Using Support Vector Machines to Eliminate False Minutiae Matches during Fingerprint Verification

Praveer Mansukhani, Sergey Tulyakov, Venu Govindaraju
Center for Unified Biometrics and Sensors (CUBS)
University at Buffalo,
Amherst, NY 14228.
{pdm5, tulyakov, govind}@buffalo.edu

Abstract

To compensate for the different orientations of two fingerprint images, matching systems use a reference point and a set of transformation parameters. Fingerprint minutiae are compared on their positions relative to the reference points, using a set of thresholds for the various matching features. However a pair of minutiae might have similar values for some of the features compensated by dissimilar values for others; this tradeoff cannot be modeled by arbitrary thresholds, and might lead to a number of false matches. Instead given a list of potential correspondences of minutiae points, we could use a static classifier, such as a support vector machine (SVM) to eliminate some of the false matches. A 2-class model is built using sets of minutiae correspondences from fingerprint pairs known to belong to the same and different users. For a test pair of fingerprints, a similar set of minutiae correspondences is extracted and given to the recognizer, using only those classified as genuine matches to calculate the similarity score, and thus, the matching result. We have built recognizers using different combinations of fingerprint features and have tested them against the FVC 2002 database. Using this recognizer reduces the number of false minutiae matches by 19%, while only 5% of the minutiae pairs corresponding to fingerprints of the same user are rejected. We study the effect of such a reduction on the final error rate, using different scoring schemes.

1. Introduction

Fingerprint images are one of the most commonly used biometric for verifying the claimed identity of a user. During an enrollment phase, done beforehand, the fingerprint image of a user is acquired, either using an ink-based impression taken on a paper, or by using an electronic sensor. In either case, the fingerprint is stored in the system, along with some identification (username or any other uniquely assigned code). However it is not the acquired image of the fingerprint stored in the system, rather a concise representation of the print is used, also known as a fingerprint template. The most commonly used representation for storage of fingerprint images is a list of the minutiae points [1]; these are the points of irregularity in the fingerprint ridges, and there are usually 30-50 of them present per fingerprint. During the verification phase, a template containing minutiae point information for the test fingerprint is similarly generated, and is compared with the user's stored template to arrive at a result.

As minutiae points are stored in terms of their position and orientation in the fingerprint image, minutiae based matching systems require a reference point for matching, enabling the system to map points from one template onto the other, using the calculated translation and rotation parameters. However, matching done in this manner is heuristic

[6], using a set of arbitrarily defined thresholds on the various comparison parameters used.

There needs to be an analysis of the feature correspondences between matched minutiae belonging to templates of the same fingerprint to be able to accurately distinguish between genuine and false matches. This could also help us eliminate minutiae features, which contain little or no information, reducing confusion while matching. In our work, we demonstrate, how using a suitable trained classifier, we can statistically capture differences between real and false minutiae matches, and classify them with greater accuracy, significantly reducing the number of false minutiae correspondences for an pair of fingerprint images. In contrast to existing approaches[6],[7], which use local minutiae information to obtain a global transformation, we also use minutiae correspondence information as a post-processing step to verify the results of the global match.

The arrangement of this paper is as follows: in the next section discuss fingerprint matching, and how the classifier can be used to eliminate false matches. Section 3 describes some of the experiments we have performed to validate our assertion, and results are discussed in detail. Finally we talk about some of the improvements and further enhancements that could be made, and also summarize the whole work in section 4.

2. Development of a SVM-based Fingerprint Matching System

2.1 Two stage minutiae- based fingerprint Recognition

Consider a two stage local-global matching system as in [5]. In the first stage, two minutiae points from one template are compared with different pairs of points from the other template. All these results are then consolidated to arrive at a single best transformation (translation and rotation) with respect to a pivot point (usually a pair of corresponding minutiae points). In the second stage, each minutiae point is converted into coordinates with respect to the pivot, and difference in distance and orientation between two points from different fingerprints is used to arrive at a matching score for that pair of points. A scoring algorithm combines these individual scores, along with global information such as the number of extracted minutiae points, and the surface area of the matched regions and the original templates to arrive at a final score.

