A version of this paper appears in the IEEE Computer Society Workshop on Biometrics at the Computer Vision and Pattern Recognition Conference (CVPR'12), Providence, RI, USA, June 2012

"Has this Person Been Encountered Before?": Modeling an Anonymous Identification System*

Brian DeCann and Arun Ross
Lane Department of Computer Science and Electrical Engineering, West Virginia University
bdecann@mix.wvu.edu, arun.ross@mail.wvu.edu

Abstract

We consider the problem of anonymous identification where a biometric system answers the question "Has this person been encountered before?" without actually deducing the person's identity. In such a system, identity profiles are created dynamically as and when the system encounters an input probe. Consequently, multiple probes of the same identity may be mistakenly placed in different identity profiles, while probes from different identities may be mistakenly placed in the same identity profile. In this work, we model the matching performance of an anonymous identification system and develop terminology as well as expressions for predicting decision errors. Further, we demonstrate that the sequential order in which the probes are encountered by the system has a great impact on its matching performance. Experimental analysis based on face, fingerprint and iris scores confirms the validity of the designed error prediction model, as well as demonstrates that traditional metrics for biometric recognition fail to completely characterize the error dynamics of an anonymous identification system.

1. Introduction

In a typical biometric system [5], the input (probe) biometric data is compared against the templates residing in the database (gallery). Each gallery template is labeled with an identity (e.g., user-id, name, etc.) and therefore, the comparison process enables the system to either *deduce* the identity of the input biometric data (referred to as identification or 1:N matching) or *verify* the identity of the input data (referred to as verification or 1:1 matching). The labeling of the gallery template occurs during the *enrollment* phase when the biometric data of an individual is acquired and stored in the gallery.

In this work, we consider a variant of the classical biometric identification system in which (a) there is no explicit enrollment process, and (b) the biometric templates in the gallery are *not* labeled with identity of individuals. Here, the system observes the probe biometric data and determines if a matching entry exists in the gallery.

Classically, a biometric system answers the question: "Who is this person?" or "Is this person who they claim to be?" However, without *a priori* identity information, the problem is fundamentally changed and the system addresses the following question: "Has this person been encountered before?" Therefore, such a system no longer performs classical identity management, but engages in what we define as *anonymous identification*. While the notion of anonymous identification has been previously expressed in the literature, it must be noted that, in this work, the phrase is used in a very different manner. Dodis *et. al.* first defined an anonymous identification scheme where users enroll in ad-hoc groups and prove group membership for subsequent access [4]. Later, Bringer *et. al.* adopted the term anonymous identification in the context of cancelable biometrics [1]. While not directly stated, the phrase has come to refer to schemes for template protection (e.g., face de-identification [7]) or quality assurances for privacy, such as k-anonymity [9]. Here, our definition of anonymous identification is *not* concerned with template protection but, rather, loosely resembles the definition of Dodis *et. al.* [4], as biometric templates are assigned a class label based on the outcome of the matching process. Further, neither the class label from the matcher, nor the matching process necessarily deduces the actual identity of an individual. Figures 1 and 2 illustrate the differences between a traditional biometric system and an anonymous identification system. Note that in our definition, an anonymous identification system does not involve a separate enrollment process and does not report a specific identity as the outcome.

Anonymous identification, as defined in this work, confers a number of benefits that cannot be realized in a traditional biometric system. Since an anonymous identification system primarily addresses the question "Has this person been encountered before?", it can be recognized as a poten-

*Sponsored by grant number N00014-08-1-0895 from the Office of Naval Research

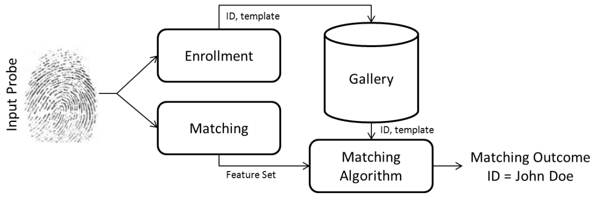

Figure 1. Flow diagram for a classical biometric identification system.

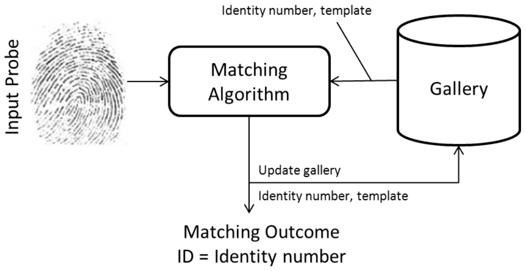

Figure 2. Flow diagram for an anonymous identification system.

tial solution for the de-duplication problem. In the context of biometric recognition, de-duplication invokes searching through a database to *strictly* determine if the probe has been encountered before. De-duplication contrasts to the classical identification problem in the sense that identity labels associated with each gallery entity may not be accurate. This problem has been gaining considerable traction as of late, particularly in the context of national scale ID programs [10]. Anonymous identification also allows for the gallery to be dynamically updated in real-time, wherein an identity profile is either created or updated following each encounter. This may be advantageous in surveillance applications, allowing the system to operate covertly.

