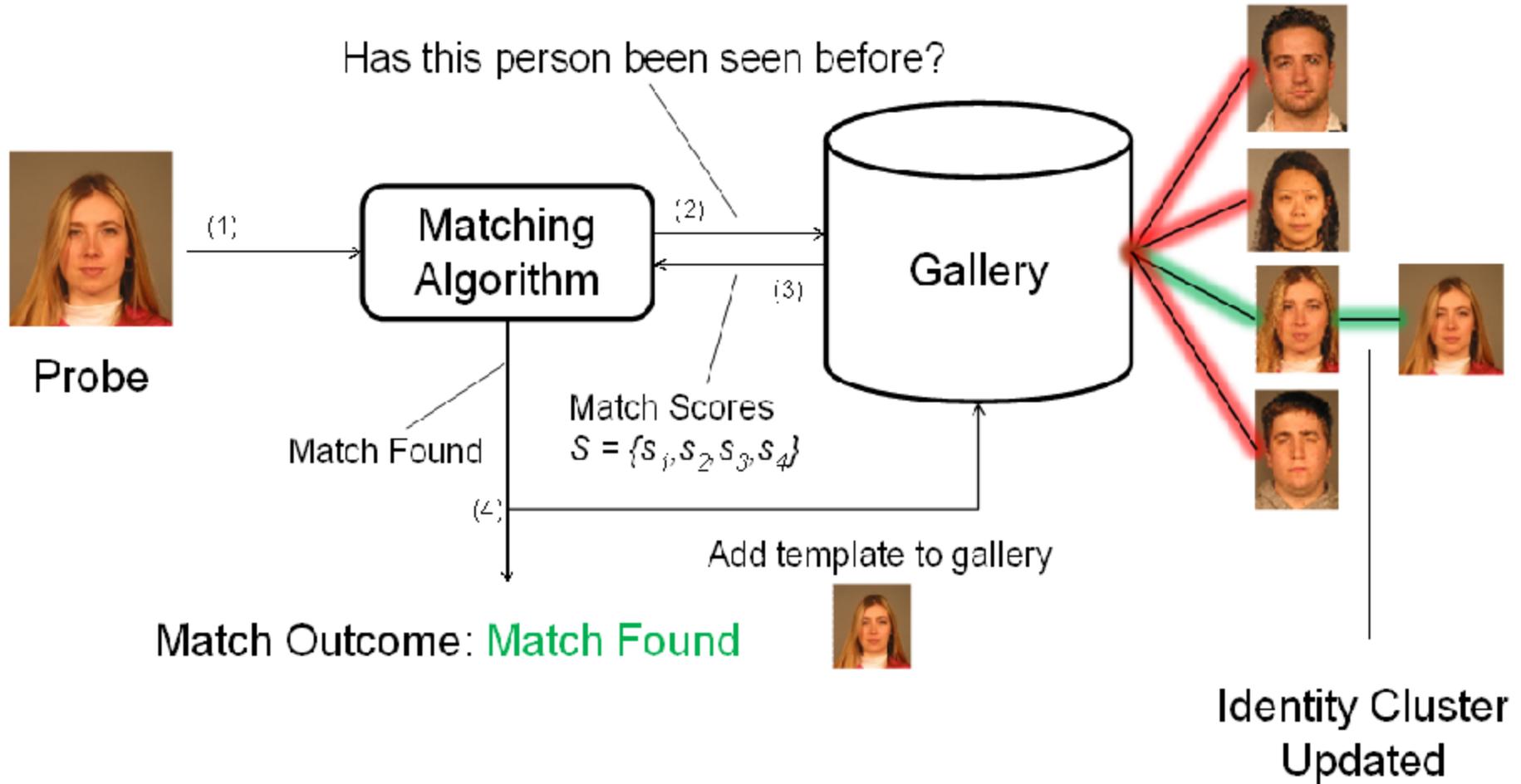
## Anonymous Identification System



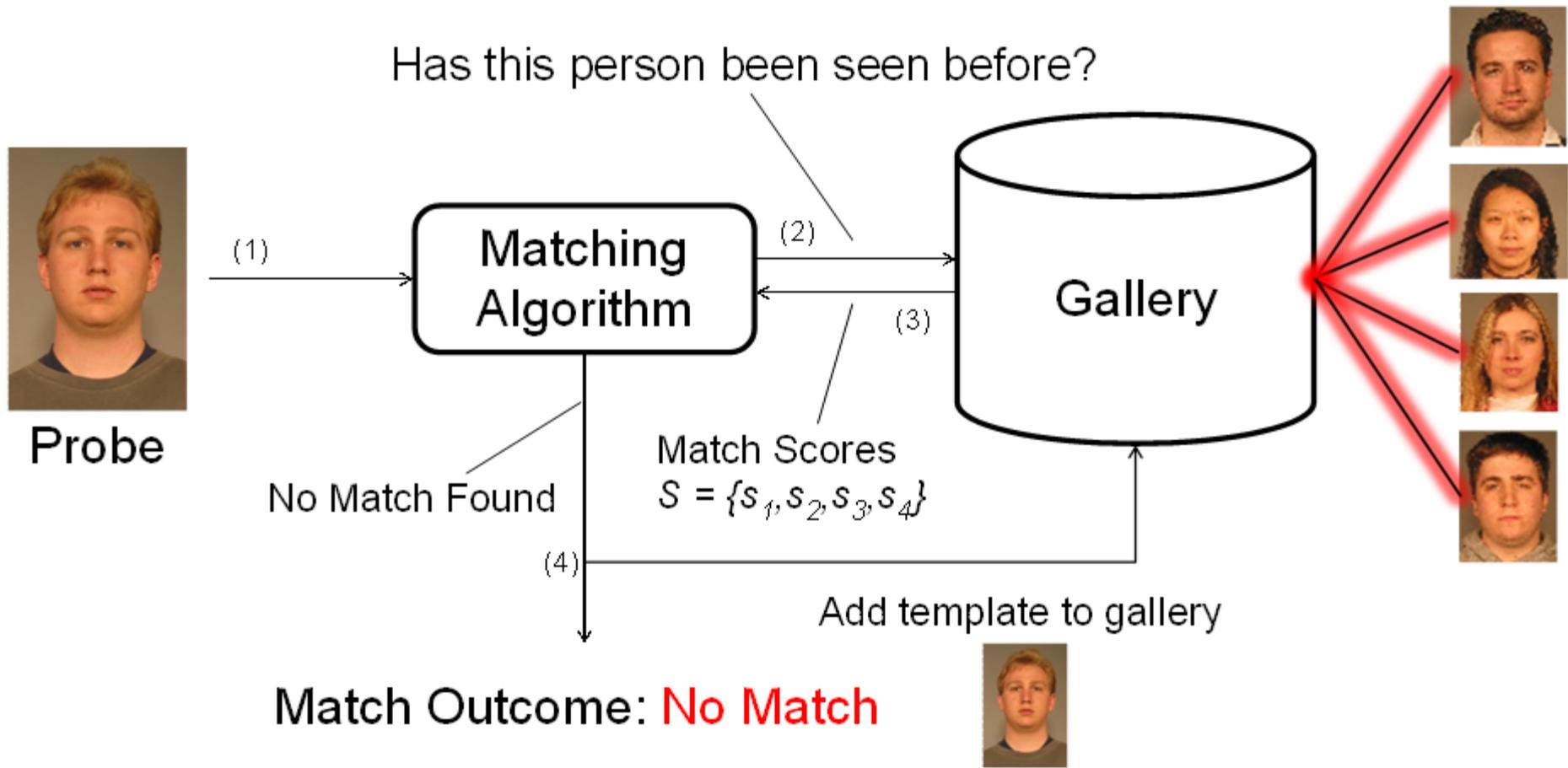
# Visual Example: Match Outcome



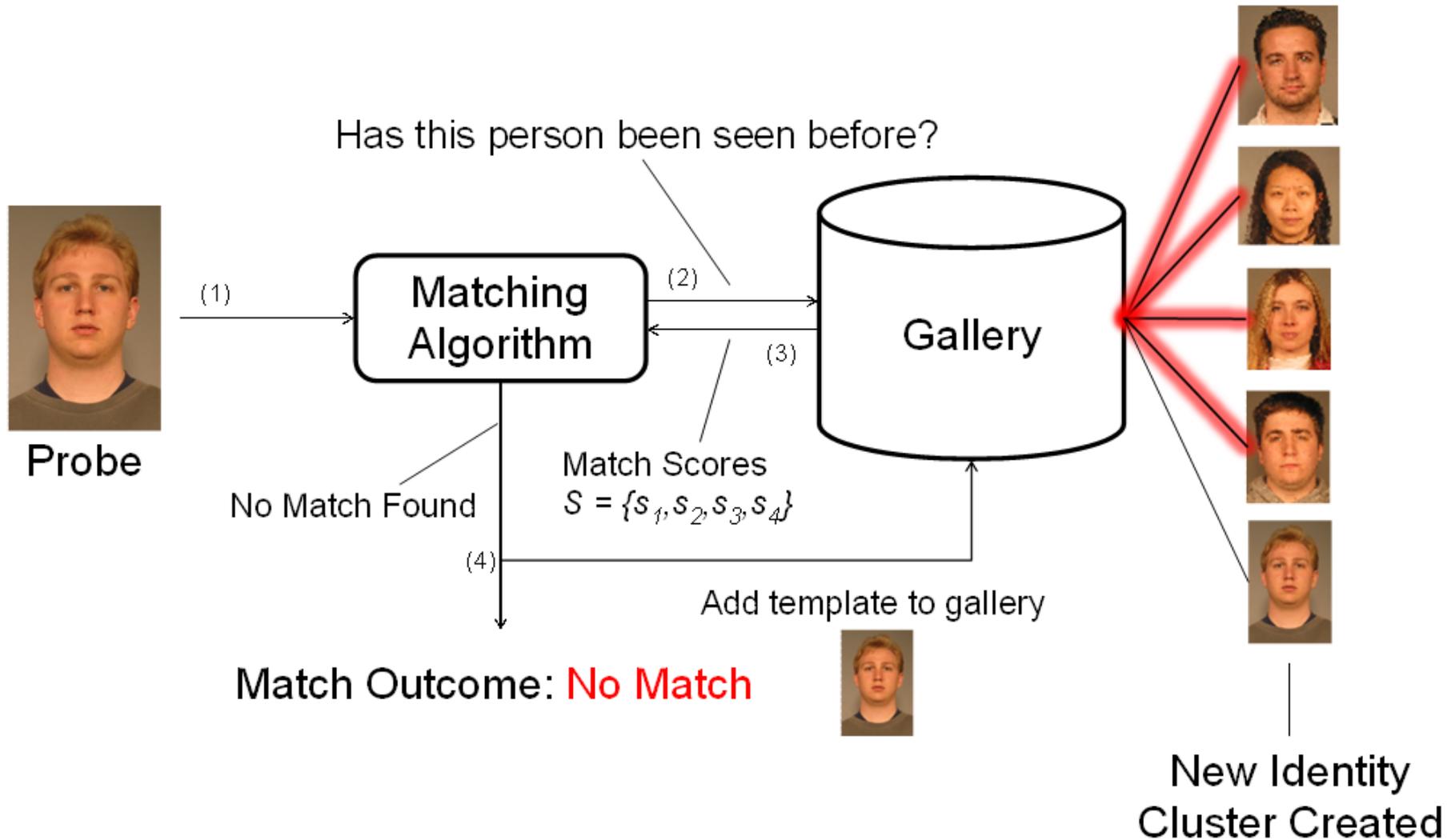
# Visual Example: Match Outcome



# Visual Example: Non-match Outcome



# Visual Example: Non-match Outcome



# Potential Applications

- De-duplication
  - The de-duplication problem invokes searching through a database to *solely* determine **if the probe matches** to an entry in the gallery.
    - i.e., not concerned with the identity of the match.
  - De-duplication contrasts to classical identification, since **gallery entries may not be accurately labeled**.
  - Problem gaining traction in the context of national scale ID programs\*.
- Surveillance
  - Allows for **real-time updating of a gallery**.
