ID-PRIVACY IN LARGE SCALE BIOMETRIC SYSTEMS

Abhijit Bendale[1],[2], *Terrance Boult*[2],[3]

MIT Media Lab[1], University of Colorado at Colorado Springs[2], Securics Inc[3]

ABSTRACT

Balancing privacy and security concerns in biometric systems is an area of growing importance. While important work has gone on in template protection and revocable biometric tokens, these avenues of research address only one aspect of the problem. Such research does not address a critical issue: balancing the need government and anti-fraud programs to do deduplication (ensure one identity per person) against the potential for abuse using that data. Any existing system capable of deduplication, even if using a template protection scheme, would allow function creep or abuse by searching with latent prints.

This paper introduces the concept of id-privacy, requiring at least i items (e.g. fingers) to be provided to resolve identity to better than d above random chance. We show how using cross-finger representation on unsegmented fingerprint slap data, we can address what may be the single most important "privacy" issue in biometrics, privacy enhanced deduplication. We prove we can achieve (2,0)-id-privacy for fingerprint-based deduplication while preventing searching with a latent print.

We introduce the Forest Finger algorithm – an approach for matching unsegmented slaps and cross-finger representations. Our results on the largest public slap database shows superior accuracy when compared with existing NIST Bozorth matcher when tested on unsegmented slaps, segmented prints or fused rolled prints.

Preprint of paper for IEEE WIFS2010.

1. INTRODUCTION

There is a growing concern about privacy in biometrics [1]. A critical issue in biometrics is the development of technology that allies the privacy concerns while supporting the security goals. A partial solution is to never store the original biometric, but rather only a cancellable or revocable token generated from it. This concept was introduced by Ratha et al [2], called cancellable biometrics. There are a wide range of techniques that convert the raw biometric data into privacy/security enhanced tokens, including Tuyls et al [3] Boult et al [4], [2], Nandakumar et al [5, 6], and Dodis et al [7]. Recent work in this area has show viable, albeit not world class, accuracy in revocable biometrics [4, 8] for single prints. However, these works still miss an important privacy/security problem in biometrics. This heretofore unaddressed fundamental problem with large scale biometric systems is the privacy/security impact of supporting search in

Thanks to NSF STTR 0750485 (Improving Privacy and Security of Biometrics Systems), NSF PFI 0650251 (ISEE:Innovation through Synergistic Entrepreneurial Education). All work done with A. Bendale was at UCCS.

large scale identity systems. For many government programs, or anti-fraud projects, it is critical that the system owner be able do deduplication, ensuring one ID per person.

One privacy/security concern is that all existing ways of searching for duplicates also support searching for whatever reason the system owner chooses, enabling abuse and function creep. Recall the function creep that transformed the US social security number from an DB identifier for social security into a widely used identifier abused in ways never imagined when it was introduced. Furthermore, once a DB with unique and searchable identifiers is hacked, the ability of attackers to use it after that security breach presents serious security concerns.

Some people may think that biometrics provide a truly unique identifier, but biometric recognition is far from perfect. There has been significant progress in both minutiae and ridge based fingerprint matching systems. A detailed survey of existing methods for single fingerprint matching can be found in [9]. However, automated systems are still quite prone to errors. The best fingerprint systems tested by US government, when using 2 fingers, have only 98% true accept rate when set to reject 99.99% of false matches. This brings us to a second security/privacy concern. With non-zero FAR, given a searchable database of millions of records, a *doppleganger attack* (a.k.a biometric dictionary attack) is possible, allowing an intruder to find a few "close enough" matches so that they can directly impersonate them [4]. Since biometrics do not change significantly over a lifetime, the *Biometrics Dilemma* ([4]) is that while biometrics can initially improve security, as searchable biometric databases become widespread, compromises will ultimately undermine biometrics role in security. This is the first paper addressing the important problem of supporting search while still enhancing privacy and deduplication, and can easily be extended to support revocation.

The paper has the following contributions: 1) We formally define the problem of id-privacy 2) Building on top of existing single-fingerprint recognition algorithm, we show how a cross-finger representation on unsegmented data can be used to address id-privacy for deduplication. 3) We experimentally demonstrate, on the largest publicly available slap dataset, that multi-fingerprint recognition/deduplication can be achieved without loss of accuracy.