Consider a biometric system that encounters some permutation of K probes denoted as $\{p_1, p_2, \ldots p_K\}$. In an anonymous identification system, in order to determine if an individual has been encountered before, the system assesses if the k^{th} probe is similar to any of the preceding $k-1$ probes. As with traditional biometric systems, it is also necessary to quantitatively determine the probability of decision errors. Two types of errors are possible: (a) an encountered probe, p_k is incorrectly matched with one of the previously encountered probes, $p_1, p_2, \ldots, p_{k-1}$ and (b) an encountered probe is incorrectly *not* matched with any of the previously encountered probes, $p_1, p_2, \ldots, p_{k-1}$. Although error analysis through traditional performance metrics such as FMR (False Match Rate), FNMR (False Nonmatch Rate) and ROC (Receiver Operating Characteristic) has been well studied in the literature [6, 8, 11], these measures cannot completely capture the dynamics of anonymous identification for two specific reasons. First, error rates for a traditional biometric system are derived from a fixed gallery. That is, for all permutations of probe encounters, the gallery used is fixed. Second, in a traditional biometric system, the occurrence of an error is a static event which cannot impact future matches. However, in an anonymous identification system, the gallery is dynamically evolving, as new identity profiles are created or old identity profiles are updated. This can lead to two error scenarios. In the first scenario, probes pertaining to a single identity may be erroneously placed in different profiles. In the second scenario, probes from different identities may be placed in a single profile. Further, the probability of such an error may increase or decrease depending on the current gallery size and its entries. Thus, the order in which probes are encountered can impact the probability of error differently. If we define $\mathcal{P}$ to be the set of all permutations of $\{p_1, p_2, \ldots p_K\}$ then two such permutations, $\Pi \in \mathcal{P}$ and $\Theta \in \mathcal{P}$ can result in different error probabilities.

The motivation for this paper is to formally introduce, model, and analyze the performance of an anonymous identification system. To the best of our knowledge, no previous work to date has formally explored biometric recognition with anonymously generated identity classes. The following section accomplishes this by providing a general algorithm for anonymous identification, along with relevant definitions. Further, the error metrics needed to quantify the performance of such a biometric system will be studied. We will also demonstrate that the order in which probes are observed can have a significant impact on the probability of system error and offer methods for predicting system performance. Evaluation will be conducted on three different sets of match scores pertaining to the face, fingerprint and iris modalities.

2. Anonymous Identification

2.1. Formal Definitions

An anonymous identification system consists of exactly the same architecture as a traditional biometric system. This includes components such as a matching algorithm, decision threshold and a gallery database of templates.

Def 1. **Matching Algorithm** - Given two probes p_A and p_B, the matching algorithm computes the similarity match score, $S(A, B)$, between them. $S(A, B)$ is assumed to be normalized in $[0, 1]$.

Def 2. **Decision Threshold** - A pair of probes, p_A and p_B, are said to match if the match score $S(A, B)$ returned by the matching algorithm is above a numerical threshold γ; else, it is a nonmatch.

Def 3. **Gallery** - Gallery G, represents a local database where the encountered probes are stored. Initially, the gallery is a null set.

The fundamental difference between anonymous and traditional biometric systems is in the definition of identity. To highlight the difference, we define identity as being either unique or anonymous.

> ***Def 4.*** **Unique Identity** - The true identity representing a biometric probe (e.g., this probe belongs to "Jason," or "user_123").
>
> ***Def 5.*** **Anonymous Identity**: An identity number that is assigned to a probe by the matching algorithm. Anonymous identities are defined in the integer interval $[1, K]$ and the list of identities are stored in set I. A matched probe receives the cluster number corresponding to the gallery entity that matched with it. Nonmatched probes receive a new cluster number which is 1 more than the maximum value in I.

In our formulation, it is assumed that the matching algorithm generates similarity scores and that the gallery G is initialized to the null set. During online operation, a biometric system will observe a set of probes in a particular order. Each observation of an individual probe is defined as an encounter.

> ***Def 6.*** **Encounter** - The instance when the biometric system observes a probe. Denoted by e_k for $k = 1, 2, \ldots, K$ probes received.