2.2 Training the SVM

For training (Figure 1) the SVM we need a large corpus of matching pairs of minutiae points, both from fingerprint pairs belonging to the same and to different users. We take a pair of fingerprint templates, perform the local-global matching as described before, and get a list of matched minutiae points. For each pair, a feature vector is extracted, which contains distance and orientation information about the matching pairs as well as data about neighboring points. This is then stored with the appropriate class information.

Once all pair information has been extracted, the SVM is trained to produce a model file. Various values of parameters such as γ might be used to arrive at the optimum set of hyperplanes and cross-validation techniques are used to determine the effectiveness of various model. The final model file is stored for use in the matching stage.

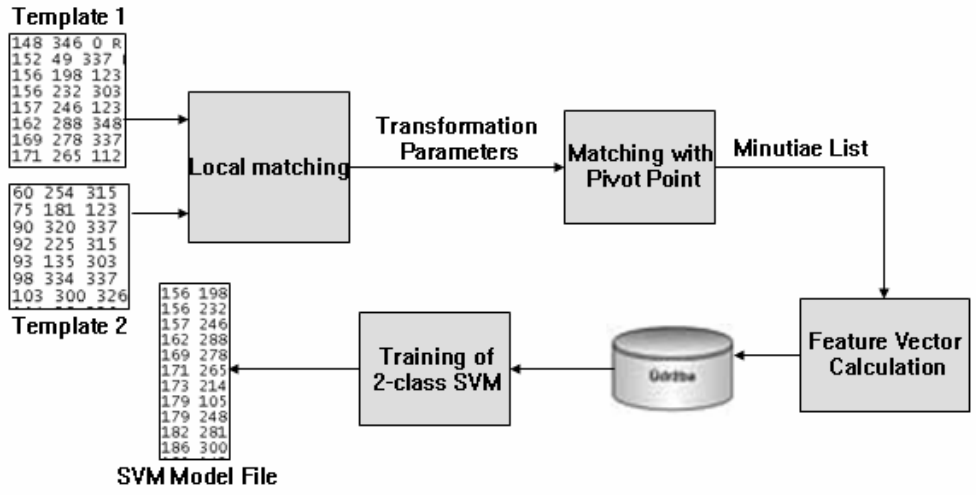

Fig 1: Training a 2-class SVM with lists of matching minutiae extracted from various fingerprint template pairs.

2.3 Pruning the matching list during fingerprint matching

As in the training phase, here we give a pair of fingerprint templates to the system (Figure 2). Two stage matching gives us the list of matched minutiae, and the feature vector is calculated for each matched pair. The SVM, along with the trained model file (obtained during the training phase) are used to classify each matched pair (on the basis of the extracted feature vector) as belonging to the same user (i.e. correctly matched) or belonging to different users (i.e. incorrectly matched).

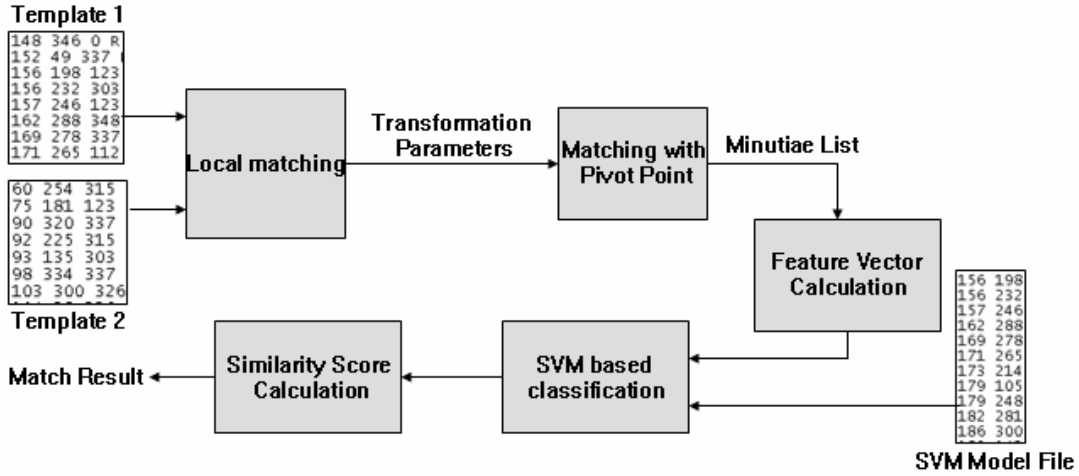

Fig 2: The list of matched minutiae (and corresponding feature vectors) and the trained model is given to the SVM. Only those pairs belonging to the same user are used for similarity score calculation.