2. ID-PRIVACY

Multi-fingerprint capture or slap capture (figure 1), is becoming more and more popular in large scale identity management systems like US and UK passports. Vendors have followed the path of segment-and-match, where the multiple fingerprints are first segmented and then matched as in traditional single fingerprint recognition [10]. Although this approach is favorable from a backwards compatibility point of view, it makes it very easy for doppleganger attacks, discussed earlier. Even though cancellable biometric methods address the issue of data protection, from a privacy point of view, it is not sufficient to just protect the template. One of the major fears with biometric data is potential abuse and function creep i.e. the data owner could use the data for other purposes than originally intended. In particular, for government systems, which is where the largest biometric systems are being developed/deployed, a serious concern is searching fingerprint databases with latent prints from crime scenes or otherwise obtained fingerprint data to identify individuals. While some may argue that only the guilty need to fear, that view ignores issues such as the use of government fingerprint data for producing fake data and planting them at a crime scene [11] and even broader issues of misidentification, as in the widely reported case of Brandon Mayfield[12] who was falsely imprisoned based on a search finding a possible match to one latent print at a bombing scene and subsequent FBI examination.

Fig. 1. Example matching Slap Image from NIST Special Database 29 [13], with the sub-regions detected by NIST slapseg overlaid in red.

Protected templates don't solve the problem as they still allow for the system owner to "search", which means they can still be used to identify (or mis-identify) an individual by searching finger-by-finger through the database. Two previous approaches ([4] [6]) address the search concern by providing password enhanced "verification" only techniques. Because these models inhibit searching, they cannot be used for deduplication.

Deduplication is a justifiable security criterion and inherently requires "recognition" and searching the database. This leads us to ask *"is there a way to support deduplication and yet ensure that recognition data may not be abused in searches?"*. This is similar in some respects to the secret sharing problem of Shamir [14], which seeks perfect security below a threshold and full knowledge above it. Our definition must deal with the approximate nature of recognition problems and is formalized as:

Definition 1 ***A recognition representation is said to have*** id**-privacy** ***when using only*** i***-1 items for the search input, the stored data cannot identify subjects with probability*** d ***greater than random chance, yet when*** i ***or more distinct items are present, the subject can be recognized at substantially above chance.***

This is a statement about the representation – i.e. for $d = 0$ no algorithm can do recognition with less than i inputs. For $d > 0$ algorithms/experiments can provide an approximate lower-bound on d. When i and d are known, they are used as a prefix i.e. if it takes 2 independent items to identify the user and $d = 0$, then we would call it (2,0)-id-privacy or simply 2-id-privacy.

This differs from, and is stronger than, the k-anonymity [15], l-diversity and related privacy concepts. We require that with the less than i identity items, the recognition is no better than a factor of d above random chance, independent of the DB size, but identity is resolvable with i or more factors. Note for $d = 0$, it is full anonymity. For a general setting the level of privacy protection of the two models can be related; in a database of N people, k-anonymity relates to $d = \frac{k}{N}$. For biometric recognition, probability above random chance scales well with population size; a particular constant k does not. The more important difference is that our goal is balancing the ability to preserve privacy while still supporting recognition. We bound the amount of data the adversary has about the subject to be recognized but require that adding one more piece of information resolves the ambiguity. Obviously the data model needs to be well matched to the actual problem.

Traditional multi-factor solutions do not provide meaningful levels of id- privacy because they store the factors separately and simply combine the results of matching on each. More recent bio-cryptographic