When the gallery G is empty, the very first probe p_1, associated with encounter e_1 is automatically placed in the gallery and assigned anonymous identity I_1. For all remaining encounters, probe p_k is matched against the current gallery. A *dynamic match* with previously encountered probe p_i occurs if $S(p_k, p_i) \geq S(p_k, p_j)$ and $S(p_k, p_i) \geq \gamma$, $\forall i \neq j$, $i, j = 1, 2, \ldots k - 1$. Following the match, p_k is enrolled into the gallery with matching anonymous identity I_i. Here, I_i indicates the anonymous identity of probe p_i. If a match does not exist, a *dynamic non-match* occurs and a new anonymous identity is created within the gallery. The algorithm describing this procedure is indicated in Alg. 1.

Finally, it is necessary to state the relationship between anonymous identification and cluster analysis. Here, we define the term identity cluster to refer to a particular subset of anonymous identity entries stored in set I.

> ***Def 7.*** **Identity Cluster** - Anonymous gallery entries in I sharing a common identity number as designated by the matching algorithm. Each unique number represents at least one entry in G.

Note that this represents one operational approach towards designing an anonymous identification system. Other approaches may be adopted in creating identity clusters (i.e., profiles) within the gallery.

Algorithm 1: Anonymous Identification

```
Input: Biometric probes $p_1, p_2, \ldots, p_K$
Output: Gallery $G$ comprised of $K$ probes with assigned
        anonymous identity numbers $I = \{I_1, I_2, \ldots, I_K\}$.
Define: $S(p_k, p_j)$ as similarity score between $p_k$ and $p_j$.
Initalize: $I_1 = 1$, $G = \{(p_1, I_1)\}$, $I_2 = I_3 = I_K = -1$
//Begin algorithm
for $k = 2$ to $K$ do    for $j = 1$ to $k - 1$ do
        $R(j) = S(p_k, p_j)$
    end for
    if $max_j\{R(j)\}_{j=1}^{k-1} \geq \gamma$ then
        $I_k = I_m$, where $m = \arg max_j\{R(j)\}_{j=1}^{k-1}$
    else
        $I_k = max(I) + 1$
    end if
    $G = G \cup \{(p_k, I_k)\}$
end for
//End algorithm
Return $G$
```

2.2. Error Analysis

An anonymous identification system incurs error like traditional biometric systems. Typically, the matching performance of a traditional biometric system is evaluated through measures such as FMR, FNMR, ROC Curves, d-prime statistic, etc. Classical ROC analysis, for example, illustrates the probability of observing a true accept or true reject, given a specific decision threshold. These curves provide meaningful data regarding separability of genuine and impostor scores, as well as optimal operating thresholds. However, ROC analysis assumes that the identity of a subject is fixed. That is, probe p_k is absolutely associated with an identity in I. In the anonymous framework, this condition does not hold. Here, depending on which permutation of encounters is observed, the actual identity pertaining to probe p_k may or may not have been encountered previously and subsequently, exist in I. Further, even if the respective anonymous identity exists in G, an error can be induced by the matching algorithm. As a result, decision errors and the order of encounter can alter the identity clusters within the gallery. Decision errors can be classified into one of two distinct types. Let M denote the number of unique subjects encountered and N denote the number of anonymous identities. The first type of error occurs when probe p_k incorrectly matches to an anonymous identity I_n, $n = 1, 2, \ldots, N$. This is defined as a *false dynamic match* (FDM). As a consequence, the single identity I_n is then associated with two or more unique individuals in M. The second type of error occurs when probe p_k, which in fact belongs to some identity in I, is not matched with any identity in I. This error is defined as a *false dynamic non-match* (FDNM). Note by definition, a genuine match for p_k must exist within the gallery for a false dynamic non-match to occur. A false dynamic match is however, not bound by this constraint. Further, a false dynamic match does not occur when a probe correctly matches to an identity cluster consisting of the true identity in *addition* to other identities.

The consequences of these errors can impact system performance in different ways. For example, a large incidence of false dynamic matches can potentially bias the matcher to repeatedly match multiple probes to the same anonymous identity in I. The extreme representation of this error occurs at a decision threshold of 0, where all probe encounters are deemed to have a "match" in the gallery. Refer to Figure 3 for a visual representation of this error.

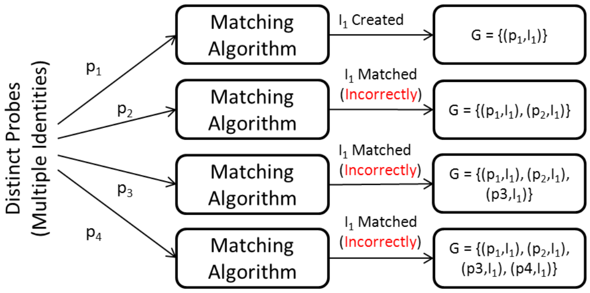

Figure 3. Flowchart of a false dynamic match. Probes of multiple (unique) identities are incorrectly merged into a single identity profile.

