NISTIR 6489

Distortion-tolerant Filter for Elastic-distorted Fingerprint Matching

C.I. Watson
P.J. Grother
D.P. Casasent [1]

[1] Carnegie Mellon University

U.S. DEPARTMENT OF COMMERCE
Technology Administration
Information Technology Laboratory
Information Access and User
Interfaces Division
National Institute of Standards
and Technology
Gaithersburg, MD 20899

NIST
National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

NISTIR 6489

Distortion-tolerant Filter for Elastic-distorted Fingerprint Matching

C.I. Watson
P.J. Grother
D.P. Casasent [1]

[1] Carnegie Mellon University

U.S. DEPARTMENT OF COMMERCE
Technology Administration
Information Technology Laboratory
Information Access and User
Interfaces Division
National Institute of Standards
and Technology
Gaithersburg, MD 20899

March 29, 2000

U.S. DEPARTMENT OF COMMERCE
William M. Daley, Secretary

TECHNOLOGY ADMINISTRATION
Dr. Cheryl L. Shavers, Under Secretary
of Commerce for Technology

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Raymond G. Kammer, Director

Distortion-tolerant filter for elastic-distorted fingerprint matching

C.I. Watson[a], P.J. Grother[a], D.P. Casasent[b]

[a]National Institute of Standards and Technology
Mail Stop 8940
Gaithersburg, MD 20899
Phone: (301) 975-4402
cwatson@nist.gov

[b]Carnegie Mellon University

ABSTRACT

This paper gives results for using distortion tolerant filters to improve performance of fingerprint correlation matching. Three types of distortion tolerant filters were tested: summation, weighted, and MINACE. A set of 55 fingers were used from NIST Special Database 24 to evaluate the filters. Our results show performance was improved from 49 % correct, using one training fingerprint, to 100 % correct, using multiple training fingerprints and a distortion-tolerant MINACE filter, with no false alarms.

Keywords: Distortion-tolerant filter, elastic distortion, fingerprint, MINACE, NIST Special Database 24

1. INTRODUCTION

Fingerprint matching has long been used in criminal applications, and its uses in security applications for verifying a person's identity may become more popular in the future. There are commercial applications allowing people to use their fingerprint to log on to their computer and there has been discussion about using a fingerprint as identification in commerce applications. Most current applications rely on minutiae based matching, which uses identifiable ridge endings and bifurcations to match fingerprints. We will explore the use of correlation to do fingerprint matching as it has direct applications in optical computing which could lead to significantly faster fingerprint matching techniques. The tests we are performing show that fingerprint correlation can work with fingerprint data as well as and possibly better in some applications than minutiae matchers.

Previous work has shown that one-to-one correlation of fingerprints on a large set of data has yielded poor results for fingerprint matching [2]. This occurs because of the elastic distortions between two fingerprints of the same finger. These can be significant enough that correlation cannot recognize elastic-distorted versions of the same fingerprint and cannot discriminate between a matching fingerprint and a non-matching fingerprint of the same class. Figure 1a-c show the significance of elastic distortions and the differences they produce in versions of the same fingerprint. Figures 1a and 1b show two versions of the same fingerprint. Figure 1c has corresponding minutiae from 1a and 1b, marked with black and white '+' symbols. The distortions present in figure 1 are a result of changes in pressure when a person dabs their finger on the scanning surface of the fingerprint reader.

This paper shows results for using distortion-tolerant filters, which use multiple elastic distorted images of a fingerprint to build a composite filter of the finger, to significantly improve the performance of fingerprint correlation matching. Data used for testing came from NIST Special Database 24 (SD 24) [1]. Data for 55 fingers was used from SD 24 to create and test the distortion tolerant filters. The results show an improvement from 49%, for one training fingerprint, to 100% recognition, for a distortion tolerant filter, with no false alarms. These initial results compare favorably to our evaluation of minutiae based matchers set to an error rate of 0.1%. While the minutia matcher had a small error rate, it also had a false negative rate around 15%. A false negative occurs when a fingerprint that should have been accepted is rejected. The minutiae matcher is a better one-to-one fingerprint matcher, but correlation with distortion tolerant filters has the potential to do better overall.