It might have been noted that the original matching system produces a matching score for each pair of matched minutiae, which are then consolidated to arrive at the final result. Here, the score information is updated by eliminating information corresponding to the incorrectly matched pairs, and an updated score is obtained.

3. Experimental Results

3.1 Description of Dataset

For our experiments we have used the Database 1 from the 2002 Fingerprint Verification Competition (FVC). [3]. DB1 consists of 100 different users, each having enrolled 8 prints from the same finger, a total of 800 fingerprints. The same minutiae extraction algorithm has been applied to each of the fingerprints, and the minutiae information has been stored in a file. We directly use this template information for our tests. The dataset has been divided into training and test fingerprints (50 users each).

For minutiae matches belonging to the matched fingerprints, we have matched all possible pairs of fingerprints from the same user(${}^{8}C_2$ pairs). This has been done for all 50 users in the training set , a total of 1400 comparisons, giving us a total of 31155 matched pairs. Features have been extracted from each of these pairs, during the matching process, and have been stored in a file. Then, we have matched a fingerprint from each user with the correspondingly numbered fingerprint from each other user, thus 9800 matches (8 * ${}^{50}C_2$) pairs have given us 22949 pairs of minutiae points. It might be noted that due to a smaller number of minutiae points matched while comparing prints belonging to different users, a larger number of pairs have been used, yet giving us a smaller number of minutiae pairs.

3.2 Training and Cross –Validation of the Classification Model

Number of features	Ratio of genuine to imposter points	Cross –validation accuracy
2	57 : 43	64 %
5	57 : 43	67.05%

Table 1: Cross Validation results for SVM

We have used libsvm (version 2.82), an implementation developed by Chang and Lin [4]. First, we perform cross validation on unscaled training data (we determined that scaling did not produce any significant increase in performance), to study the effects of various features on the performance of the system. Finally a 5-feature set is selected $\{d_{ij}/d_{IJ}$, d_{ik}/d_{IK}, d_{jk}/d_{JK}, $(\theta_{jik} - \theta_{JIK})$, $(\alpha_{ij} - \alpha_{IJ})$ $\}$ where i,j,k are the pivot point, matched minutia point and a randomly selected point from the matching list of the reference template and I,J,K are the corresponding points from the test template. d_{xy} represents the distance from point x to y , α_{xy} is the orientation of point x with respect to y, and θ_{xyz} is the angle formed by the 3 points keeping y as the center. We also generated a smaller model file using the feature set $\{ (d_{jk}/d_{JK}, (\theta_{jik} - \theta_{JIK})\}$, i.e. just using features unique to this particular combination of the matching minutia and the randomly selected point.

We performed five-fold cross validation keeping $\gamma = 0.1$ and tabulated our results (Table 1.)

3.3 Effect of Classification on Number of Points matched

	No. of Fingerprint Pairs Compared	Total Matched Point Pairs	Rejected Matched Points	Accepted Matches
Same User	1400	37705	1831	95.14%
Different User	1225	3991	722	81.91%

Table 2: Using SVM Classifier reduces number of false matches

Table 2 shows us the effect of using the classifier on a test dataset. We can see that applying the classifier reduces a significantly high number of false matches for minutiae pairs belonging to fingerprints of different users. Almost four times as many false minutiae are correctly rejected for every true match that is incorrectly discarded.

