

Comparative Analysis of Registration Based and Registration Free Methods for Cancelable Fingerprint Biometrics

Achint O. Thomas, Nalini K. Ratha, Jonathan H. Connell and Ruud M. Bolle

IBM T.J. Watson Research Center
19 Skyline Dr, Hawthorne, NY - 10532
{aothomas, ratha, jconnell, bolle}@us.ibm.com

Abstract

Cancelable biometric systems are gaining in popularity for use in person authentication for applications where the privacy and security of biometric templates are important considerations. A variety of approaches have been proposed in the literature. In this work, we have chosen two (a registration based and a registration free) techniques and performed a comparative study focusing on template representation size, useful dataset coverage, system accuracy and transform strength. Results show that both systems have their own advantages that are suited for use in specific applications.

1. Introduction

Cancelable biometrics has been shown to be of great use in securing the privacy and revocability of biometric templates [1, 2]. Privacy involves not being able to cross-match biometric templates from different databases while revocability allows an individual to be issued a new template should an existing template be compromised (stolen by an imposter). In the fingerprint biometric domain alone, a number of cancelable techniques have been proposed [3, 4, 5, 6]. In this work, we compare two techniques for generating cancelable fingerprint templates from fingerprint images. One is a registration based technique and the other is a registration free technique. Hereinafter, the two techniques will be referred to as the folding and the triangles techniques respectively. A real time dataset is used for performing the comparative analysis. In section 2, we present an overview of the two techniques. Section 3 gives detailed performance analysis of the two techniques in terms of template

representation size, useful dataset coverage, system accuracy and transform strength. In section 4, we summarize the results and contrast the advantages of each technique.

2. Prior Work

The folding technique is described in [4]. It requires an explicit registration step to align a fingerprint image to a pre-determined point of reference on some co-ordinate system. Registration is achieved by using the fingerprint's core (singular point) location and orientation [7] as the anchor on which the co-ordinate system is overlaid. The technique works by performing a one-way transformation in the feature domain using a parametric one-way (secret) function. The one-way function takes the form of a surface-folding transform. Figure 1 shows this technique.

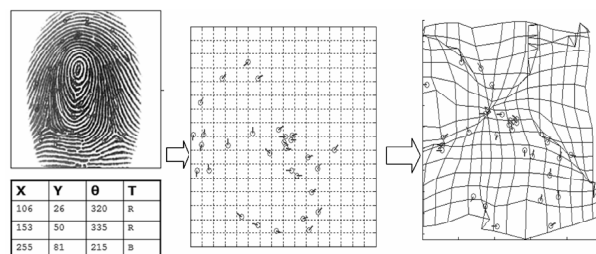


Figure 1: Folding technique [4]

The triangles technique is described in [5] and extended in [8]. It does not use the minutiae directly as features but instead computes higher level meta-features (triangles). For any set of three minutiae, a triangle can be formed. Three sides of the triangles, three angles of minutiae orientation and the height of the largest triangle side are used as invariants. Each invariant is quantized to allow for intra-user variance. If sides are quantized by s bits, angles by a bits and the

height by h bits, a triangle can be represented by an index of $n=3*(s+a)+h$ bits. By considering only unique triangles, a binary histogram of 2^n bins can be constructed. This representation can be secured by shuffling the bins and then encrypting based on some key or token. Figure 2 shows this technique.