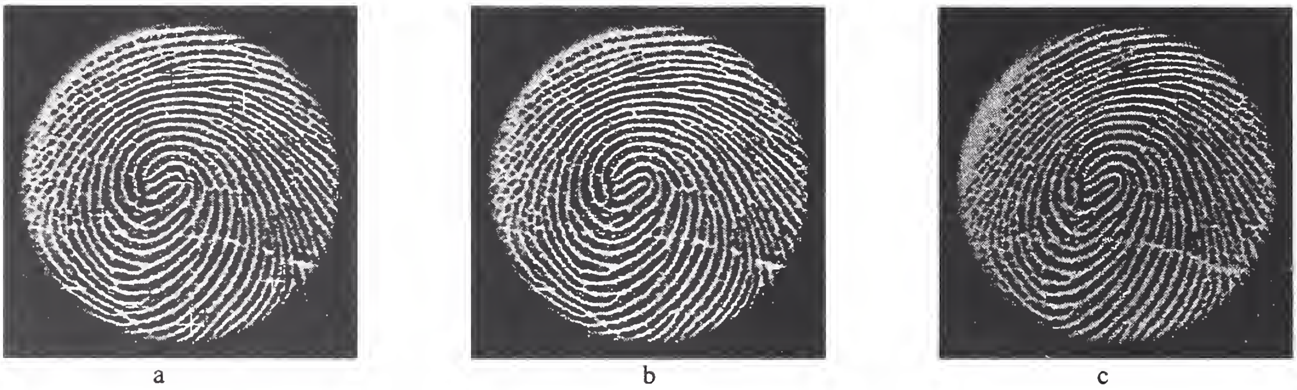

Figure 1: Minutiae points marked on two versions of the same fingerprint.

2. DATABASE

Many current databases contain only two variations of each fingerprint [3,4]. They were designed to test one-to-one fingerprint matching. Use of modern fingerprint readers makes it fast and easy to capture several dabs of each finger. The fingerprint data for this paper was taken from NIST Special Database 24, a live-scan digital video fingerprint database and extra data not published in the database release; a total of 200 test samples were available. The database contains two 10 second captures of 200 fingerprints from a live-scan fingerprint reader. The first 10 seconds of data had individuals making changes in pressure to create elastic distortions. This data was not used for results in this paper. The second 10 seconds captured had each individual "dab" their finger through a set of angles to capture a set of rotated fingerprint data. The fingerprint data used in this paper was taken from the second 10 seconds of data captured as it simulated the dabbing of the finger onto the scanner surface without the extra "smearing" present in the first 10 seconds of data. The data contained equal samples from all ten fingers and was split between male and female fingers.

The image size was 420X480 pixels, but many fingerprints did not fill the full image area, leaving white areas in the background. These white areas will contribute to the correlation peak value so they were set to 0 (black) as described in section 2.1. The current distortion-tolerant filter was designed to compensate for elastic distortions in the fingerprint but the fingerprint data from NIST Special Database 24 contained rotation. The rotations were removed using the procedure described in section 2.2.

2.1 Background

The white background areas were removed with some simple digital image processing procedures [5]. The fingerprint area was detected by making the image binary (threshold of 180), dilating/eroding (3x3 window) making the fingerprint ridge area a "blob", then using the foreground blob to mark the background. The edges of the applied background were smoothed to reduce the sharp cutoff transition from the background to the fingerprint ridge area. Figure 2a shows an original image and figure 2b shows the image with the background set to zero.

2.2 Rotation

The rotations were removed in two steps. First a coarse alignment was done by hand marking two minutiae points on each image. The first point was the fingerprint core and the second was a minutia point within roughly 50 pixels from the core. All the core points were aligned to the image center and then the images were rotated so that a line draw between the core point and the marked minutia were aligned to the same angle. All digital rotations were done using bilinear interpolation. This gave a coarse alignment of the fingerprint images. We expect the digital rotations, even using bilinear interpolation to provide poor accuracy. This is quantified by digitally rotating a fingerprint by θ degrees and then rotating it back using bilinear interpolation for both rotations. This digital rotation caused a 7.5% decrease in the correlation peak value. The decrease appeared independent of the angle θ being used in this experiment, so we just accept that all correlation outputs will have the same decrease.

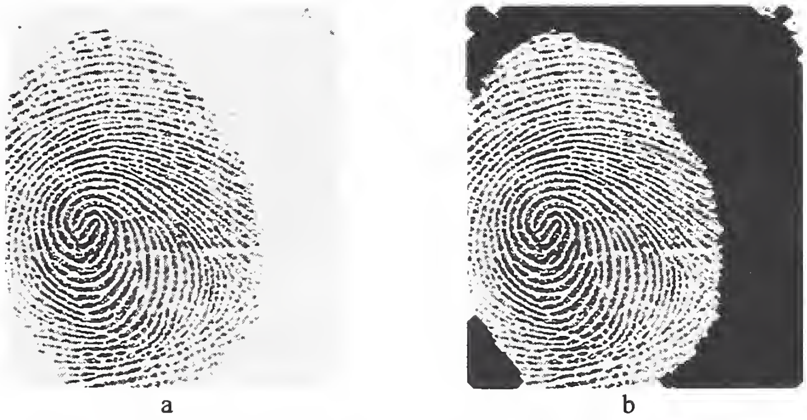

Figure 2: Background detection applied to fingerprint.