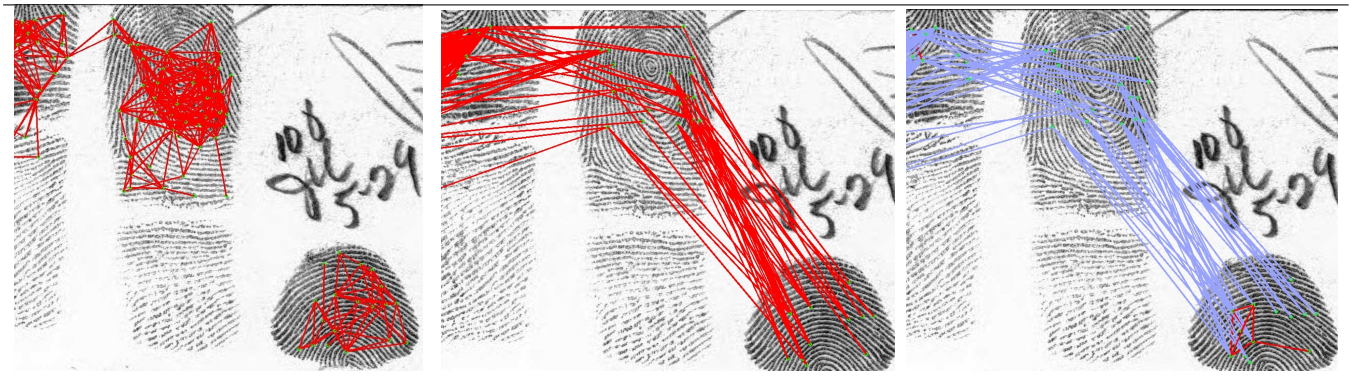

Fig. 2. Left show Forest-Fingers for "within finger" matching on A090_13 from NIST DB29. The lines are minutiae pair features that were matched to a pair in gallery. The middle images shows a portion of the Forest-Fingers for cross-finger matching to support 2-id-privacy. The right image is the cross-finger (blue) with small local features (in red). Note that all start from the same minutiae points, but have different rules for allowed edges.

approaches such as [4] [6] mix the biometric and the password into an inseparable token and can be said to provide (2,0)-id-privacy as they require both the fingerprint and the password to be present. Without the password they are effectively random chance for identification. Unfortunately, the data model of these approaches is not useful for privacy protecting deduplication because the system owner would need passwords for each token to search for duplicates. With the passwords, the system owner could effectively use one or more latent prints for searching.

3. CROSS-FINGER AND FOREST-FINGERS

Our goal is privacy-protecting deduplication using only biometric data, where a latent cannot be used for searching or matching. In our specific problem, we are considering features computed from standard slap images or parts thereof. We want to ensure that with an image of a single finger (e.g. latent), the person cannot be recognized, i.e. we seek at least 2-id-privacy. To do this we introduce the idea of a ***cross-finger representation*** which uses features inherently drawn from different fingers. We can also combine cross-finger features with some local features. Figure 2 shows examples. Before we can prove the id-privacy of our approach, we introduce the type of data and an algorithm for using it.

A fingerprint matching algorithm compares two given sets of fingerprints and returns either a degree of similarity or a binary decision (mated/non-mated). We call the input fingerprint the *probe* and the on-record fingerprints against which the probe is matched is the *gallery*. A slap image also contains crucial information on spatial relationships of features from adjacent fingers. Hence an approach is desired that allows formation of sub-graphs not just within a single finger but also across multiple fingers in order to support cross-finger representations for id-privacy. No existing fingerprint matching algorithm was designed to do this.

For directly matching slaps, we expand upon the NIST Bozorth fingerprint matcher [16], which uses a minutiae-pair representation and builds a graph of matched pairs. Existing algorithms, such as Bozorth, are designed to match a single fingerprint from probe with a single fingerprint in gallery. It is common to attempt to find the largest connected set of matching features between the probe and gallery. When a single fingerprint matching approach like Bozorth is applied on an unsegmented slap image, it generally finds a single matching finger between the slaps and ignores all other fingers. For matching slaps, the approach should support formation of multiple matching connected components as a set or forest of trees/graphs. In Forest-Fingers, we form a forest of trees of minutiae pairs, where the size of these forests defines the match-score between two slap or fingerprint images. We use minutiae pairs because they are translation/rotation independent. The approach presented herein is a true multiple fingerprint matching approach as opposed to fusing matching results from individual fingers. These extensions also improve the matching

accuracy.

We briefly explain the matching process, the first part of which closely follows [16]. From the slap images for the probe and gallery, we extract minutiae points, (x, y, q, θ) where (x, y) is the position of minutia point in fingerprint image, θ is the orientation angle of the ridge at minutia point and q is the NIST quality of the minutia point. Based on list of minutiae points, an intra-fingerprint pair table is formed. A pair table contains the distances and angles between pairs of minutiae points within a fingerprint image. Each pair of minutiae points is represented by the pixel distance between the two minutiae points, the relative angles between the two points and minimum of the quality between the two minutiae points. Pairs with distances outside an allowed rage are discarded. When the pair table formation is completed, each entry in the pair table consists of $\{d_{kj}, \beta_1, \beta_2, k, j, \theta_{kj}\}$ where d_{kj} is the relative distance, $\beta_1, \beta_2, \theta_{kj}$ are relative angles and k, j are indices of the minutiae points under consideration. For further details on computation of distances and angles, the reader is advised to check [16]. The entries in the pair-table of the probe are compared with entries in the pair-table of a gallery to form a match-table with potentially matching entries with differences in distance and angles within certain tolerances. Each entry in the match-table contains matched edges, represented indices of pairs in probe and gallery (p_1, p_2, g_1, g_2). If the edge corresponds to a true match, then the pair p_1, p_2 would correspond to the points g_1 and g_2 respectively. The match-table holds all possible pairs, and is generally not a consistent set.