The result of a false dynamic non-match is different from that of a false dynamic match. Instead of multiple unique identities being represented in one identity cluster, here a single unique identity appears in several identity clusters. Such clusters often remain small in size, as members have low similarity scores with respect to the range of candidate probes. Again, the extreme case of this error occurs at a decision threshold of 1, where the decision outcome is a "non-match," even for genuine scores. Figure 4 presents a simple flowchart illustrating false dynamic non-matches.

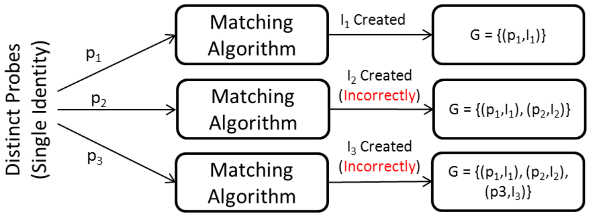

Figure 4. Flowchart of a false dynamic non-match. Probes of a single (unique) identity incorrectly appear in several identity profiles.

2.3. Error Prediction

Although the gallery of an anonymous identification system is dependent on the order in which probe elements are observed, prediction of expected error rates can still be accomplished. Assuming that the probability of encountering any one of K probes is uniform, an analytical approach using combinatorics can be used for error prediction. In this approach, the "events" contributing to the errors need to be identified.

2.3.1 False Dynamic Match

By definition, a 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. This occurs if one of the following events occur.

> ***Event A***: When p_k (observed during encounter e_k) is matched against G, there are no genuine scores generated and at least one impostor score is greater than γ.
>
> ***Event B***: When probe p_k (observed during encounter e_k) is matched against G, both genuine and impostor scores are generated, and there is at least one impostor score that (a) exceeds γ and (b) is greater than all generated genuine scores.

The probabilities of these events are summarized in Equations (2) and (3), respectively. The union of these events defines the general probability of observing a false dynamic match at the k^{th} encounter and is given in Equation (1). In defining these equations, the following auxiliary variables are used. Let N_G, N_I^γ, and C, represent the total number of genuine probes (i.e, those probes for which a matching identity does exist in G), number of impostor scores above γ, and a set of genuine probe combinations, respectively. Further, define N_I^G and C_ℓ as the number of impostor scores above the maximum genuine score during a particular encounter, and the length of each genuine score subset in C, respectively.

$$P(FDM|p_k, e_k) = P(A \cup B|p_k, e_k) \tag{1}$$

$$P(A|p_k, e_k) = \sum_{z=1}^{N_I^\gamma} \frac{\binom{N_I^\gamma}{z}\binom{K-N_I^\gamma}{k-z-1}}{\binom{K}{k-1}} \cdot \frac{\binom{N_G}{0}\binom{K-N_G}{k-1}}{\binom{K}{k-1}} \tag{2}$$

$$P(B|p_k, e_k) = \sum_{\forall C} \sum_{z=1}^{N_I^G} \frac{\binom{N_I^G}{z}\binom{K-N_I^G}{k-z-1}}{\binom{K}{k-1}} \cdot \frac{\binom{K-N_G}{k-C_\ell-1}}{\binom{K}{k-1}} \tag{3}$$

Mathematically, Equations (2) and (3) define the probability of observing a *combination* that satisfies events A and B. Note that the notation $\binom{a}{b}$ represents the binomial coefficient and is defined as "choosing" b elements from a set of a elements.

From Equation (2), the term $\binom{N_I^\gamma}{z}$ defines the number of combinations exactly z imposter probes above γ can be selected from a total of N_I^γ. The next term, $\binom{K-N_I^\gamma}{e_k-z-1}$ defines the number of combinations of $k-z-1$ elements from the remaining $K-N_I^\gamma$ probes. Multiplication of the two terms yields the total number of combinations for a set containing exactly z imposter probes above γ with $k-1$ elements. This number is divided by the total number of all possible combinations of $k-1$ probes, yielding the probability the set of interest occurs. Finally, the summation term satisfies the "at least" condition, allowing the probability to be evaluated for $z = 1, 2, \ldots, N_I^\gamma$. This same principle can be applied to the remainder of Equation (2) and components of Equation (3). Note that $k-1$ elements are "chosen," as upon the k^{th} encounter, the gallery contains $k-1$ elements.

2.3.2 False Dynamic Non-Match

Conversely, a false dynamic non-match occurs when a probe does not match to a genuine gallery entry and all impostor probes which potentially could match have not been observed. Then, the probability of observing a false dynamic non-match for probe p_k at e_k is dependent on the intersection of the following two events.