After the coarse alignment, a circular window was applied to the image highlighting the most useful information around the core of the fingerprint. The edge of the circular window uses a gaussian roll-off to smooth the transition into the fingerprint area and help reduce artifacts in the Fourier domain.

The problem with the coarse alignment is that elastic distortions could distort the second minutiae point location enough to disrupt the rotation alignment. An improvement to this problem was to use correlation to rotationally align the fingerprints. This "fine" alignment was done using one fingerprint in the set as the "base" fingerprint. The other fingerprints were rotated to +/- 5 degrees, from the coarse aligned angle, in degree steps around the core. At each step the fingerprint was correlated with the "base" fingerprint and the angle resulting in the largest correlation was selected as the "fine" alignment angle. The angles from the coarse and fine alignments were combined and the original fingerprint data was rotated one time into its aligned position. This was done to reduce the effects caused by using digital rotations with bilinear interpolation and limit the drop in correlation peak value to the anticipated 7.5%. Figures 3a and 3b show the fingerprint from figure 2b after removing rotation and with the circular window and cropping.

2.3 Training and Testing Data

The choice to only use 55 fingers from SD 24 was based on the number of useful input training fingerprints available for each finger. Initial testing indicated that about 8 or more fingerprints were needed to make a useful distortion tolerant filter. After removing background and rotations, the images were cropped to 350X350 pixels, the size of the applied circular window applied in section 2.2. For this set of 55 fingers, one image of each finger was set aside for the testing set and the remaining images were used as the "training" set to build the distortion tolerant filters. All the fingerprint data used for training and testing were normalized, by dividing each image pixel by the image rms value.

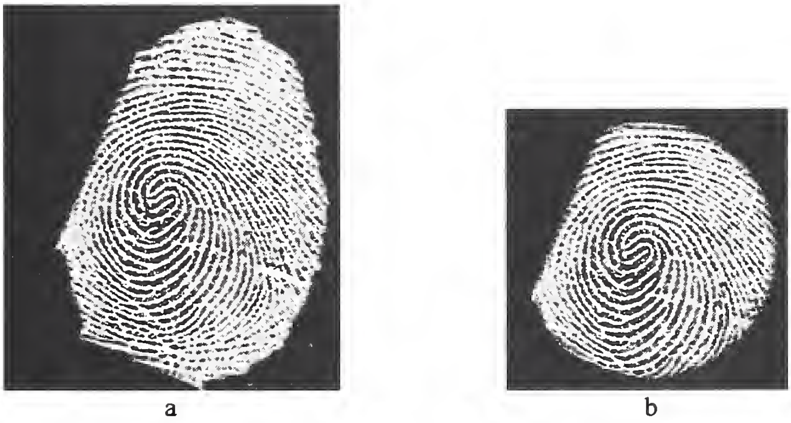

Figure 3: Rotation and circular window applied to fingerprint.

3. DISTORTION FILTER DESIGN

The idea to use a composite distortion tolerant filter resulted from previous work with optical fingerprint correlation [6]. Using a Vanderlugt correlator setup, we were unable to get discrimination among a test set of fingerprints when doing direct one-to-one correlation. A simple summation composite filter was created on a thermal plastic recording material, that used ten seconds of live video input from a fingerprint scanner to record elastic distortions of the fingerprint. Using this very simple technique the optical correlator was able to discriminate between matching test prints and a non-matching test prints. We decided to test more complex distortion tolerant filters to see if further improvements in performance were possible. All of the work on more complex filters was done digitally.

Three distortion tolerant filters are compared in this paper: summation, weighted, and MINACE. All of the distortion tolerant filter designs were sensitive to translation in the input training images. Filters formed with aligned data were expected to do better, since they had more common information in a smaller region of support and require fewer images in the filter. Since the core points were marked by hand (section 2), they were only approximate, and thus a more detailed alignment was needed. The alignment was done using correlation. A nice feature of correlation is that it is shift-invariant. The training set images were all shifted with respect to one of the images in the training set until their maximum correlation peak was centered in the correlation plane. This was the final alignment of the training data before using it in filter synthesis.