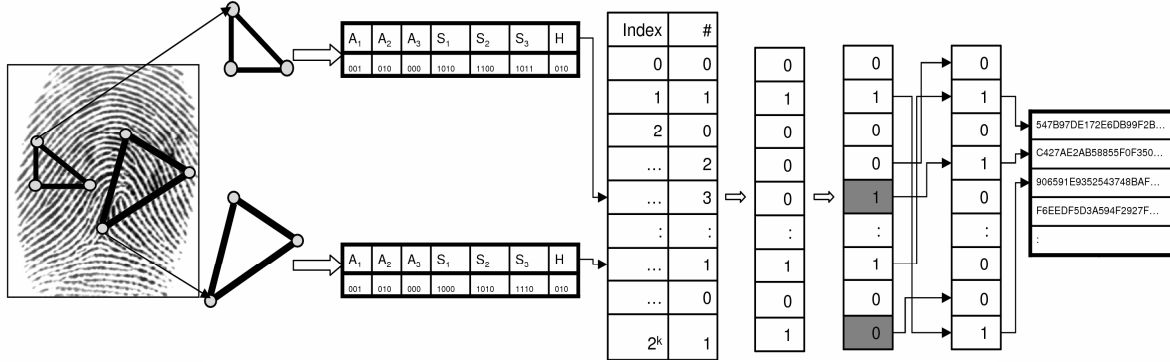


Figure 2: Triangles technique [5]

3. Performance Comparison

Performance evaluation was carried out using the IBM99 optical fingerprint dataset which contains 780 individual fingerprints with 2 samples per finger. No prints were discarded. For the cancelable tests, each fingerprint was enrolled with a unique token. Imposters used the token of the user they were testing against. This simulates a realistic scenario where it is possible for the tokens (identities) to be stolen.

The folding technique uses the minutiae themselves as features in the matching of two templates. This allows using a variety of existing feature extractors and matchers. We have used two systems. One is an in-house experimental system and the other is a commercially available system. A combination system, using the feature extractor of the commercial system and the in-house matcher, was also tested. The triangles technique uses a system developed in-house.

3.1 Template Representation Size

The transformed templates generated by the two techniques have different representations. For the folding technique, the template takes the form of a set of m triplets $\langle x_i, y_i, \theta_i \rangle$ where m is the number of minutiae extracted from a fingerprint image and each triplet represents a transformed minutia. Hence, the total size of a template will be $s_{RB}=m*3*bpf$ where bpf is the number of bits, per feature, in the triplet. For the triangles technique, the template takes the form of a set of b quadruplets $\langle index_i, \theta_i, x_i, y_i \rangle$ where b is the number of bins in the binary histogram that contain a 1

(triangles present) and $index_i$ is the index, θ_i is the median of angle orientations and x_i and y_i , are the centroids of the i^{th} triangle (see [8]). Hence, the total size of a template will be $s_{RF}=b*(bpi+3*bpf)$ where bpi is the number of bits for the index. Table 1 shows a comparison in average representation sizes between the two techniques.

Table 1: Average template representation size

	In-house	Commercial	Triangles
Feature Count	36.33	50.47	991.93
Template Size	0.218 KB	0.303 KB	8.93 KB

The folding technique generates a more compact template. Typical number of minutiae extracted is between 30 and 60. This is an order of magnitude less than the number of valid triangle indices generated by the triangles technique. The per-feature-size also varies between the techniques. Assuming 2 bytes for each of θ_i, x_i, y_i and 3 bytes for each $index_i$, the folding technique needs 6 bytes per feature while the triangles technique needs 9 bytes. A point to note is the feature count for the triangles technique. For 30 minutiae (minimum) extracted from a fingerprint, there should be ${}^{30}C_3 = 4060$ triangles. However, not all triangles will be considered as valid triangles. A lower bound, slb , is placed on each triangle side. Also, only the first f triangles formed for any given minutia are considered. This pruning increases computational efficiency, while ensuring that the triangles capture the distinctiveness of the fingerprints. The thresholds f and slb are set empirically (see [5]).

3.2 Dataset Coverage

The folding technique depends on reliable detection of the singular points in the fingerprint. However, fewer samples will exist with a reliability value greater than some threshold T , as T increases. This is seen in

figure 3. Label core+ T is for all samples with singular points detected with a reliability of at least T . The effective size of the database falls as T increases. This can be viewed as a combination of the failure to enroll (FTE) and failure to acquire (FTA) errors. During enrollment of a fingerprint, the sample can only be enrolled in the dataset if its singular point detection reliability is greater than some T . Otherwise a FTE error is generated. Similarly, during verification, if the singular point detection reliability is less than T , the sample is rejected resulting in a FTA error.