    - Identity profiles can be newly created or updated following each encounter.
  - **Covert operation**.
    - Subjects do not need to be enrolled in order to be later recognized.

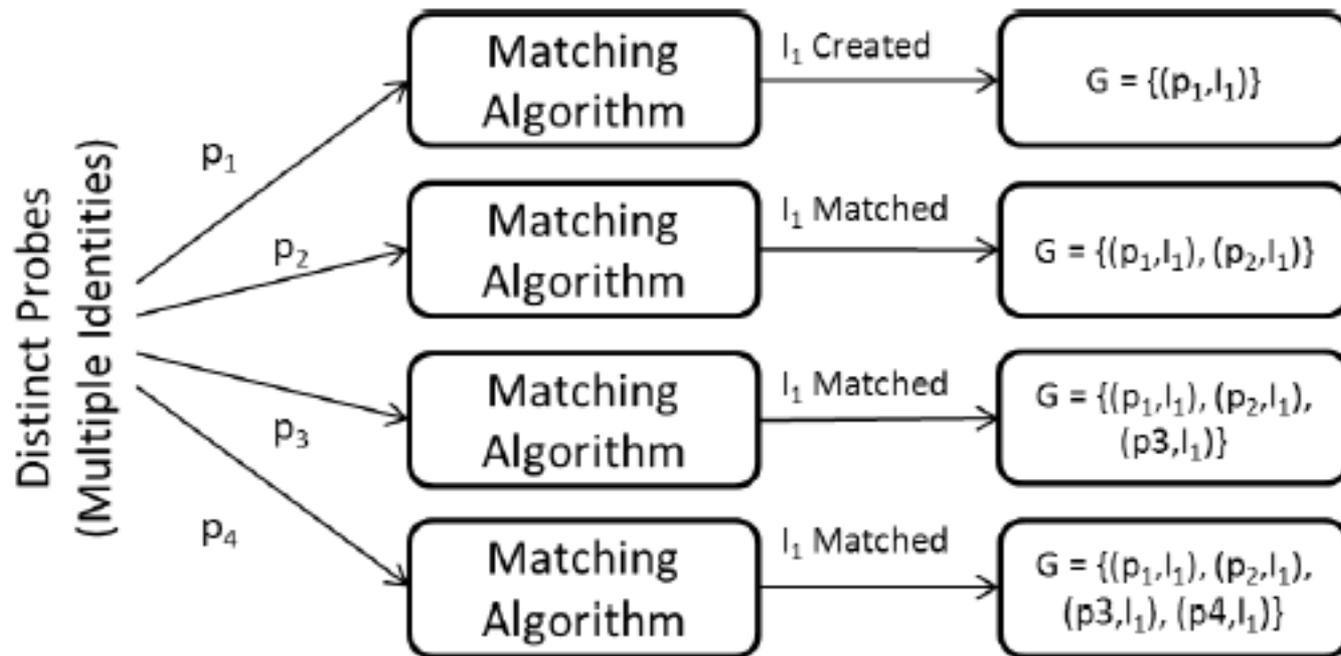
# Error Analysis

- Traditional system
  - Error is computed using a **fixed** set of gallery and probe images.
- Anonymous system
  - Since the gallery expands, the error rate **changes** depending on the current gallery and future probes.
- How?
  - In a traditional analysis, probe  $p_k$  is absolutely associated with a specific set of gallery entries.
  - In an anonymous identification system, the actual identity pertaining to probe  $p_k$  may or may not have been previously encountered.
  - Further, if the proper identity has been encountered, it may exist in **multiple identity clusters** due to decision error.