3.1 Summation Filter

The summation filter was very easy to implement. All training images were Fourier transformed and summed into a single composite filter and the final filter values divided by the total number of training images.

In order for the summation filter to work correctly, each training image was high pass filtered to remove DC and low frequency information. The higher frequency information left contains the important ridge structure information that was useful in discrimination between fingerprints. The suppression of low frequency information improved false correlation rejection while maintaining recognition of true correlation outputs. A high pass filter was designed using a small sample of test images. The test set contained several fingerprints that were true matches to the filters and several false fingerprints but from the same class as the filter's, since they are assumed to be most similar. The size, R, of the suppressed low frequency region was selected to give the largest difference between the smallest true correlation and the largest false correlation. Above a certain value, R, the higher frequencies are suppressed leaving no useful information. Figure 4 shows the high pass filter that was used, where R = 30 (shown in pixels) and all frequencies below 0.2π were blocked.

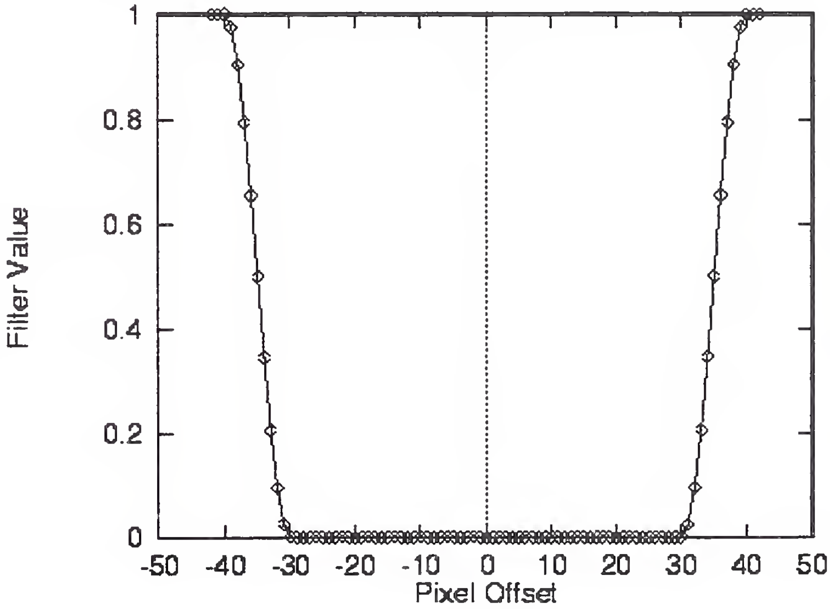

Figure 4: High-Pass filter used for summation and weighted filters.

3.2 Weighted Filter

A problem with the summation filter was that all the training images were weighted equally. If one of the training fingerprints contained useful information that others did not, its effect was reduced. The next filter applied different weights for each training image, depending upon the similarity of the different training images. This allowed each training fingerprint to contribute to the final distortion tolerant filter as needed. The weights were elements of the $\underline{\mathbf{w}}$ vector and chosen to satisfy $\underline{\mathbf{w}} = \underline{\mathbf{V}}^{-1}\underline{\mathbf{u}}$, where $\underline{\mathbf{V}}$ was the vector inner product matrix and $\underline{\mathbf{u}}$ was set to all 1's. So the filter is designed to provide correlation peak values of 1.0 for all training images in the filter.

3.3 MINACE Filter

The MINACE filter [7,8] is a more advanced distortion tolerant filter and by design suppresses the low frequency information, which has more energy than the higher frequencies. The filter was designed in the frequency domain as a vector $\underline{\mathbf{H}}$, with the constraint that correlation peak values for training images included in the filter were 1.0. The synthesis of the filter was done using the formula $\underline{\mathbf{H}} = \underline{T}^{1}\underline{X}(\underline{X}^{+}\underline{T}^{1}\underline{X})^{-1}\underline{\mathbf{u}}$. Matrix $\underline{X}$ was the data matrix of the training image Fourier Transforms. Vector $\underline{\mathbf{u}}$ specifies the correlation peak values for the training images, all 1.0. $\underline{T}$ is a diagonal matrix containing the maximum energy over the training set at each frequency, with a constraint based on the energy at DC. So $\underline{T}$ = max[$\underline{S}_1$(u,v), $\underline{S}_2$(u,v), …, $\underline{S}_n$(u,v), N], where $\underline{S}$(u,v) = $|\mathbf{FT}|^2$ for each training image, N = **c** x max[$\underline{S}_n$(0,0)], and **n** is the number of training images used in the filter. The **c** parameter was selected by the user and set to give the optimal performance.