> ***Event C***: When p_k (observed during encounter e_k) is matched against G, all genuine scores generated are below γ.
>
> ***Event D***: When p_k (observed during encounter e_k) is matched against G, all impostor scores generated are below γ.

As with Equations (2) and (3), Equations (5) and (6) define the probability of creating a combination of gallery entries that satisfy the conditions of events C and D. Event C represents the first condition for a false dynamic non-match, by choosing a gallery whose entries do *not* produce a match score greater than γ. However, probe p_k must also not match to an impostor entry, since a false dynamic would occur. Therefore, a combination of gallery entries is chosen such that all impostor scores must be below γ as well. This is the purpose of Event D. The probabilities for Event C and D are summarized in Equations (5) and (6). The intersection of these events is given in Equation (4). Here, the following auxiliary variables are used. Let N_G^γ represent the number of genuine probes above γ. N_G and N_I^γ retain their previous definitions.

$$P(FDNM|p_k, e_k) = P(C \cap D|p_k, e_k) \tag{4}$$

$$P(C|p_k, e_k) = \sum_{z=1}^{N_G-N_G^\gamma} \frac{\binom{N_G-N_G^\gamma}{z}\binom{N_G^\gamma}{0}\binom{K-N_G}{k-z-1}}{\binom{K}{k-1}} \tag{5}$$

$$P(D|p_k, e_k) = \frac{\binom{N_I^\gamma}{0}\binom{K-N_I^\gamma}{k-1}}{\binom{K}{k-1}} \tag{6}$$

As is, Equations (1) and (4) define the probability of a specific probe, p_k, observing an error during encounter e_k. The mean of this probability for all probes yields the general probability of error at e_k. Further, summation of this probability yields an estimation of observed errors for K encounters. Appropriate scaling establishes an expected value for each of the two rates of error, resulting in:

$$E(FDMR) = \frac{100}{K} \sum_{e_k} \sum_{p_k} P(FDM|p_k, e_k) \tag{7}$$

$$E(FDNMR) = \frac{100}{K} \sum_{e_k} \sum_{p_k} P(FDNM|p_k, e_k) \tag{8}$$

3. Experimental Results

3.1. Datasets

Experiments were conducted using similarity scores generated from three distinct biometric datasets. The first dataset is the WVU Face dataset [2], which contains 5 frontal face images for each of 240 unique individuals. The second dataset is the WVU Fingerprint dataset [2], which consists of 5 fingerprint images for each of 240 unique individuals. Fingerprints captured include the right index (R1), right middle (R2), left index (L1), and left middle (L2) fingers. In the interest of being concise, we restrict analysis to R1 scores. The final dataset is the CASIA Iris Version 3 dataset. Here, a subset of the database is used consisting of 5 left iris images for each of 122 subjects. In total, 2,400 genuine and 717,000 impostor scores were generated from the WVU Face and Fingerprint datasets and 1,220 genuine and 184,525 impostor iris scores were generated from the CASIA Iris Version 3 dataset. Match scores for face, fingerprint and iris were obtained from Veriface, Verifinger, and an open source IrisCode [3] software. DET Curves for the WVU Face, WVU Fingerprint, and CASIA Iris Version

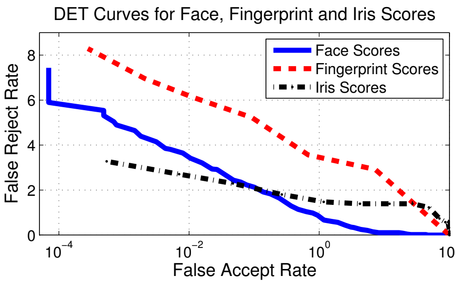

Figure 5. DET curves for face, fingerprint, and iris scores.

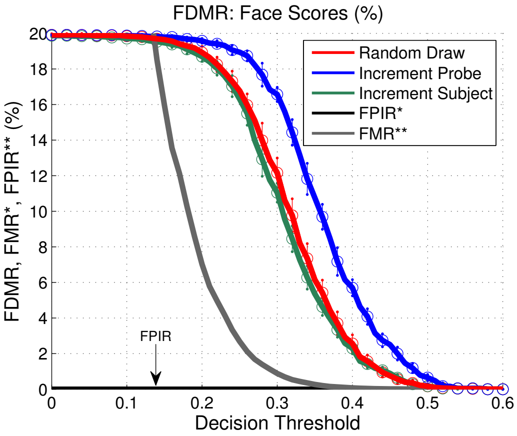

Figure 6. Comparison of FDMR, FMR, and FPIR for face scores.