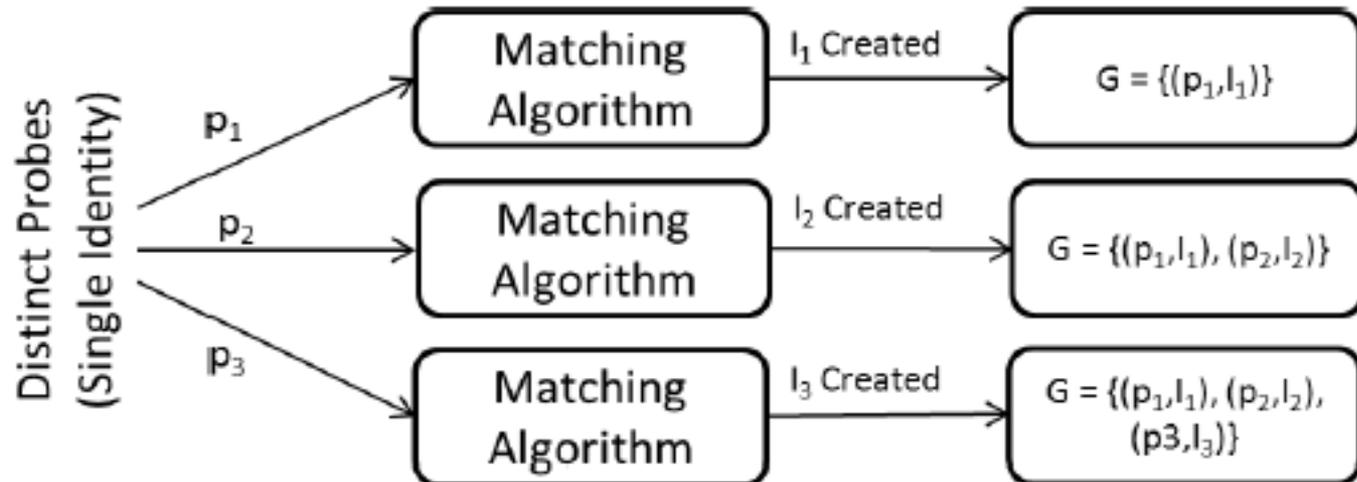
# Types of Errors

- False Dynamic Match (FDM)
  - Occurs when **a probe incorrectly matches to an identity cluster** that does not contain an entry belonging to the encountered individual.
- False Dynamic Non-Match (FDNM):
  - Occurs when **a probe, which should match** to at least one existing identity cluster, **does not match to any identity cluster**.
    - Thus, if the individual has not been seen by the system, a false dynamic non-match cannot occur.
    - A false dynamic non-match does not occur when a probe correctly matches to an identity cluster consisting of the true identity, in addition to other identities.

# False Dynamic Match: Visualization



# False Dynamic Non-Match: Visualization



# Error Prediction

- Analytical Error Prediction
  - Derive an **analytical** approach for **estimation** of **FDMR** (False dynamic match rate) and **FDNMR** (False dynamic non-match rate) given a set of test data.
- Constraints
  - Assume all probes have an equal probability of being observed.

# Error Prediction – False Dynamic Match

- False Dynamic Match

- Occurs when a probe is incorrectly matched to an identity cluster whose entries do not contain the true identity of the probe.

- Events

- **Event A:** When  $p_k$  is matched against  $G$  at encounter  $e_k$ , there are **no genuine scores generated** and at least **one impostor score** is **greater** than  $\gamma$ .
  - $\gamma$  = decision threshold
- **Event B:** When  $p_k$  is matched against  $G$  at encounter  $e_k$ , both genuine and impostor scores are generated, and there is at least **one impostor score** that **(a) exceeds  $\gamma$**  and **(b) is greater than all genuine scores**.

# FDM - Mathematical Representation

- Mathematical Representation

- $P(FDM|p_k, e_k) = P(A|p_k, e_k) \cup P(B|p_k, e_k)$

- $P(A|p_k, e_k) = \sum_{z=1}^{N_I^\gamma} \frac{\binom{N_I^\gamma}{z} \binom{K-N_I^\gamma}{k-z-1}}{\binom{K}{k-1}} * \frac{\binom{N_G}{0} \binom{K-N_G}{k-1}}{\binom{K}{k-1}}$

- $P(B|p_k, e_k) = \sum_{\forall C} \sum_{z=1}^{\zeta} \frac{\binom{\zeta}{z} \binom{K-\zeta}{k-z-1}}{\binom{K}{k-1}} * \frac{\binom{K-N_G}{k-C_\ell-1}}{\binom{K}{k-1}}$

- Auxiliary Variables

- $N_G$  = Number of genuine probes in G

- $N_I^\gamma$  = Number of potential\* imposter scores above  $\gamma$ .

- $C$  = Set of genuine probe combinations (e.g. {1,2,4}, {3,4}, {2},...)

- $\zeta$  = Number of potential\* imposter scores above the maximum

# Error Prediction – False Dynamic Non-match

- False Dynamic Non-match

- A probe does not match to a genuine gallery entry and any impostor probes that could procure a match have not been observed.

- Events

- **Event C:** When  $p_k$  is matched against  $G$  at encounter  $e_k$ , **all genuine scores generated are below  $\gamma$ .**
- **Event D:** When  $p_k$  is matched against  $G$  at encounter  $e_k$ , **all impostor scores generated are below  $\gamma$ .**

# FDNM - Mathematical Representation

- Mathematical Representation

- $P(FDNM|p_k, e_k) = P(C|p_k, e_k) \cap P(D|p_k, e_k)$

- $P(C|p_k, e_k) = \sum_{z=1}^{\rho} \frac{\binom{\rho}{z} \binom{\omega}{0} \binom{K-N_G}{k-z-1}}{\binom{K}{k-1}}$

- $P(D|p_k, e_k) = \frac{\binom{N_I^\gamma}{0} \binom{K-N_I^\gamma}{k-1}}{\binom{K}{k-1}}$

- Auxiliary Variables

- $N_G$  = Number of genuine probes in G

- $N_I^\gamma$  = Number of potential\* imposter scores above  $\gamma$ .

- $\rho$  = Number of potential\* genuine scores below  $\gamma$ .

- $\omega$  = Number of potential\* genuine scores above  $\gamma$ .

\*Inclusive to entities outside the gallery.