A **c** value was selected using the same sample of data used to select R in the summation filter. The **c** parameter was varied over a range of acceptable values (0.0-1.0) and the final value (0.00005) was selected to give the maximum difference between the smallest true test print correlation value and the largest false test print correlation value. This **c** value was tuned to work with filters that had 8 or more fingerprints in the training set. If less fingerprints are present per finger, **c** may need to be increased so the filter can better recognize a matching test print. The trade off might be more false alarms. In the present tests, the same **c** value was used for all the filters. The best results, for a training set with varying numbers of training fingerprints, should be obtained by varying the **c** value during filter creation based on the number of training fingerprints available per finger.

4. RESULTS

For our initial testing, we selected all the fingerprints from SD 24 that had 8 or more fingerprints in the training set after doing the pre-processing in section 2. This gave a set of 55 fingers for testing. This set of 55 fingers was used to test each of the three types of distortion tolerant filters. For each filter type 55 filters were made, one per finger. A test was also run using only one of the training prints and doing a one-to-one correlation with the test fingerprints, to compare versus the distortion tolerant filters. In the one-to-one correlation test, low frequency information was suppressed as described in section 3.1.

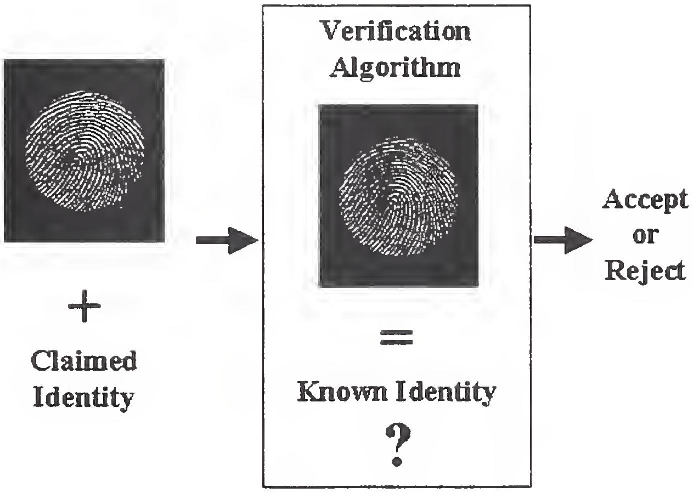

Figure 5: Block diagram of verification.

Scoring results are shown for verification and identification. For verification (see figure 5), all 55 test fingerprints are compared against each filter and any result above a certain threshold is accepted. Ideally, only the matching test fingerprint will exceed the threshold. Any non-matching test fingerprints exceeding the threshold are false alarms. In a verification application, if an input is incorrectly rejected the user would have to redo the input process to be accepted. In our tests, only one matching test fingerprint is used and it is either accepted or rejected. A useful future test may allow for several test inputs to see if the filter is able to recognize some majority of the fingerprints, providing a measure of its reliability. In identification (see figure 6), a test fingerprint is compared against all the filters and the filter with the largest output correlation is identified as the match, if the output is above a given threshold. If no output exceeds the threshold, the print doesn't match any currently in the filter bank.

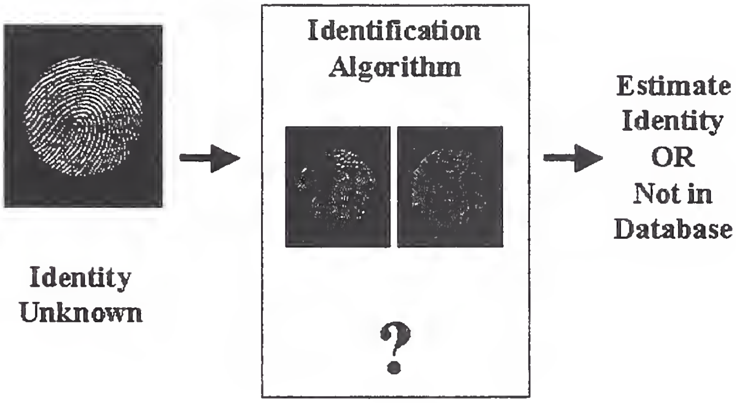

Figure 6: Block diagram of identification.