Input: matchTable (of pairs as in Bozorth)
Output: $matchScore$
foreach *row i in matchTable* **do**
  find all rows consistent with i that is create CMPGs
  foreach *row j in each CMPG* **do**
    find all pairs that form edge with row j
  end
  foreach *each edge-pair formed in CMPG* **do**
    if *edge B ϵ same tree as edge A* **then**
      union(edge A, edge B)
      $parent[B] = A$
    end
  end
  foreach *forest* **do**
    if *no. of vertices in tree $k >$ pruneThreshold* **then**
      $consistentForests+ =$
        $totVertices(tree(k))$
    end
  end
end
$matchScore = size(consistentForests)$

Algorithm 1: The forest-finger matching algorithm

The next task, and where we differ from Bozorth, is to divide the match-table into consistent subgroups. Bozorth searches for the largest consistent web; we build the largest consistent forest. Algorithm 1 presents an overview of this stage of the Forest-Fingers approach. The first step is Consistent Minutiae Pair Group (CMPG) formation. In this process, the match-table is divided into multiple groups of entries of rows such that within each group there is a unique correspondence between a minutia point in the probe match-table and the corresponding minutia point in gallery (i.e p_i corresponds to only one g_j). Each consistent minutiae pair group is a collection of consistent assignments between probe and gallery minutiae points. Another way to view minutiae pair groups is as collection of vertices (match-table entries) in a graph. Two vertices are considered connected if there is a common minutia point between two vertices (match-table entries). The problem now reduces to finding connections within these vertices to form a set of undirected graphs, where the vertices represent the match-table entries (and in turn pairs of

minutiae points). Geometrically, the edges represent relative distance-based local structures and collections of such edges are trees/graphs that represent global structure of minutiae. On a slap, disjoint-set forests are an excellent way to represent this problem, where *find* operation can be used to check whether a new vertex belongs to a tree and *union* operation can be used to merge trees into disjoint-set forests. A collection of all such forests is the representation of the fingerprint slap image. The match-score is the number of vertices in the forest, i.e total number of vertices that form consistent connected graphs within the set of minutiae. While this might seem, at first, to be quadratic in E (number of pairs), the processing is done walking through mutually sorted lists with constant distance requirements, not exhaustive scanning for pairs, so its cost is dominated by the sorting, i.e. $O(E \log E)$.

One of the issues that must be addressed is to make the pair-features stable across images while dealing with noise. In the case of slaps, the local image coordinate system and physical repeatability of close finger placements provide that stability. Without slaps an alternative would be to use consistent segmentation and reliable key feature localization (e.g. core/delta), to align individual fingerprint images to support pair features. An even more aggressive approach would be segmentation and then optimization over possible alignment parameters.

This approach of defining cross-finger matching. i.e. using features constructed from distinct elements of the i different data sources, can clearly be used in a much broader set of algorithms and data. One could use pairs between features in other modalities, e.g. feature points between two independent irises. One could also extend it to cross modality data, e.g. points in thermal and visible imagery, or iris points and eye/retina veins or fingerprint minutiae and finger veins. The pairs need not be graph edges, as we used herein, but could also be conditional or functional pairs, where one element defines a local transformation of the feature, similar to how the [6] uses a password to mix its minutiae data.

4. PROOF OF ID-PRIVACY FOR CROSS-FINGERS

In this section we show how Forest-Fingers can be used to support id-privacy. To implement 2-id-privacy, cross-fingers uses the end-points on separate fingers. As described above, let the model for "items" be single finger images, with the deduplication process taking slaps as input. Assume input with $m \geq 2$ fingers. Create cross-finger forests, where each edge uses data from two separate fingers among the m input fingers.

Recall 2-id-privacy requires two properties, which we now show hold for this model.