# Expected Error Rates

- Expected Error Rates

- $E(FDMR) = \frac{100}{K} \sum e_k \sum p_k P(FDM | p_k, e_k)$

- $E(FDNMR) = \frac{100}{K} \sum e_k \sum p_k P(FDNM | p_k, e_k)$

\*Expected FDMR and FDNMR over K encounters

# Experiments

## • Datasets

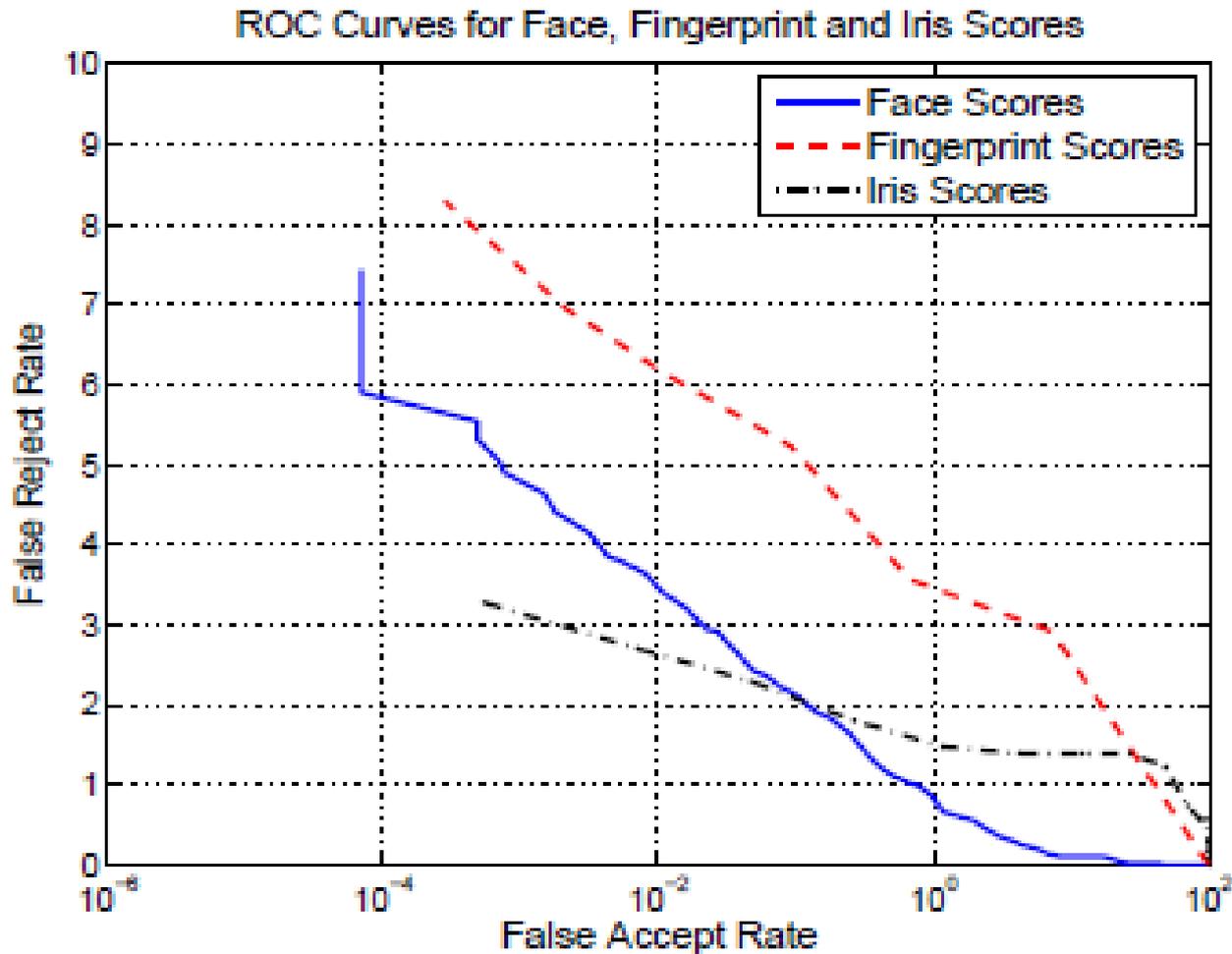
- WVU face dataset
  - 5 frontal face images for 240 subjects.
  - Similarity scores computed from VeriFace.
- WVU fingerprint dataset
  - 5 fingerprint images corresponding to the R1, R2, L1 and L2 fingers for 240 subjects.
  - Similarity scores computed from VeriFinger.
- CASIA Iris Version 3 dataset
  - Subset using 5 left iris images for 122 subjects.
  - Similarity scores computed using an open source IrisCode algorithm.

# Experiments

## • Datasets

- WVU face dataset
    - 5 frontal face images for 240 subjects.
    - Similarity scores computed from VeriFace.
  - WVU fingerprint dataset
    - 5 fingerprint images corresponding to the R1, R2, L1 and L2 fingers for 240 subjects.
    - Similarity scores computed from VeriFinger.
  - CASIA Iris Version 3 dataset
    - Subset using 5 left iris images for 122 subjects.
    - Similarity scores computed using an open source IrisCode algorithm.
- Note:** We are interested in the *meaning* of the numbers, rather than the value(s).

# DET Curves for Match Score Sets



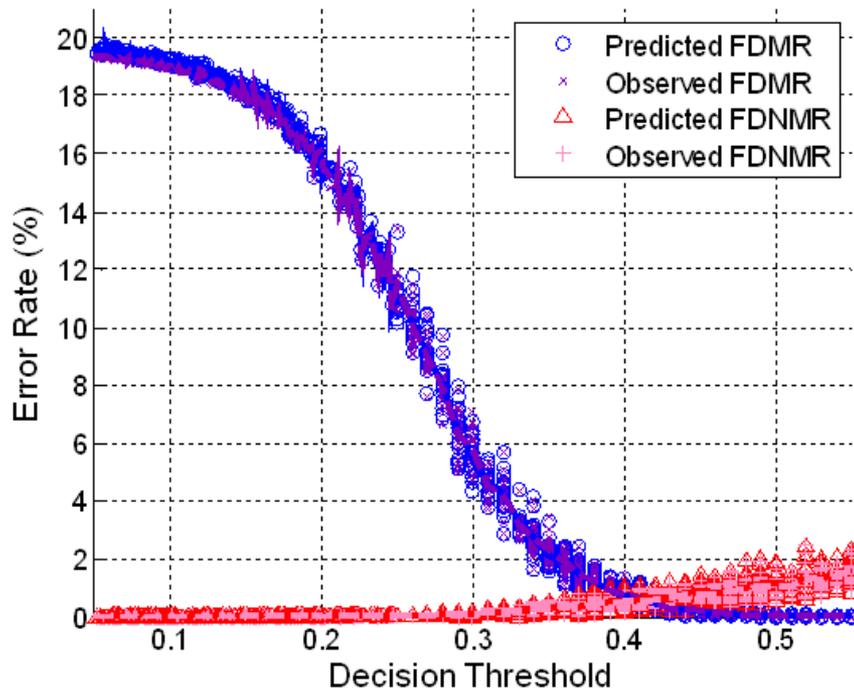
DET curves for face, fingerprint, and iris scores.