The first test performed was to verify that rms normalizing the data and doing the fine alignment was necessary to give the best results. Figures 7a-c show verification results for the three filters for the various combinations of coarse (cor) or fine (fin) alignment and raw (unrm) or normalized (nrm) data. In all three cases, as expected, the fine alignment and normalized data gave the best results.

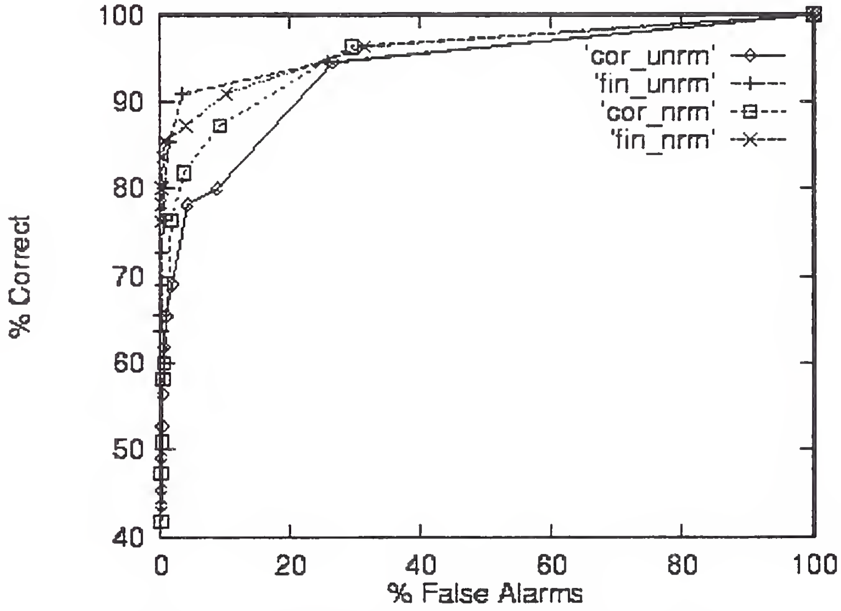

Figure 7a: Summation filter verification results for data combinations.

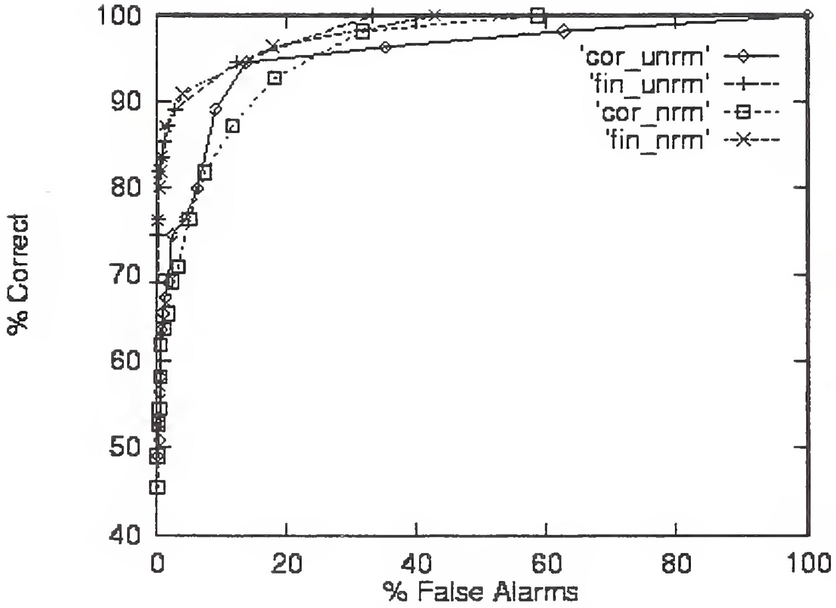

Figure 7b: Weighted filter verification results for data combinations.

