

Using Weighted Minutiae for Fingerprint Identification

F.R. Johannesen, S. Raaschou, O.V. Larsen, P. Jürgensen

Laboratory of Image Analysis, Aalborg University, Denmark
email: ovl@vision.auc.dk

Abstract. This paper describes how a minutiae reliability measure can be defined and integrated in an automatic fingerprint identification system. The reliability measure denotes the quality of the minutiae and is used to weight the minutiae in the matching of two fingerprints. To strengthen the matching even further, relational information is used along with attribute information for describing a fingerprint. Experimental results strongly suggest that the use of weighted minutiae can improve the matching performance significantly.

1 Introduction

In criminal courts around the world fingerprints have for many years been used for person identification. The main reasons why fingerprints are well suited for reliable person identification are that a fingerprint is unique, not only for every person but also for each finger, it remains unchanged over a lifetime and is easy to acquire. Furthermore, fingerprints can be recorded at the scene after the crime has taken place.

Identification of an unknown fingerprint often involves comparison with a rather large number of known fingerprints. Basically, the automated fingerprint identification process consists of two different tasks - fingerprint recording and fingerprint matching. In the recording phase, the fingerprint to be identified is acquired. Then a matching with a number of known fingerprints from a database is performed to find the true match, if it is present in the database. To allow for unique identification, the matching must be based on the minutiae in the fingerprint.

In the fingerprint recording task the primary concern is to scan the fingerprint to obtain a digitized version of the fingerprint. In this work, prescanned, inked impressions from the National Institute of Standards and Technology have been used¹, and thus, the fingerprint recording task was not of further concern.

To obtain the minutiae required for the matching, the digital fingerprint images were initially processed. One of the main problems in matching is that false minutiae might occur in the digitized version of the print due to noise, either introduced during scanning or in the image processing prior to minutiae

¹ The set of fingerprint images was from the NIST Special Database 4 containing 2000 pairs of 512x512 fingerprint images.

extraction. Such false minutiae will have a negative influence on the matching performance and at worst cause the matching to fail. Due to the importance of avoiding false minutiae many fingerprint identification systems only use a limited subset of the available minutiae in the matching. The selection of the best minutiae is typically done manually. This selection process, however, constitute a major problem as some of the minutiae left out just might be the ones needed to make a match with the right print, e.g. obtained at a scene of a crime.

In technical terms the above problem is mainly due to the fact that all minutiae have been given the same importance in the matching. The authors of this paper believe that it is possible to accommodate for the above problem by retaining all minutiae, but attaching a weight to each one, telling how reliable it is. It is expected that false minutiae will be unreliable. This means that it is not necessary to discard uncertain minutiae and at the same time the matching would not be weakened as much if an uncertain minutiae turns out to be false. It is the working hypothesis that it is possible to define, calculate and integrate a minutiae reliability measure in a fingerprint identification system. It is furthermore hypothesized that a more reliable and faster matching is obtainable by using weighted minutiae.

To be able to verify the hypothesis, a fully automatic fingerprint system has been implemented. After a scanning, which is not necessary here, the image is pre-processed to extract the minutiae required for the matching. The minutiae are evaluated to find out how reliable they should be regarded and the features used for the matching are calculated for each minutiae. Based on the extracted features and the minutiae reliability, the unknown fingerprint is then matched to the fingerprints in the database and the best matches are output in a list ranked according to their matching score.

The paper will describe the system and document the experiments performed to verify the hypothesis.

2 Pre-processing

The purpose of the image pre-processing is to automatically detect the minutiae present in the fingerprint. Reliable detection of the minutiae is complicated by two main factors: 1) the original fingerprint images are gray-level images of varying quality and 2) the width of the ridges varies within each fingerprint and among different fingerprints. Therefore the minutiae extraction is based on binarized and thinned images.

Due to noise in the thinned image, primarily originating from noise in the original image, errors that can take shape as *minutiae* sometimes occur. Such errors are falsely detected as minutiae and should be removed. To aid the determination of the false minutiae, information about the border of the fingerprint is useful because many false minutiae, especially ridge endings, will be detected at the border of the fingerprint where the ridges end abruptly. In the fingerprint images, the gray-level variation of the fingerprint is much higher than the variation of the background. Based on this observation, the fingerprint was localized by