# Evaluating the Prediction Model

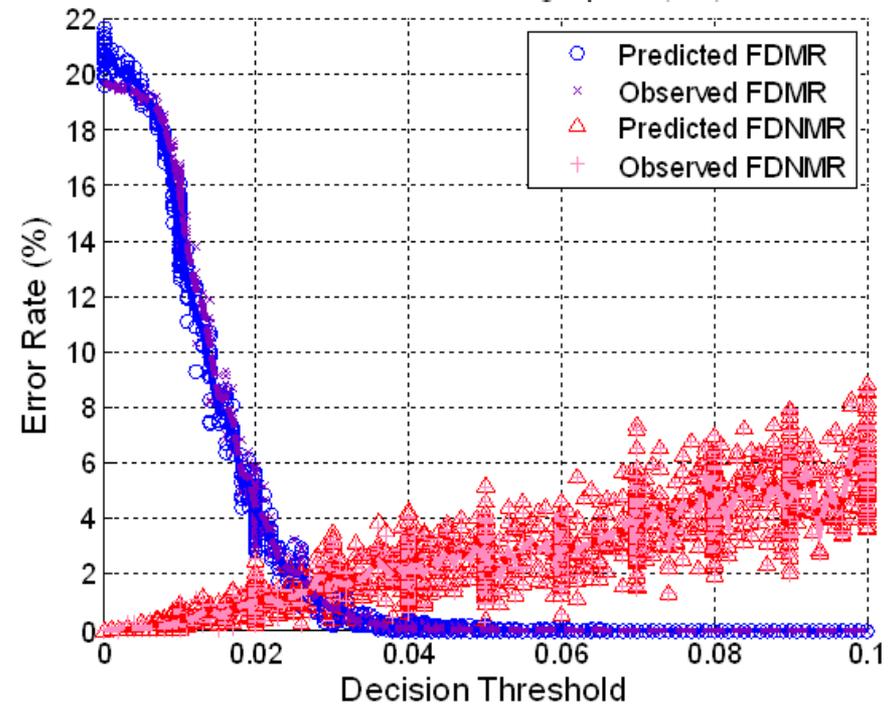
- Model Prediction
  - Evaluate the ability of the model to accurately predict error rates given a set of test scores.
- Experimental setup
  - Create a bootstrapped test set of 300 probes
    - Each bootstrapped test set contains 5 genuine probes for 60 identities.
    - **Allows for variation** in the test data for evaluating the model performance.
    - Aids in **mitigating numerical errors** from computing very large combinatorics.
  - Compare theoretical and observed FDMR and FDNMR.

# Evaluating the Prediction Model

## Face Scores

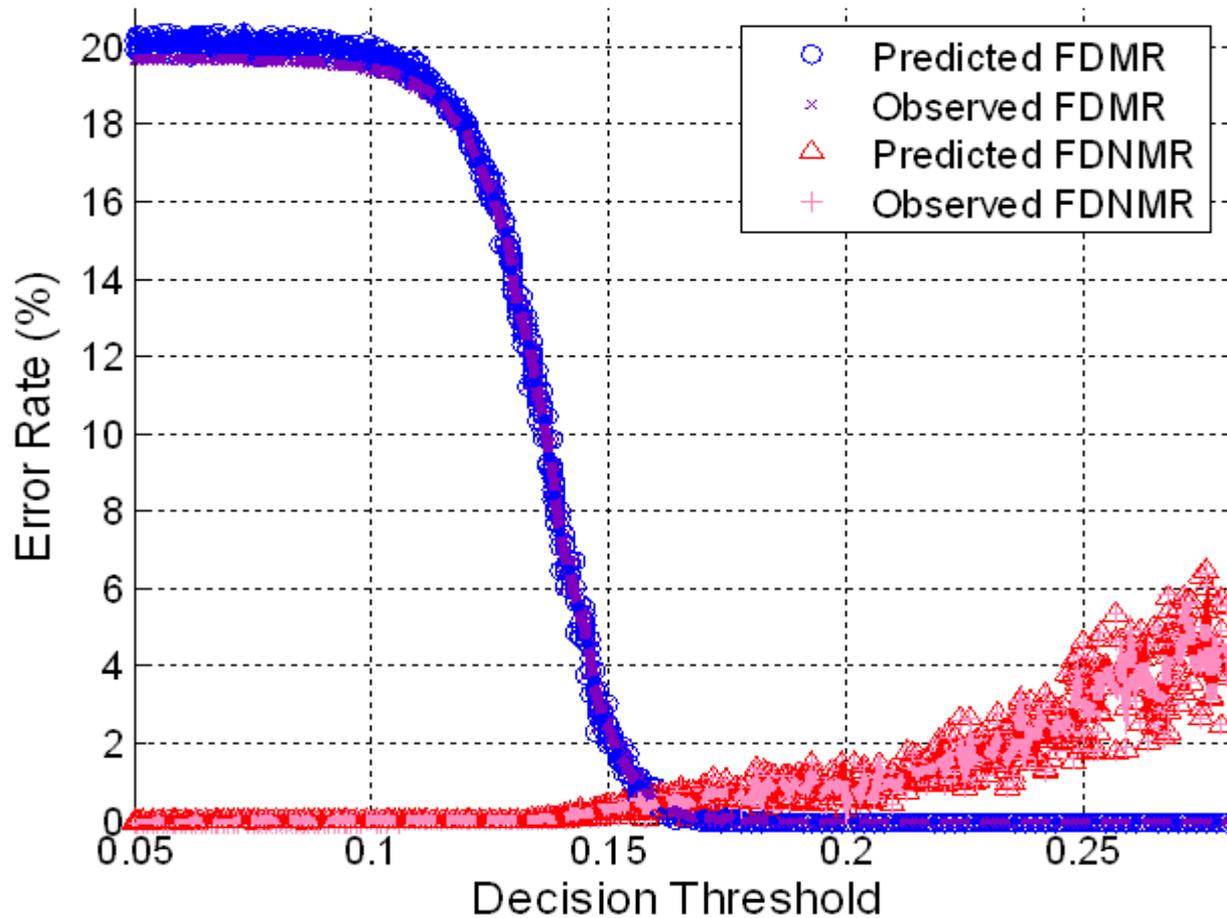


## Fingerprint (R1) Scores



# Evaluating the Prediction Model

## Iris Scores



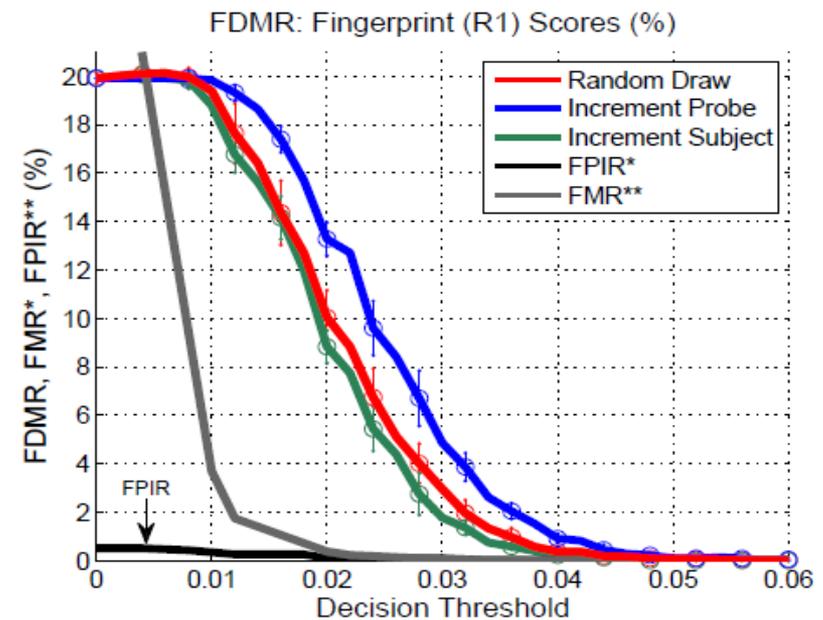
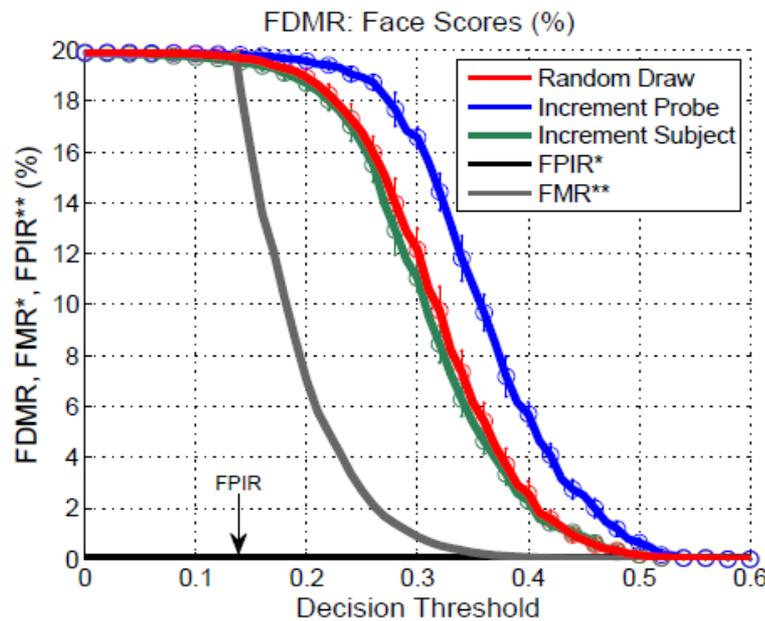
# Summary