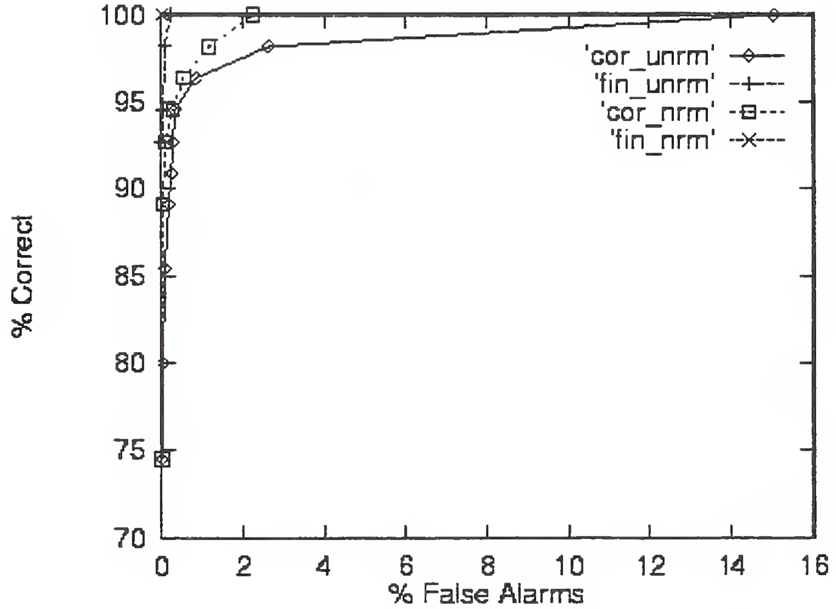

Figure 7c: MINACE filter verification results for data combinations.

Figures 8a-b show the verification and identification results of the three filters using normalized and fine aligned data on the same plot, along with the one-to-one correlation results. In both cases the MINACE filter was able to correctly match all 55 fingerprints without any false alarms.

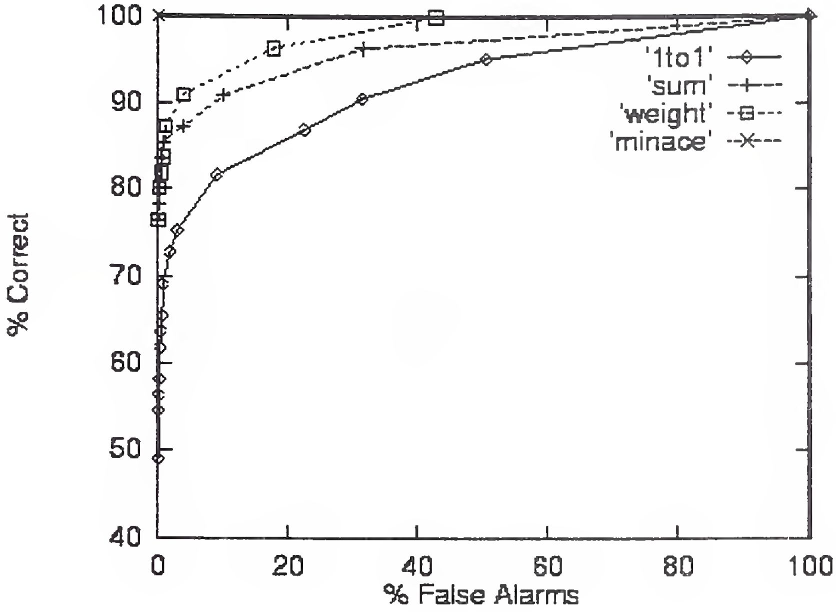

Figure 8a: Verification results for the three filters and one-to-one correlation.

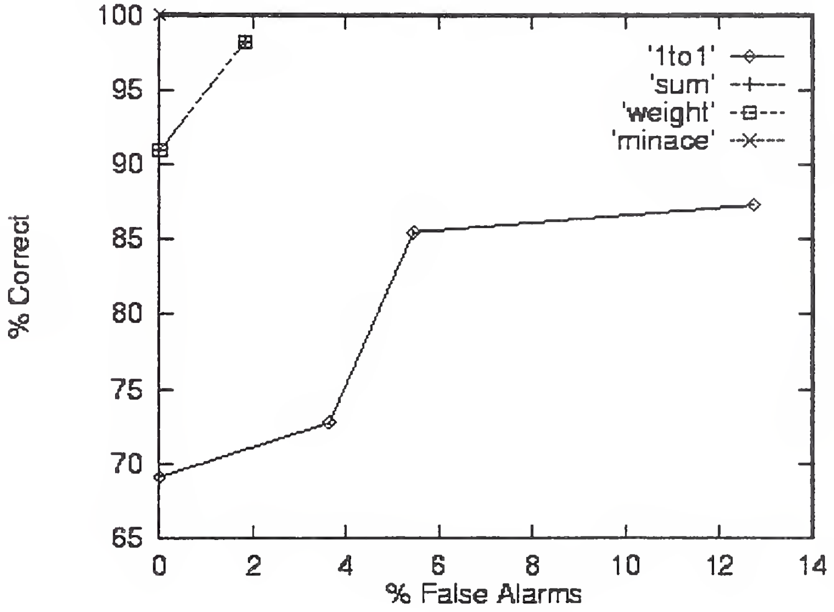

Figure 8b: Identification results for the three filters and one-to-one correlation.