Property 1: no recognition from single finger input: Given images/minutiae from one finger (i.e. $(i-1)$ inputs), it is impossible to generate correct pairs that match a significant fraction of the stored pairs since no data about the second finger is known. An adversary could generate random data or use dictionary prints to forms pairs, but such pairs would not be consistent with the subjects print. Hence randomly choosing an subject index, the most effective attack produces performance at random chance. Thus $d = 0$.

Property 2: 2 or more inputs matches above random chance: Assume 2 or more finger inputs each of which have overlap with a subject's gallery images. Then valid cross-finger features can be formed in probe and gallery. Because there is data overlap, the pair matching will be better than random resulting in a probability of recognition substantially above chance. If the number of minutiae pairs is small, the recognition level maybe only slightly above random chance. Increasing pair counts improves the recognition rate. Even if the 2 fingerprint images are not from a slap, an algorithm can test multiple alignments and optimize over the alignment space to produce matching results above random change.
Q.E.D.

We have described and tested pairs. However, the concept is clearly extendible to triples or n-tuples of data being used as the primary representation. E.g. with triples (effectively triangles as in [17]) can be used which could then require at least 3 fingers to be presented. There is security/usability tradeoff here, as it could mean that someone that looses 2 fingers on a hand would no-longer be matchable by the system. Another practical issue is that the number of pairs grows with the square of the number of minutiae, while the number of triangles grows with the cube.

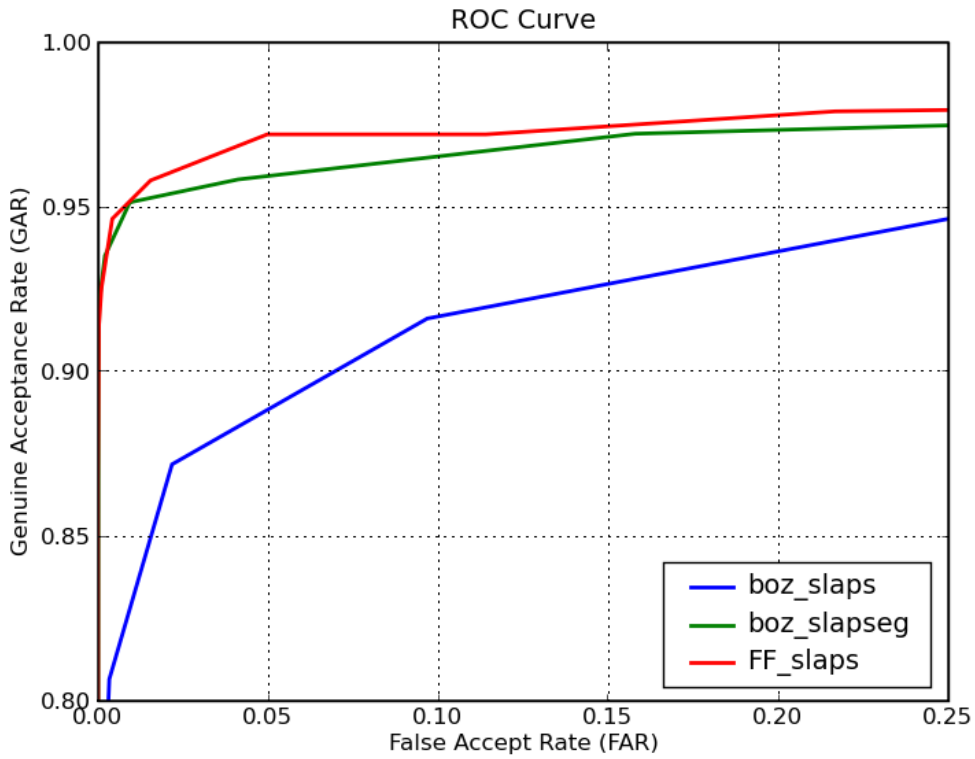

Fig. 3. ROC curve comparing NIST Bozorth Matcher on segmented images with our Forest-Fingers algorithm on unsegmented slap images. In spite of not segmenting the data, Forest-Fingers outperforms Bozorth Matcher. Performance of Bozorth Matcher when applied on straight slaps degrades significantly indicating its dependence on segmentation and inability to address cross-finger matching.