- Anonymous Identification
  - Discussed the concept of an *anonymous identification* system.
  - This approach does not ask for unique identity information and **only determines if a person has been encountered before.**
- Error Dynamics
  - Defined the types of error in an anonymous identification system.
- Error Prediction
  - **Developed a prediction model** for estimating the expected error, provided a test set of match scores.
  - The prediction model accurately predicted observed error rates within  $\pm 1.5\%$  for three modalities.

# Summary

## • Other Accomplishments

- Demonstrated the order in which probes are encountered affects the observed error rates.
- Traditional metrics for evaluating biometric system performance fail to accurately quantify the dynamics of an anonymous identification system.





Thank You!

Acknowledgments  
Office of Naval Research  
WVU Night Biometrics Team

# Literature Review

- Anonymous Identification in Literature
  - Dodis *et al.* first defined an anonymous identification system where users enroll in ad-hoc **groups** and prove **membership** [1].
  - Bringer *et al.* adopted the term anonymous identification in the context of **cancelable biometrics** [2].
  - Phrase has come to refer to **template protection** or quality assurances for **privacy**.
- Present Form
  - Here, this definition is **not concerned** with **template protection**.
  - Loosely resembles the work of Dodis *et al.* [1], as the **matching** process **does not** necessarily **deduce identity**.

[1] Y. Dodis, A. Kiayias, A. Nicolosi, V. Shoup, "Anonymous Identification in ad-hoc groups," *Advances in Cryptology – Eurocrypt* (2002)

[2] J. Bringer, H. Chabanne, B. Kindarji, "Anonymous identification with cancelable biometrics," *International Symposium on Image and Signal Processing and Analysis* (2009).

# Experiments

- Performance as a function of permutation
  - Demonstrate that the **order** in which probes are encountered **affects the observed error**.
- Experimental setup
  - Define three types of permutations
    - Random Draw
      - Draw K probes at random without replacement.
    - Increment Probes (IP)
      - Probes corresponding to a single unique identity repeat every M encounters. (M = Number of distinct identities in test set)
    - Increment Subjects (IS)
      - Probes corresponding to a single unique identity repeat successively.
  - Record observed error rates of each permutation type at many values of  $\gamma$ .
    - Also note the FMR, FNMR, FPIR, and FNIR of each score set for all values of  $\gamma$ . ( $\gamma$  = decision threshold).

# Algorithmic Representation

---

## Algorithm 1: Anonymous Identification

---

*Input:* Biometric probes  $p_1, p_2, \dots, p_K$

*Output:* Gallery  $G$  comprised of  $K$  probes with assigned anonymous identity numbers  $I = \{I_1, I_2, \dots, I_K\}$ .

*Define:*  $S(p_k, p_j)$  as similarity score between  $p_k$  and  $p_j$ .

*Initialize:*

$I_1 = 1$  \ \ the first probe is automatically assigned cluster number 1.

Gallery entries  $G = \{p_1, I_1\}$  \ \ the first probe is now placed in the gallery.

$I_2 = I_3 = \dots = I_K = -1$  \ \ the rest of the probes are yet to be observed.

//Begin algorithm

**for**  $k = 2$  **to**  $K$  **do** \ \ iterate through the rest of the probes.

**for**  $j = 1$  **to**  $k - 1$  **do** \ \ upon encountering probe  $p_k$ , compare it with the previous set of encountered probes that are in the gallery database.

$R(j) = S(p_k, p_j)$  \ \ compute similarity between  $p_k$  and  $p_j$ .

**end for**

**if**  $\max_j \{R(j)\}_{j=1}^{k-1} \geq \gamma$  **then**

$I_k = I_m$  where  $m = \arg \max_j \{R(j)\}_{j=1}^{k-1}$  \ \ there is a match with the  $m^{\text{th}}$  gallery entry.

**else**

$I_k = \max(I) + 1$  \ \ if there is not a match, assign  $p_k$  an anonymous identity number one higher than the maximum value in  $I$ .

**end if**

$G = G \cup \{p_k, I_k\}$  \ \ add the new probe, along with its anonymous identity number to the gallery.