The final test performed was only done with the MINACE filter over the entire set of 200 fingers available in SD 24. The available training fingerprints ranged from 3-7 for the additional 145 fingers. Figure 9 shows that with less training data available to the distortion tolerant filter, there is a significant decline in performance, but still better than one-to-one correlation. MINACE performance could be improved by tuning **c**, in filter synthesis, based on the number of training fingerprints available.

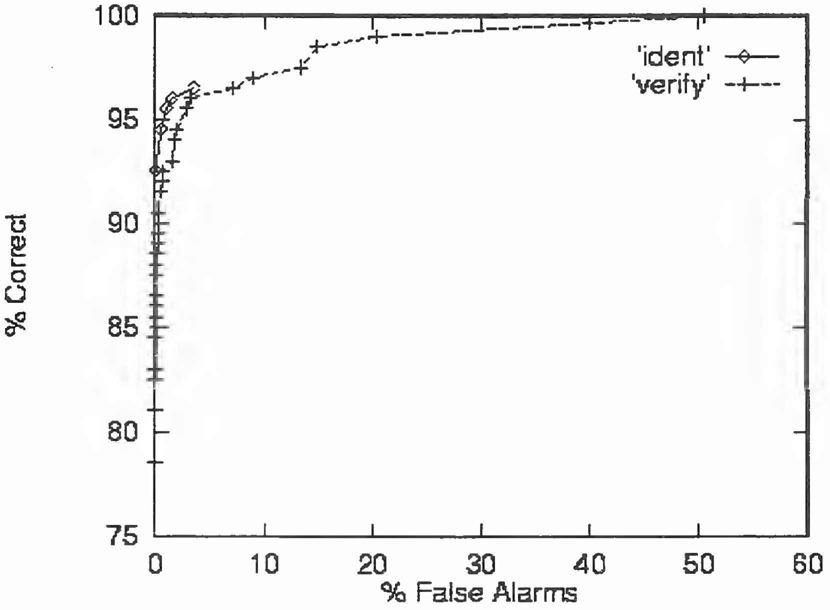

Figure 9: MINACE filter results using all 200 fingers in the data set.

The data in SD 24 was collected without any controls on how the person placed their finger on the scanning surface, other than making a dab at varied angles. Clearly, with the type of unconstrained data in SD 24, the MINACE filter needs at least 8 training fingerprints to make a useful distortion tolerant filter. If constraints were placed on the person inputting their finger, a direct one-to-one correlation may work, but most likely elastic distortions would still be large enough that a distortion tolerant filter (with a smaller "constrained" training set) should still perform better.

The MINACE results are comparable to testing on minutiae based matchers. The minutiae matcher has an error rate of 0.1% but had about 15% false negatives, which is rejecting a fingerprint that should have been accepted. The main problem with making a final comparison is that the current minutiae based matcher being used doesn't allow easy input of the data from SD 24. Software is being developed that will allow future tests of the two methods on the same fingerprint data and a more direct comparison can be made.

5. REFERENCES

1. C.I. Watson, "NIST Special Database 24- Live-scan Digital Video Fingerprint Database", July 1998.
2. C.L. Wilson, C.I. Watson, E.G. Paek, "Combined Optical and Neural Network Fingerprint Matching", *Optical Pattern Recognition VIII, SPIE Proceedings* Vol. 3073, p. 373-382, April 1997.
3. C.I. Watson, "NIST Special Database 4", March 1992.
4. C.I. Watson, "NIST Special Database 9", February 1993.
5. R.C. Gonzalez and P. Wintz, *Digital Image Processing*, 2nd edition, Addison-Wesley, 1987.
6. C.I. Watson, P.J. Grother, E.G. Paek, C.L. Wilson, "Composite Filter for Vanderlugt Correlator", *Optical Pattern Recognition X, SPIE Proceedings* Vol. 3715, p. 53-59, April 1999.
7. G. Ravichandran and D. Casasent, "Minimum Noise and Correlation Energy Optical Correlation Filter", *Applied Optics*, Vol. 31, p. 1823-1833, April 1992.
8. D. Casasent and S. Ashizawa, "Synthetic Aperture Radar Detection, Recognition and Clutter Rejection with new Minimum And Correlation Energy filters", Optical Engineering, Vol. 36, no. 10, p. 2729-2736, October 1997.