5. EXPERIMENTS

We performed experiments with Forest-Fingers on unsegmented slap images and compared them with NIST Bozorth matcher on both segmented and unsegmented data. We evaluate on NIST DB29 [13] which is, to our knowledge, the largest publicly available dataset of fingerprint slap images. The database contains slap images from 216 individuals (214 distinct), with probe and galley taken at two different instances. Each collection is a 10-print card, with slap prints from left and right hand giving a total of 432 slap images each in of the probe and gallery sets. For segmented data, we used NIST's NFSEG package followed by minutiae extraction process via MINDTCT [16]. When using segmented data, each probe fingerprint sub-image was compared with its respective fingerprint sub-image from the gallery (i.e. the index finger from probe was compared with the index finger of gallery). The final score was the sum of scores from the comparison of all fingers, i.e. sum-score fusion over all segmented fingers was used.

For slap matching, minutiae points were extracted from the unsegmented slap image with identical data fed directly into the matching algorithms. Bozorth parameters were changed to accept the larger number of points and greater range of data needed for the slap data. Forest-Fingers algorithm was used for probe and gallery and score was computed as discussed previously.

The results of all the three experiments mentioned above are summarized in figure 3 as receiver operating characteristic (ROC) curve plotting the genuine accept rate (GAR) against false accept rate (FAR) at various thresholds.

Cross-Finger Matching: In order to show the viability of 2-id-privacy, we performed some initial experiments on cross-finger data, with pair endpoints on different fingers. This can be done either using segmentation or by ensuring the minimum distance between the two minutiae in a pair is greater than the maximum distance between

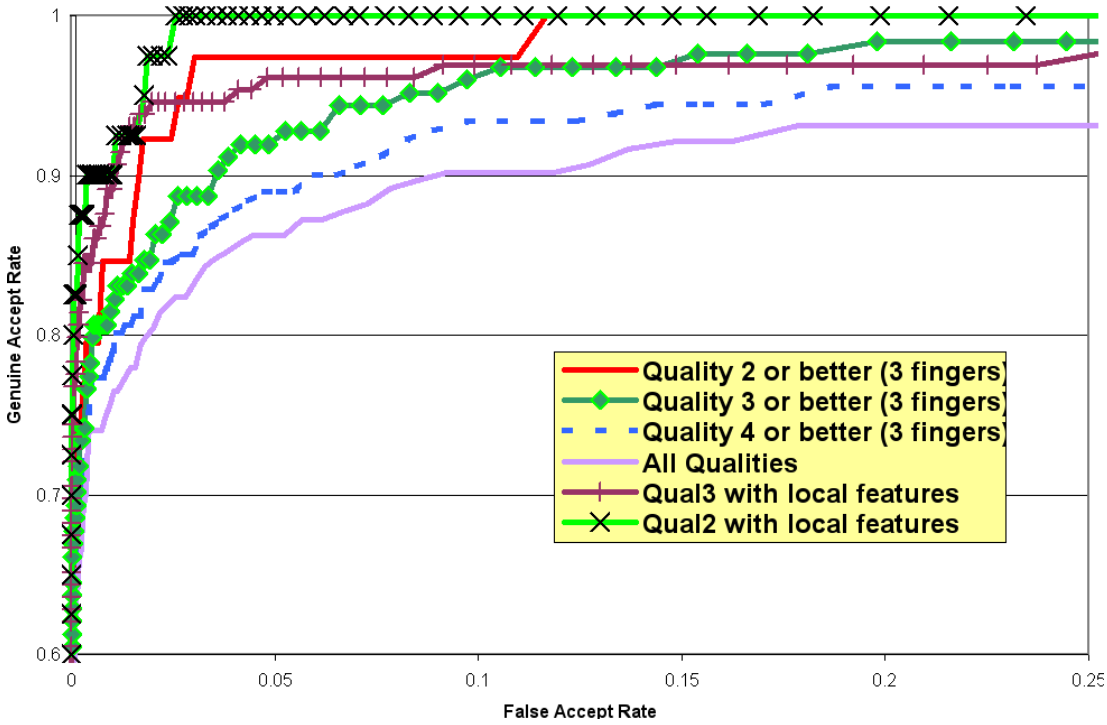

Fig. 4. ROC curve showing performance of the 2-id-privacy crossed-finger approach using Forest-Fingers. Because of the weak definition of features for pairs, this is more significantly impacted by fingerprint quality, making it more difficult to use even if there were latent slaps. The curves shown are for different levels of minimum quality, with each curve using only data with at least 3 fingers per slap having the specified NFIQ quality or better. Also shown are cross-finger matching with a small amount of local-finger pairs, which results in (2,.04)-id-privacy.

minutiae within a single finger. The latter is the approach used for the experiment herein allowing pairs to span 2 or 3 fingers and sidestepping the need for segmentation. This cross-finger representation matched with Forest-Fingers is the first of its kind and we do not claim it to be the definitive or optimal way to provide 2-id-privacy. Still, the data shown in figure 4, is promising.