**end for**

//End algorithm

*Return*  $G$

---

# Experiments

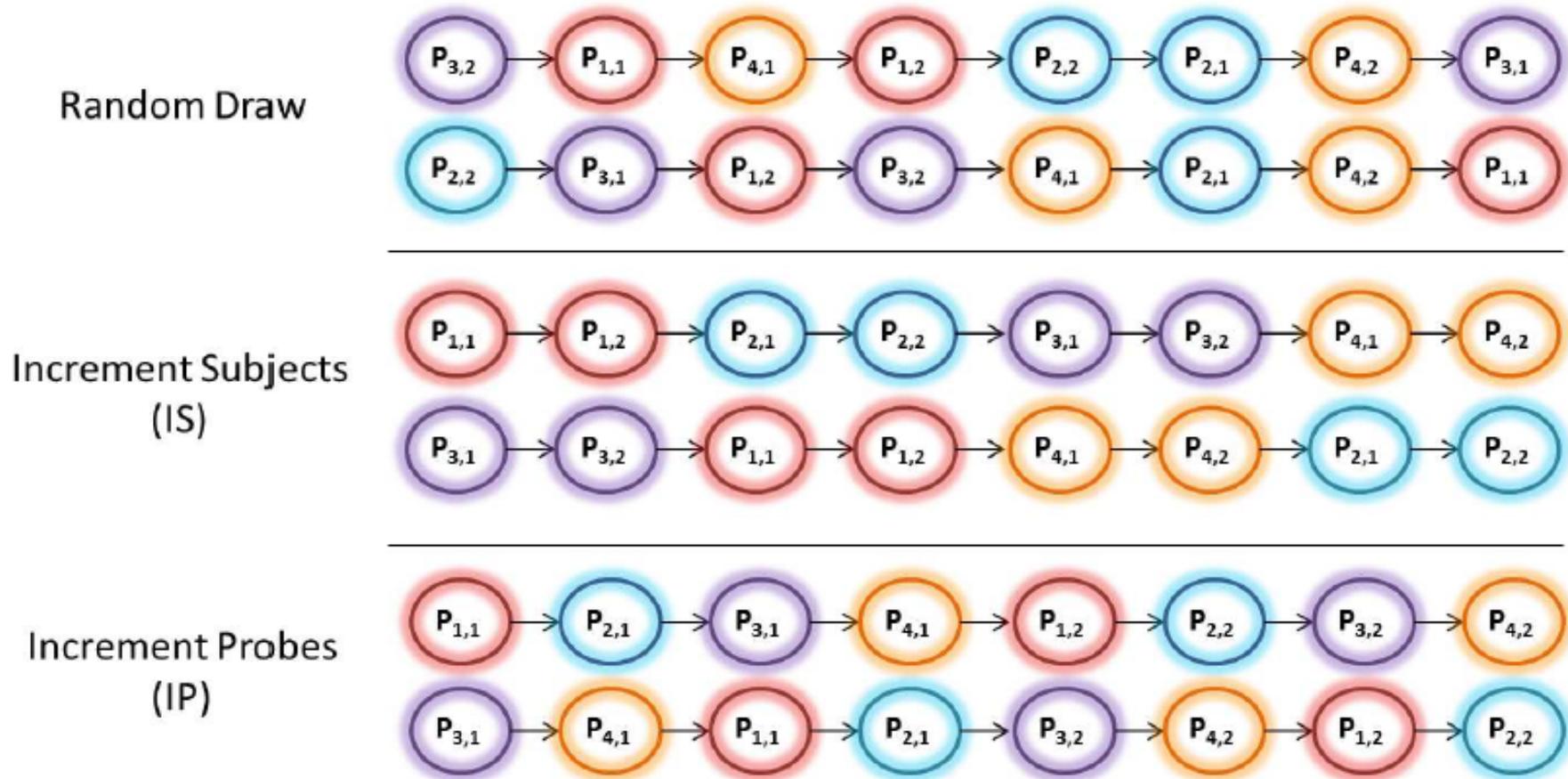
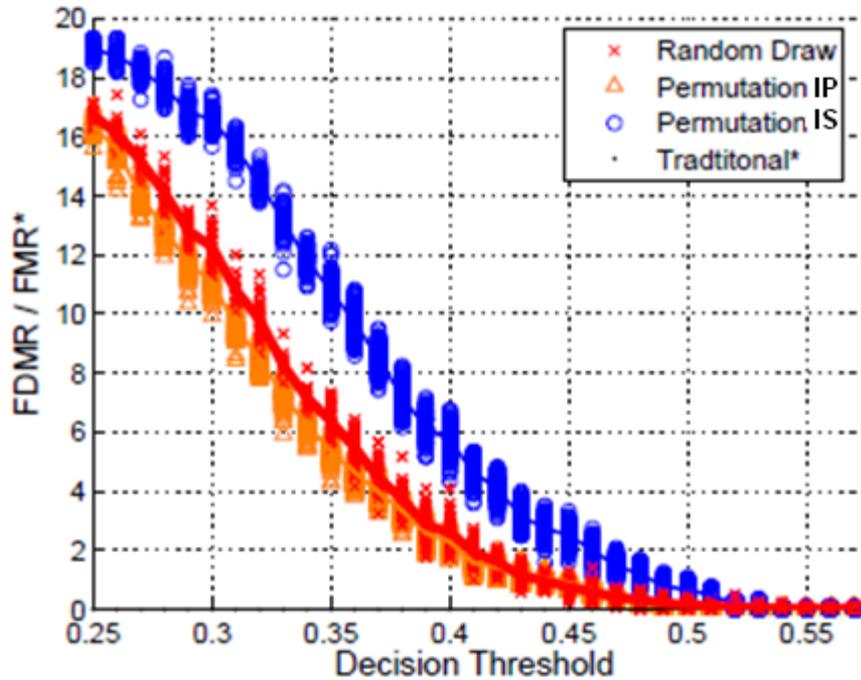


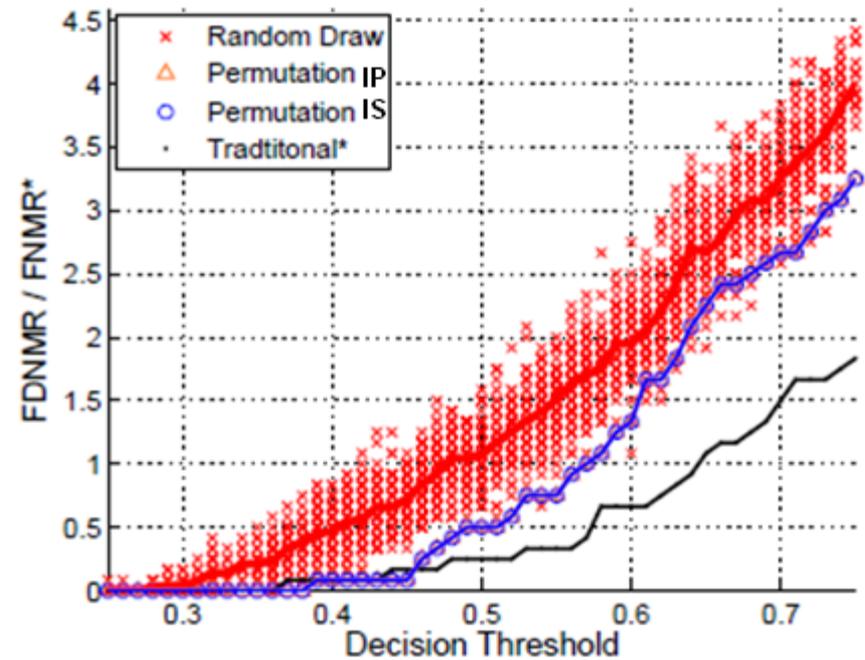
Figure 7: Observation flowchart of permutations “Random Draw”, “Increment Subjects” (IS), and “Increment Probes” (IP), where  $M = 4$  and  $T = 2$ . Note that for permutations IS and IP, the first subscript denotes the  $m^{\text{th}}$  subject and the second subscript denotes the  $r^{\text{th}}$  probe of that subject. In addition, the first subscript does not necessarily follow  $1, 2, \dots, M$ , but rather any combination of  $1, 2, \dots, M$  (e.g.,  $2, 1, 3, 4$ , or  $3, 2, 4, 1$ ).