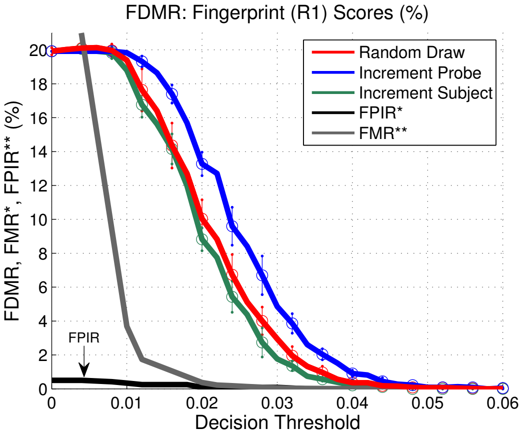

Figure 7. Comparison of FDMR, FMR, and FPIR for fingerprint (R1) scores.

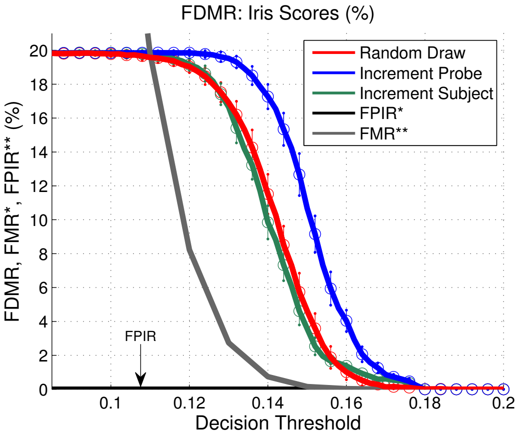

Figure 8. Comparison of FDMR, FMR, and FPIR for iris scores.

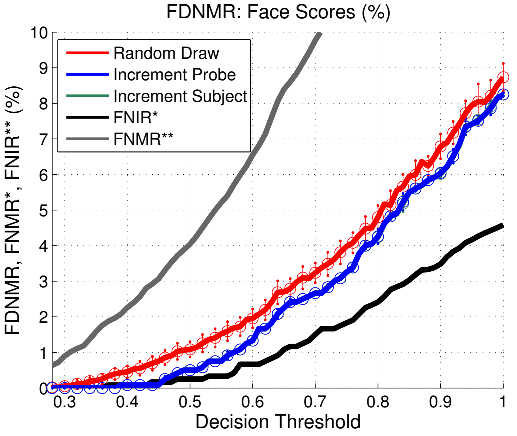

Figure 9. Comparison of FDNMR, FNMR, and FNIR for face scores.

3 datasets are provided in Figure 5. Note the equal error rate (EER) for the face, fingerprint, and iris score sets are 0.912%, 2.121%, and 1.324%, respectively.

3.2. Performance as a Function of Permutation

In the first experiment, the raw performance of an anonymous identification system is evaluated across a range of specified decision thresholds. We evaluate three different types of permutations. The first type of permutation is denoted as *random draw*. Permutations generated via random draw are created by drawing probes at random without replacement. The second permutation, defined as *Increment Probe* (IP), arranges probes such that the probes corresponding to a unique identity occur after every M encounters, i.e., the first set of M probes correspond to the first sample of M different identities, the second set of M probes correspond to the second sample of M different identities, and so on. The third permutation, defined as *Increment Subject* (IS), arranges the probes such that all probes corresponding to a unique identity occur successively.

For each permutation, the observed false dynamic match rate and observed false dynamic non-match rate pertaining to a specific γ is computed. Here, 10,000 distinct permutations of random draw, IS and IP are created and for each permutation, a random value is assigned to γ. For each permutation and γ pair, Alg. 1 is implemented using the specified permutation order. Using the true identity of each subject as ground truth, error rates are extracted by noting the percentage of encounters where a decision error occurred.

Figures 6-11, summarize these results for both false dynamic match rate and false dynamic non-match rate on each of the test datasets. For comparison, a traditional analysis is also conducted, providing FMR, FNMR, FPIR, and FNIR. The FPIR and FNIR is obtained using a leave one out cross validation scheme; that is, for each observation, the gallery consists of every probe except the one in question. Note the traditional analysis is included as a means to compare the respective metric's ability to describe the dynamics of anonymous identification, *not* the performance. In Figures 6-11, each circle (o) denotes the mean FDMR (or FDNMR)

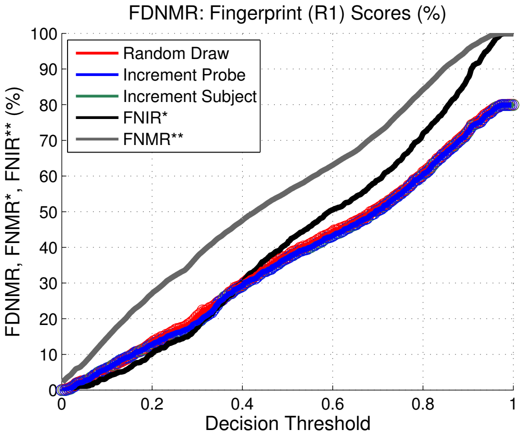

Figure 10. Comparison of FDNMR, FNMR, and FNIR for fingerprint (R1) scores.