In analyzing the cross-finger recognition performance, three things became apparent. First, poor quality prints were significantly increasing false matches and their scores. Second, there were considerably more high-scoring false matches than in the per-finger matching. Thirdly, some false rejects had particularly low-scores, in part because of finger movement between slaps. We briefly discuss how these might be addressed.

At first the dependence on quality might sound like a disadvantage, but modern optical scanners used in deduplication generally produce high-quality images. The fact that latents are almost always low quality means this dependence will actually improve privacy while allowing digital image-based deduplication. (The quality issue is aggravated by the fact that this data was from scanned FBI fingerprint cards and not a live-scan device so deduplication performance may be even better.) To help understand the impact of quality, we ran new experiments using subsets of the data where we filtered on quality. We also removed the 2 duplicates in the dataset and the 2 people where the images were not actually slaps but rather where the person repeatedly applied the same finger instead of a 4-slap. Then we processed for actual print quality. Unfortunately the NFIQ program does not seem to accurately measure quality of an slap image, so we instead used NFIQ on each of the segmented images with the requirement that three of the four slap fingers have a quality of X or better. This reduces the population and number of matching attempts. For quality 2,3,4 and 5(all) the resulting subsets allowed for comparisons with Subjects/Total Matches of 40/12348, 129/52735,186/80914,209/90999 respectively. Figure 4 shows the ROC curves for cross-finger Forest-Fingers matching results for different levels of quality.

The high-scoring false matches could be reduced by adding more descriptive features to the minutiae. This paper uses basic features that would be computable with any ANSI/ISO-standard fingerprint minutiae extractor. It is well documented that other, often proprietary, features can improve per-finger matching algorithms. These features may expose some information about the individual suitable for latent matching, so some care would be needed in their design/usage. To show the potential impact of local information, testing allowing a limited number of pairs within a single finger (with distances only up to 75 pixels) to be part of the Forest-Fingers information. With this local per-finger information we no-longer have (2-0)-id-privacy, as there is some potential for local matching. Attempting to match rolled prints (also in NIST DB29) against the cross+local information, the EqualErrorRate decreased to 46% from the random rate of 50%. Thus one might say this cross-fingers with local information approach achieves approximately (2,0.04)-id-privacy while substantially improving the overall recognition rate at low FAR.

6. CONCLUSIONS AND FUTURE WORK

This paper presented a new formal model: id-privacy. The algorithm/experiments herein show **the first solution to one of the most pressing privacy problems in large-scale identity biometrics: how to allow automated detection of duplicates while ensuring it cannot be abused by using a latent to search for people**. This paper also introduced id-privacy as a model for this important problem. We showed how our approach solves 2-id-privacy, presenting ROC curves showing accuracy tradeoffs. The performance is, admittedly, not yet as good as using the best known algorithms. However, remember that deduplication only needs to be done once. The goal here was to formalize the problem and develop a new model and algorithm that shows potential. The early protected-template research did not provide sufficient performance to be of practical use, but continued research increased performance and now there are multiple commercial products in that space.

This paper introduced Forest-Fingers for direct slap matching, showing how simultaneous matching can improve multi-fingerprint matching. We demonstrated improved accuracy on the NIST standard dataset against the NIST baseline algorithm. The increase is largely because the errors in segmentation do not propagate to limit the slap matching, which means the concept should improve other matching algorithms as well. It is important to note that we are not presenting here a definitive slap fingerprint recognition approach. There are many other fingerprint recognition algorithms that perform better than Bozorth matcher on single fingerprint recognition. Bozorth was chosen as the the best performing open-source fingerprint recognition algorithm, simplifying comparison. It is known that the best performing matchers use features beyond simple minutiae location, and the Forest-Fingers approach could easily be extended to handle such information. If the pair end points were more descriptive of their local neighborhood, e.g. using minutiae descriptor features as mentioned in [18], it would reduce false pair matching, and could definitely improve results.

The paper introduced the cross-finger representation as one means of achieving id-privacy. We believe that many fingerprint algorithms could be extended with concepts based on Cross-finger data and Forest-Fingers to fuse information from multiple fingers to provide id-privacy.