3.4 Effect on Error Rate

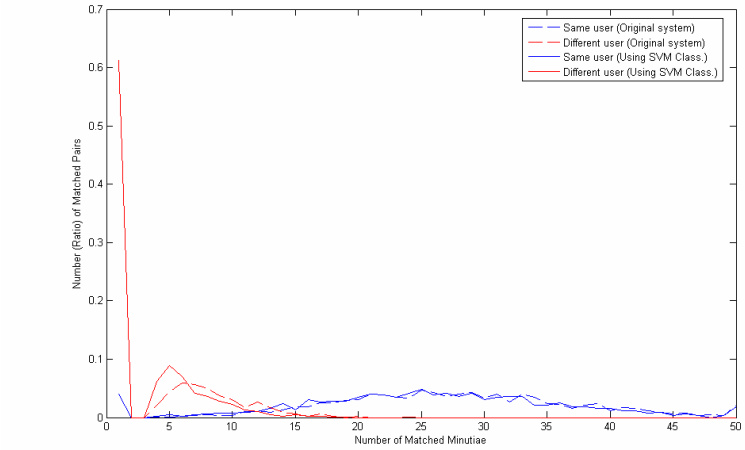

Fig 3: Distribution of number of matched minutiae pairs for original system, and using SVM

Using a scoring rate based on the number of minutiae points matched is the most intuitive method of evaluating a fingerprint matching system. Based on this technique, our method does show a slight improvement over the original system. Figure 3 shows the histrogram of the number of matched minutiae for same and different users, in the original and the SVM-based system, and a clear reduction on the number of minutiae points matched for prints belonging to different users can be seen. [5] has developed a scoring algorithm, which takes into account the area of overlap of the matched points, as well as the individual scores of the matched pairs. This additional information improves the performance of the system, to levels comparable with existing fingerprint verification systems. Using the same scoring technique, on our system, a slight decrease in accuracy is observed. (Table 3)

	Scoring using Minutiae Count		Score with Area, Individual Scores	
	Equal Error Rate (EER)	**Improvement**	**Equal Error Rate (EER)**	**Improvement**
Original System	7.59%	+0.31%	2.04%	-0.24%
Using SVM Classifier	7.28%		2.28%	

Table 3: Effect on EER of final system, using different score calculation techniques

4. Conclusions and Further Work

This work shows how applying a static classifier such as a Support Vector Machine can eliminate a significant number of falsely matched minutiae in a fingerprint verification system. By treating it as a 2-class classification problem, we have been able to explore different feature sets and generate the corresponding model. Our system does show a slight improvement in the error rate, and is able to reject a large number of falsely matched points; a further analysis and modification to the scoring algorithm should produce better system accuracy. Moreover the classifier could also be used to study the effectiveness of different minutiae features and develop a feature set most suitable for matching on particular fingerprint dataset.

Our system does not incorporate any of the classification confidences into the score calculation, rather it just uses the final class information. Further study of the scoring used, and developing a new scoring technique could allow us to improve the performance of the system. We could also generate multiple feature sets per matched minutiae point (using multiple neighboring minutiae selected at random) and depending on the total classification result, we could classify that point as a correct or incorrect match.

References

1. American National Standard for Information Systems, Data Format for the Interchange of Fingerprint Information, Doc # ANSI/NIST-CSL 1-1993. ANSI, New York, 1993
2. C. Cortes, V. Vapnik. “Support Vector Network”, Machine Learning, vol. 20 1995.
3. 2nd International Fingerprint Verification Competition (FVC) 2002 – http://bias.csr.unibo.it/fvc2002
4. C. Chang, C. Lin. “LIBSVM: A Library for Support Vector Machines” http://www.csie.ntu.edu.tw/~cjlin/libsvm
5. Tsa-Yang Jea. “Minutiae –based Partial Fingerprint Recognition” PhD Thesis, University at Buffalo, 2005
6. Xudong Jiang; Wei-Yun Yau, "Fingerprint minutiae matching based on the local and global structures," Pattern Recognition, 2000. Proceedings. 15th International Conference on, vol.2, no.pp.1038-1041 vol.2, 2000
7. Ratha, N.K.; Bolle, R.M.; Pandit, V.D.; Vaish, V., "Robust fingerprint authentication using local structural similarity ," Applications of Computer Vision, 2000, Fifth IEEE Workshop on. , vol., no.pp.29-34, 2000