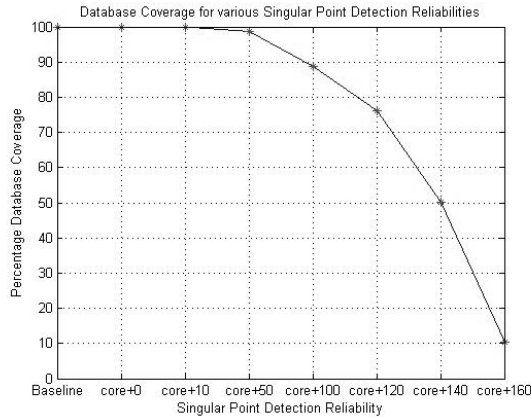


Figure 3: Dataset coverage for different values of singular point detection reliability

Note that this only applies to the folding technique and is not an issue for the triangles technique.

3.3 System Accuracy

Figure 4 shows the performance of the folding technique as singular point detection reliability varies. When the reliability value increases, the performance improves. The behavior is as expected since more reliable singular points means the registration will be more accurate.

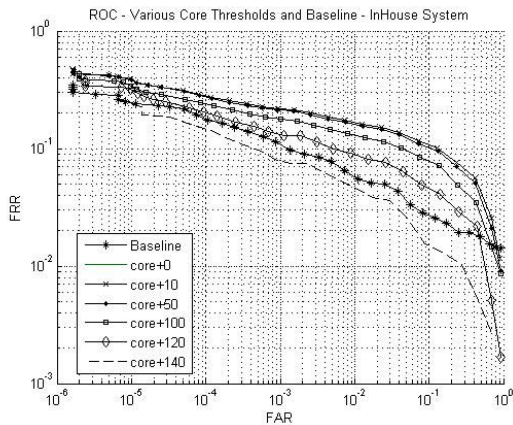


Figure 4: ROC for in-house system

Figure 5 shows the performance curve for the combination system in comparison with both standalone systems. The performance improves in the cancelable case when using the combination system compared to the standalone systems. The baseline performance for the commercial system is much higher than for the combination system. It was also noticed that this performance gap does not translate to the case when cancelable transforms were applied. This could be because the in-house matcher was built to be more robust in handling any distortions introduced in the transformed features.

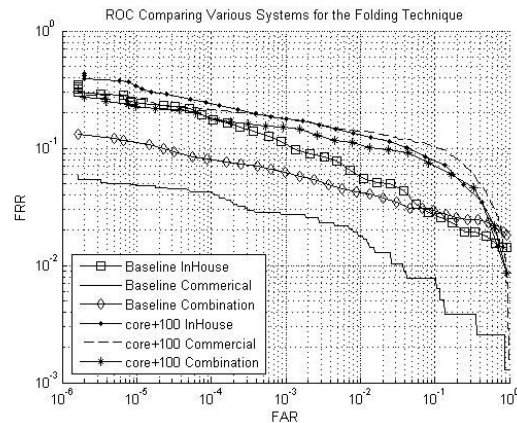


Figure 5: ROC for folding technique

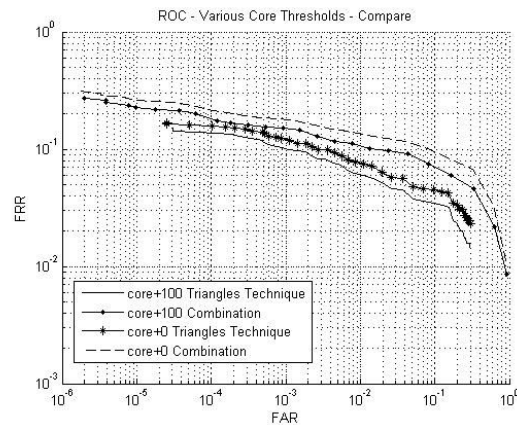


Figure 6: ROC comparing both techniques

Figure 6 compares the performance of the two techniques. Two configurations, core+0 and core+100, were tested; the triangles technique performs better in both. Exactly the same sets of prints were discarded for both techniques when using the reliability threshold. Hence, the comparison can be considered fair. Higher reliability threshold configurations may be suitable for high security, controlled access applications, where the dataset size is limited and re-enrollment on FTE or re-acquisition on FTA is not a big concern. For a user-

friendly system where FTE and FTA rates must be maintained low, it is better to opt for lower thresholds.