There are some elements of both practically and privacy that have not yet been discussed, but form an important part of our planned future work. The first is applying a privacy-enhance transform and template protection scheme to the slap "pairs". While it is unknown if these cross-finger pairs could be used to construct an approximate fingerprint, the privacy enhancing transforms of [4, 8], can be applied to these types of "pairs", with the latter has the added advantage of allowing key embedding. The key embedding could then be used to enhance the actual deduplication processing by allowing human comparison of actual images to distinguish difficult cases. If the images are protected by person-specific encryption keys, then if there is sufficient matching, i.e. a potential duplicate, the system could decrypt the images for secondary

processing. The system owner does not need to keep keys, potential duplicates would match well enough to release the needed keys!

Finally, if during enrollment (i.e when submitting for deduplication) a verification only privacy-enhanced biotoken which permits deriving new tokens from its the base enrollment ([8]) is linked to the ID, then we can finally have a "biometric-based" ID system with moderate privacy/security protection that still supports rapid 1-1 secure revocable verification tokens. We hope that this introduction to the problem of privacy-protecting deduplication will encourage biometric designers to join us in trying to build practical solutions to this important problem.

7. REFERENCES

[1] A.K.Jain S.Prabhakar, S.Pankanti, "Biometric recognition: Security and privacy concerns," *IEEE Security and Privacy*, vol. 1, pp. 33–42, March 2003.

[2] J. Connell N. Ratha, S. Chikkerur and R. Bolle, "Generating cancelable fingerprint templates," *IEEE TPAMI*, vol. 29.4, pp. 561–572, 2007.

[3] T.A.M.Kevenaar G.J.Schrijen A.M.Bazen R.N.J.Veldhuis P. Toils, A.H.M.Akkermans, "Practical biometric authentication with template protection," *AVBPA*, 2005.

[4] W.J. Scheirer T.E. Boult and R. Woodworth, "Revocable fingerprint biotokens:accuracy and security analysis," *CVPR*, 2007.

[5] A.K.Jain K. Nandakumar and S.Pankanti, "Fingerprint-based fuzzy vault:implementation and performance," *IEEE Transactions of Information Forensics and Security,*, vol. 2, pp. 744–757, December 2007.

[6] A. Nagar K. Nandakumar and A. K. Jain, "Hardening fingerprint fuzzy vault using password," *ICB*, 2007.

[7] L. Reyzin Y. Dodis, R. Ostrovsky and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. of Computing*, vol. 38, pp. 97–139, 2008.

[8] T.E. Boult W.J. Scheirer, "Bipartite biotokens: Definition, implementation, and analysis," *ICB*, pp. 775–785, 2009.

[9] S.Prabhakar D.Maio, D.Maltoni and A.K.Jain, "Handbook of fingerprint recognition," *Springer*, 2009.

[10] C. Watson M. Indovina K. Kwong B. Ulery, A. Hicklin, "Slap fingerprint segmentation evaluation 2004 analysis report," *NISTTIR 7209*.

[11] S. Jasanoff, "Just evidence: The limits of science in the legal process," *J. of Law, Medicine & Ethics*, vol. 34(2), pp. 328–341, 2006.

[12] S. A. Cole, "More than zero: Accounting for error in latent fingerprint identification," *J. of Criminal Law and Criminology*, vol. 95, 2005.

[13] C.I.Watson, "Nist special database 29: Plain and rolled images from paired fingerprint cards," .

[14] A. Shamir, "How to share a secret," *Communications of the ACM*, p. 612613, 1979.

[15] B. Malin E. M. Newton, L. Sweeney, "Preserving privacy by de-identifying face images," *IEEE Trans. on Knowledge and Data Eng.*, vol. 17(2), pp. 232–243, 2005.

[16] M. D.Garris. E.Tabassi C.I. Wilson R.M.McCabe S.Janet C.I.Watson, "Nist fingerprint image software 2," 2004.

[17] Jin Teoh A. B. Ong T. S. Jin, Z. and Tee C, "Secure minutiae-based fingerprint templates using random triangle hashing," *Int. Conf. on Visual informatics: Bridging Research and Practice*, vol. LNCS 5857, pp. 521–531., 2009.

[18] K. Nandakumar A. Nagar and A. K. Jain, "A hybrid biometric cryptosystem for securing fingerprint minutiae templates," *Pattern Recognition Letters*, vol. 31, pp. 733–741, June 2010.