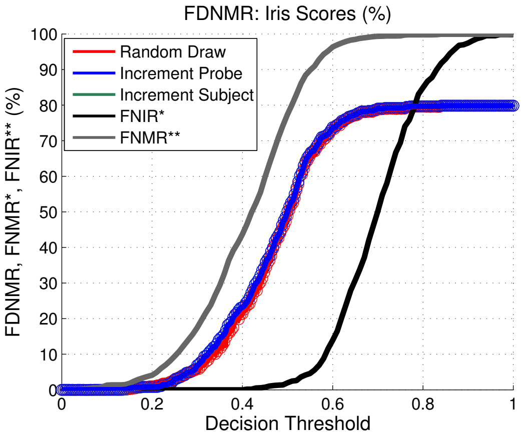

Figure 11. Comparison of FDNMR, FNMR, and FNIR for iris scores.

at that threshold, while dots $(\cdot)$ indicate one standard deviation from the mean.

3.3. Error Prediction

For this experiment, the ability to predict error rates is evaluated. To enable this, we compare the predicted error rates based on Equations (1) and (4) to observed error rates. Predicted and observed error rates are created as follows. First, a bootstrapped test set of 300 probes is sampled from the entirety of a given modality. Each bootstrapped set consists of 5 genuine probes for 60 identities. Bootstrapping into smaller test sets is performed to mitigate computational errors introduced when computing very large combinatorics. In addition, bootstrapping also allows for variation in the data for prediction, allowing for additional prediction and observation pairs to be made at a single decision threshold. Using the bootstrapped data, predicted error rates can be obtained by applying Equations (1) and (4). Observed error rates are generated by averaging the experimental FDMR and FDNMR over 5,000 random draw permutations. Results are presented in Figures 12-14 using the same test sets as in Section 3.2.

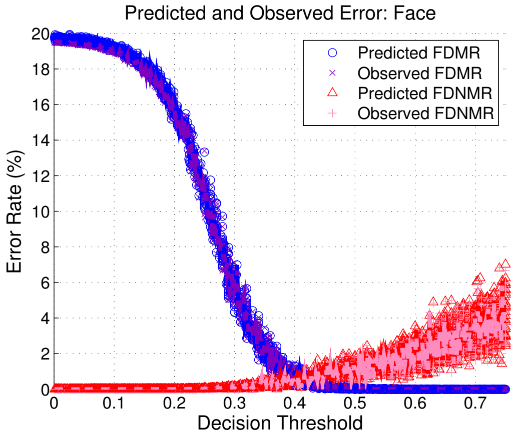

Figure 12. Predicted and observed error rates for face scores.

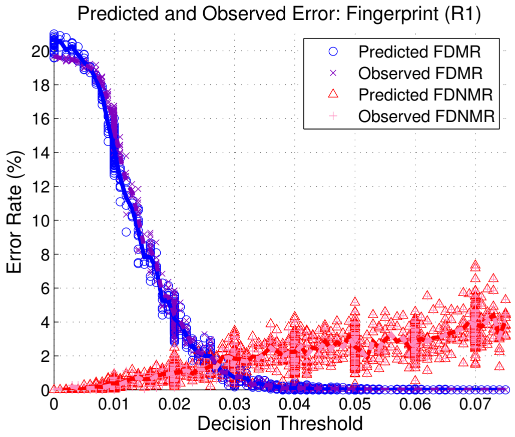

Figure 13. Predicted and observed error rates for fingerprint (R1) scores.

3.4. Discussion and Future Work

From the experiments, it is immediately apparent that the general shape of the curves in Figures 6-11 are not unlike performance curves for traditional biometric recognition, which suggests anonymous identification is certainly a capable means of biometric recognition. However, such similarities are strictly visual. With regard to comparing FDMR and FDNMR to FMR, FNMR, FPIR, and FNIR, Figures 6-11 show that classical metrics poorly describe the errors of an anonymous identification system. Consider first the "false match" error. The traditional analysis generally yields lower rates because of the conditions imposed during testing. In particular, the FPIR is obtained in a leave-one-out cross validation scheme, which presumes each tested probe will always be compared against four additional genuine gallery entries. Such a condition cannot be presumed