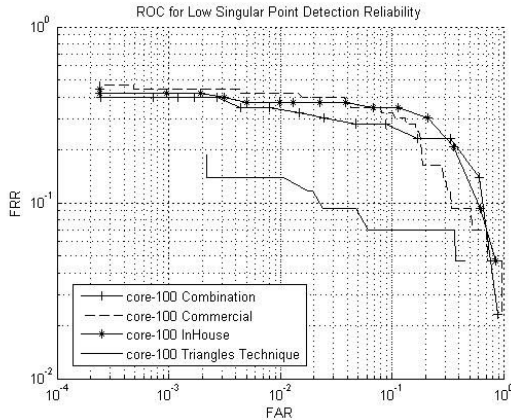


Figure 7: ROC for low singular point detection

Figure 7 compares the techniques in situations where the singular points cannot be detected with high reliability. The core-100 configuration denotes all samples with singular point detection reliability less than 100. The triangles technique performs better. The folding technique would discard these prints.

3.4 Transform Strength

For the folding technique, an attacker must overcome $\log(N C_m) + 8m$ possibilities ≈ 125 bits for a template with N minutiae of which only m need to be inverted (see [4]). For the triangles technique, $2^{24}! * (1-r/360) / HW$ possibilities must be overcome by a matcher able to tolerate r degrees of variation and an image size of height H and width W (see [8]). For typical values of variables m , N , r , H and W , the triangles technique is more resistant to a brute force attack. Intrinsicly, a fingerprint has a complexity of 70-80 bits [4]. Any cancelable scheme with at least this strength makes it useless to try anything other than a brute force attack in the minutia domain.

4. Conclusion

We have compared two techniques for generating cancelable fingerprint templates. The folding technique has, up to an order of magnitude, a more compact representation making it suitable for memory limited applications. It is backward compatible since it can be applied as a transformation step after the minutiae extraction. A disadvantage is that a high singular point reliability threshold must be set to obtain good performance results. This reduces the effective size of datasets and increases FTE and FTA rates. For

fingerprints without singular points, the technique will fail. The advantage of the triangles technique is higher accuracy. It performs better in situations where singular points cannot be detected reliably. It has superior transform strength enabling it to better resist brute force attacks. It is not backward compatible as it uses a new matching method.

References

- [1] N.K. Ratha, J.H. Cornell and R.M. Bolle, Enhancing Security and Privacy in Biometrics-based Authentication Systems, *IBM Systems Journal*, 40(3):614-634, 2001.
- [2] *NSF Workshop*, Biometrics Research Agenda, April/May 2003.
- [3] R. Ang, R. Safavi-Naini and L. McAven, Cancelable Key-based Fingerprint Templates, in *10th Australian Conference on Information Security and Privacy, ACISP 2005*, pp 242-252, Brisbane, Australia, July 2005.
- [4] N.K. Ratha, S. Chikkerur, J.H. Cornell and R.M. Bolle, Generating Cancelable Fingerprint Templates, in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):561-572, 2007.
- [5] F. Farooq, R. Bolle, T. Jea and N. Ratha, Registration Free Anonymous and Cancelable Fingerprint Recognition, in *IEEE Computer Society Workshop on Biometrics (CVPR '07)*, IEEE 2007.
- [6] U. Uludag, S. Pankanti and A.K. Jain, Fuzzy Vault for Fingerprints, in *AVBPA 2005*, pp 310-319, 2005.
- [7] K. Nilsson, Symmetry Filters Applied to Fingerprints, *PhD Thesis*, Chalmers University of Technology, Sweden, 2005.
- [8] F. Farooq, N. Ratha, T. Jea and R. Bolle, Security and Accuracy Trade-off in Anonymous Fingerprint Recognition, in proceedings of *Biometrics: Theory, Applications and Systems*, (BTAS '07), Sep 2007.