# Experiments

FDMR – Face Scores

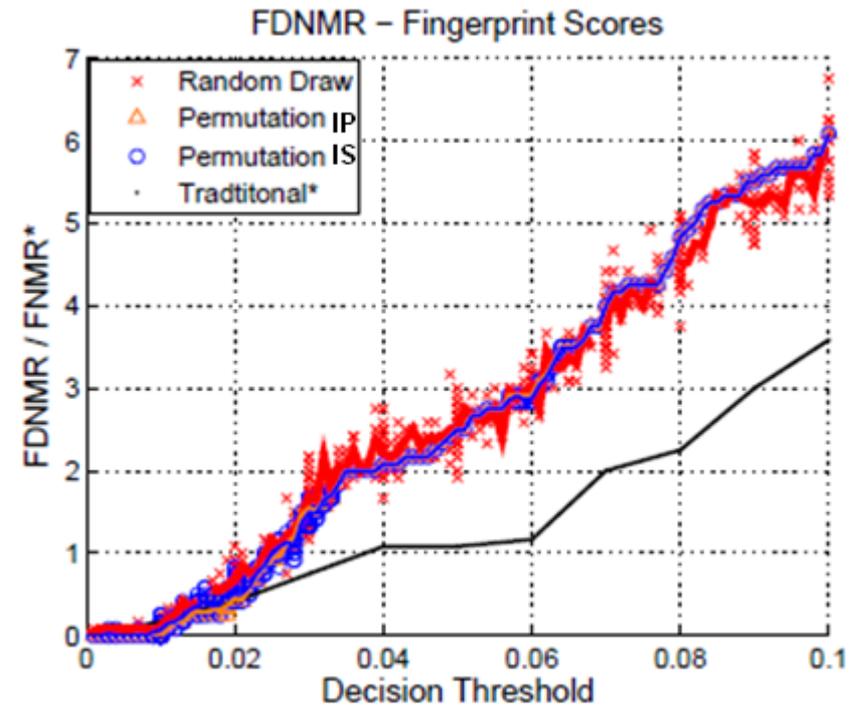
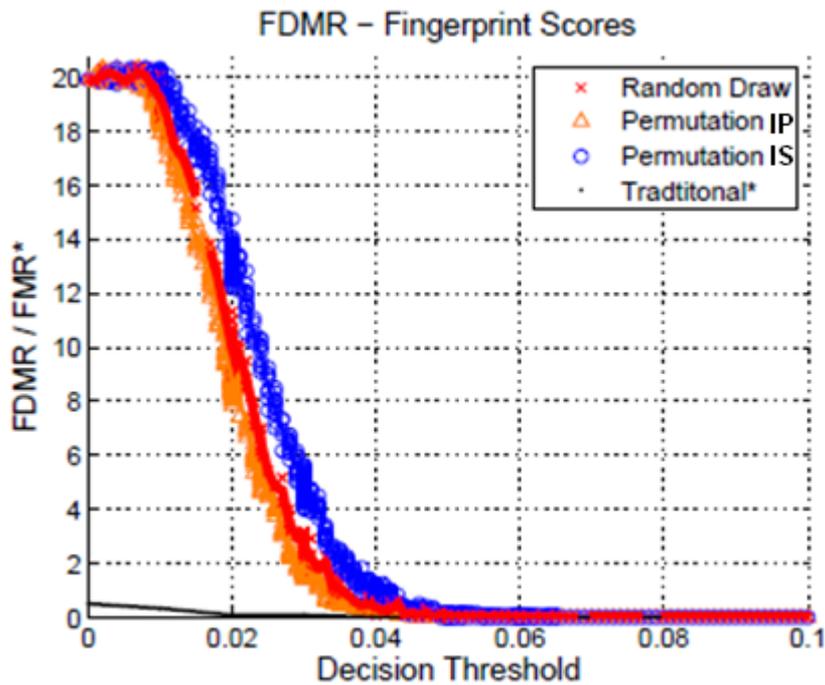


FDNMR – Face Scores



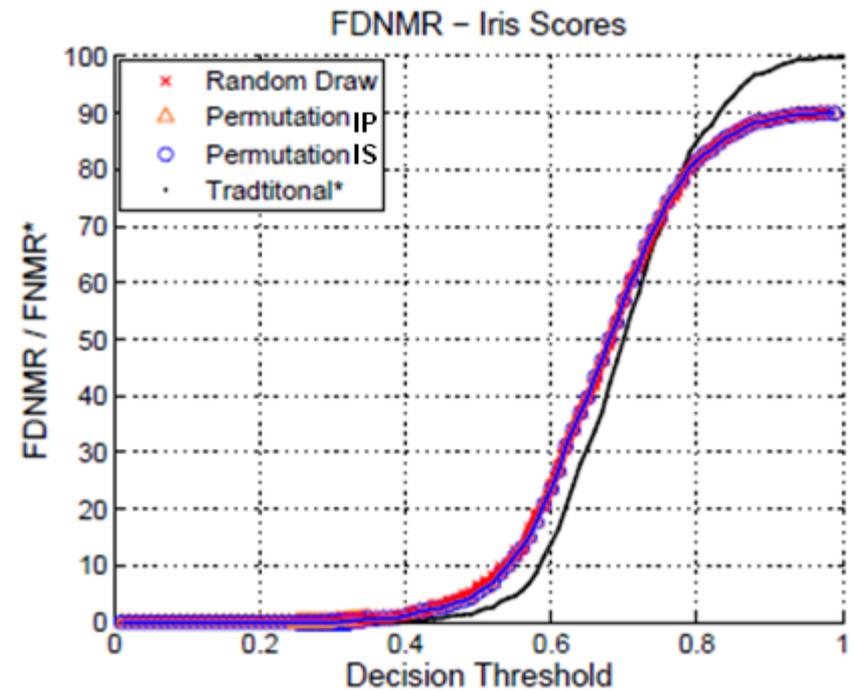
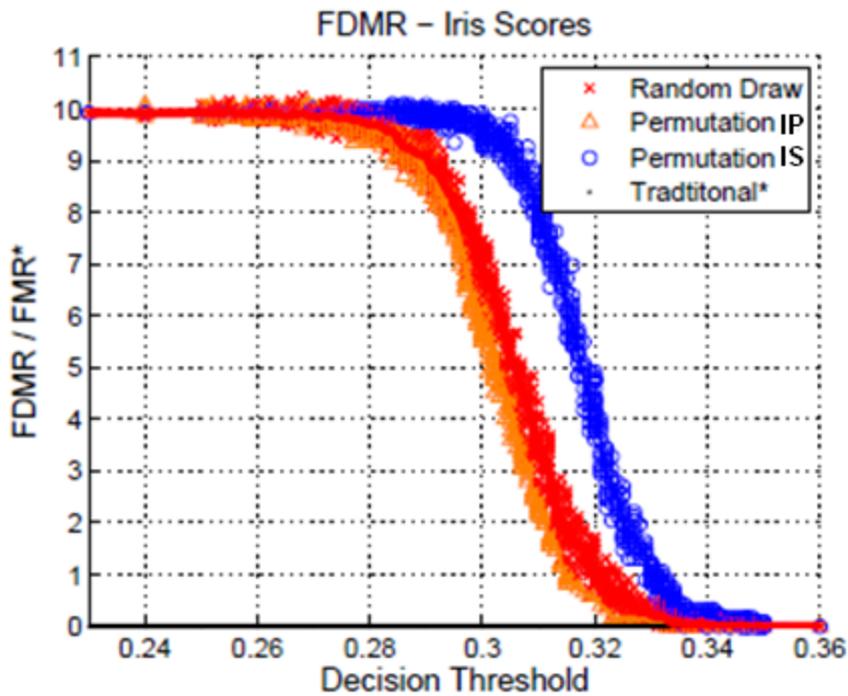
False dynamic match and false dynamic non-match rates for face scores.

# Experiments



False dynamic match and false dynamic non-match rates for face scores.

# Experiments



False dynamic match and false dynamic non-match rates for iris scores.

# Summary

- Traditional vs. Anonymous
  - **Shape** of performance curves **similar**.
  - Intersection of FDMR and FDNMR approximately equal to stated EER
  - Suggests performance is comparable to the state of art.
  - **FMR** and **FNMR** are **poor predictors** of **FDMR** and **FDNMR**, respectively.
- Performance as function of encounter
  - Figures demonstrate the **probability** of observing a false dynamic match can be **significantly impacted** by probe **order**.
    - Evidenced in permutation scatter
    - Permutation IS – Highest Error
    - Permutation IP – Lowest Error
- Error Prediction
  - Accurately predicted observed error rates within +/- 1.5%