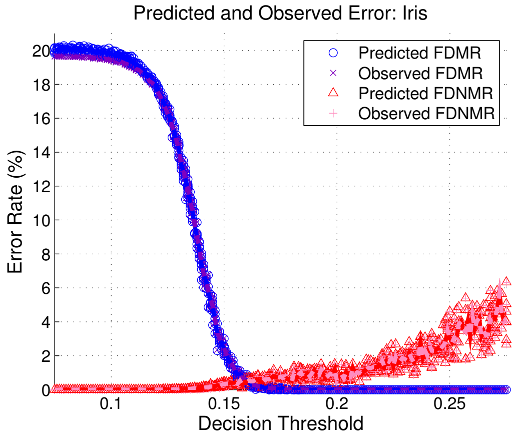

Figure 14. Predicted and observed error rates for iris scores.

to occur in an anonymous identification test, which is why the rates of a "false match" are slightly higher. FNIR and FNMR are not predictors of FDNMR either. While both FNIR and FDNMR represent the probability of a probe incorrectly not matching to some subset of gallery entries, the size and composition of that subset varies for FDNMR, as it may contain some genuine entries (and potentially some impostor entries), while the subset for FNIR is again fixed. For these reasons, metrics such as FMR, FNMR, FPIR, and FNIR cannot be used to describe anonymous identification performance.

Regarding the experiments demonstrating the effect of permutation on observed error, Figures 6-8 demonstrate that the probability of observing a false dynamic match can be significantly impacted by order of encounter. This is evidenced from the differing mean and standard deviation of each permutation. Note that of the three test permutations, IP often resulted in the lowest FDMR and FDNMR rates. This implies a relationship between the number of distinct individuals encountered by the system in its early operating life and future performance.

The proposed prediction performance model proved to be very good, as shown in Figures 12-14, where differences between pairs of predicted and observed errors are within $\pm 1.5\%$. Expanding the analysis to observe prediction against all evaluated bootstraps, the scatter between all predicted and observed values is generally within 2% and 6%. This suggests that the prediction model is able to reasonably approximate error rates even if the test set is isolated from data collected during live operation.

Future studies will include additional tests with match scores generated from other datasets and/or algorithms. Further, it would be interesting to compare performance metrics of traditional recognition and anonymous identification on a large-scale biometric dataset. In particular, it is likely that the observed error rates of traditional and anonymous systems may be proportional as the number of encounters approaches infinity. Future work will also consider on-line and off-line schemes for rectifying errors induced through live operation. Such a scheme could regulate the decision threshold as a function of encounter, thereby maintaining system integrity.

4. Summary

This study accomplishes the following:

- Discusses 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.
- Defines how an anonymous identification system incurs error and how errors from the matching algorithm can be impacted by the order probes are encountered.
- Develops a prediction model for estimating the expected error given a test set of match scores.
- Evaluates the prediction model on three sets of match scores, extracted from recognized matchers.

References

[1] J. Bringer, H. Chabanne, and B. Kindarji. Anonymous Identification with Cancelable Biometrics. *IPSA*, pages 494–499, September 2009. Salzburg, Austria. 1

[2] S. Crihalmeanu, A. Ross, S. Schuckers, and L. Hornak. A Protocol for Multibiometric Data Acquisition, Storage and Dissemination. Technical report, West Virginia University, 2007. 5

[3] J. Daugman. How Iris Recognition Works. *IEEE Transactions on Circuits and Systems for V*, 14(1):2130, 2004. 5

[4] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup. Anonymous Identification in Ad Hoc Groups. *Advances in Cryptology - Eurocrypt 2004*, 3027:609–626, 2004. 1

[5] A. Jain, R. Bolle, and S. Pankanti. *Biometrics: Personal Identification in Networked Society*. Heidelberg, 1999. 1

[6] A. Jain, P. Flynn, and A. Ross. *Handbook of Biometrics*. Springer, 2008. 2

[7] B. Malin, E. Newton, and L. Sweeney. Preserving Privacy by De-identifying Face Images. *IEEE Transactions on Knowledge and Data Engineering*, 17(2):232–243, Feb 2005. 1

[8] A. Mansfield and J. L. Wayman. Best Practices in Testing and Reporting Performance of Biometric Devices. Technical report, UK Govt. Biometrics Working Group, 2002. 2

[9] L. Sweeney. k-Anonymity: A Model for Protecting Privacy. *International Journal on Uncertainty Fuzziness and Knowledge-based Systems*, 10(5):557–570, 2002. 1

[10] UIDAI. Role of Biometric Technology in Aadhaar Enrollment. Technical report, Government of India, January 2012. 2

[11] J. Wayman, A. Jain, D. Maltoni, and D. Maio. *Biometric Systems: Technology Design and Performance Evaluation*. Springer-Verlag, 2005. 2