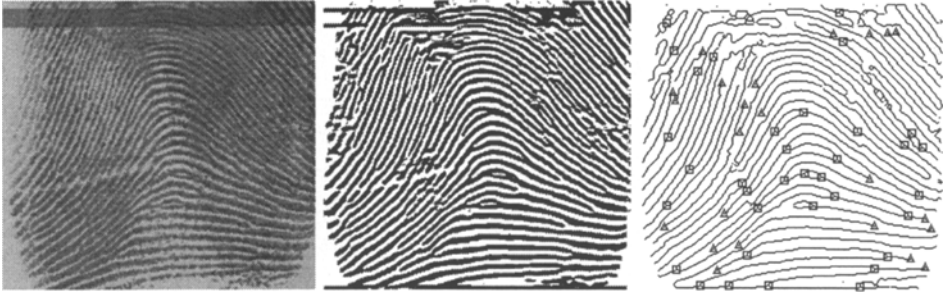


Fig. 1. (left) shows an example image from the database of fingerprints. (middle) is the binarized image, and (right) is the thinned and cleaned image. In (right) those of the detected minutiae that were accepted by the cleaning algorithm as being true are marked. The triangles mark ridge endings while squares mark bifurcations.

letting a pixel be part of the fingerprint if the gray-level variance in a 9×9 window centered at the pixel of interest was larger than some threshold. In noisy areas of the fingerprint, small inconsistencies in the localization sometimes occur due to the low variance of such areas. To remove these inconsistencies, a morphological closing operator was applied using a square 5×5 structuring element.

The original images used were of a varying quality with high contrast in some areas and very low contrast in other areas. Therefore, it was necessary to perform a contrast enhancement to allow for a reliable binarization. The contrast enhancement was based on the use of oriented filter kernels as suggested by O’Gorman [6]. The binarized image was thinned using an iterative algorithm [3]. From the thinned image two types of minutiae - ridge ending and bifurcations - were detected. The approach taken for removal of falsely detected minutiae was to use a combination of statistical and structural information about the minutiae in the fingerprint (see [8, 4]). Along with this, the information about the fingerprint border was used to identify and remove the false minutiae structures.

Figure 1 shows an original image, a binarized image and a thinned image after cleaning with polygons marking the accepted minutiae.

3 Minutia Reliability

The purpose of the minutiae reliability measure is to be able to map unreliable minutiae to a low reliability value and more reliable to a higher reliability value thus allowing for making a distinction between minutiae of different reliability.

To design the minutiae reliability measure, the fingerprint experts at the Danish police were asked to describe what characterizes the reliability of a minutiae and to mark and evaluate the minutiae in 10 fingerprints from the database used here. The minutiae were evaluated on a scale from 1 to 5, where 5 denoted a reliable minutiae while 1 was given to very unreliable minutiae. Along with this, the

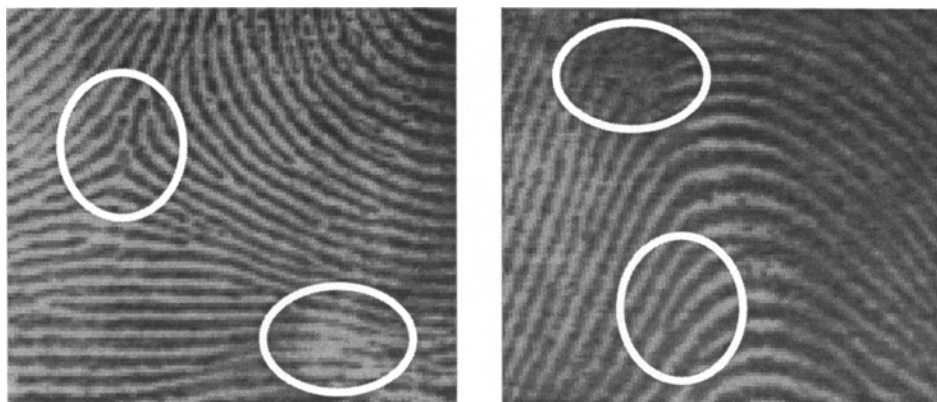


Fig. 2. The minutiae in the upper(left) and lower(right) marked areas are minutiae of rather high reliability, while minutiae in the lower(left) and upper(right) marked area have a much lower reliability.

methods used in the image pre-processing were investigated to find out how different factors influence the performance of each method. For example, the quality of the orientation estimate was found to be very dependent upon the contrast in the original image. In smudged areas the orientation estimate was sometimes erroneous thus causing the enhancement filtering and the binarization to fail. Therefore, false ridges will be introduced in such areas increasing the chance of detecting false or unreliable minutiae here. This implies that the intermediate results of the pre-processing also hold valuable information for describing the reliability of minutiae.

Based on the combined knowledge obtained from the police and the pre-processing, the reliability of a minutiae was primarily found to depend on i) its position in the fingerprint and ii) the local image quality.

In figure 2 minutiae of different reliability are marked in an enlarged area of a fingerprint. The dominant criterion for distinguishing the reliability of the minutiae marked in figure 2 is the local image quality. The minutiae with high reliability lie in areas of high contrast and are therefore considered very reliable. The minutiae with low reliability lie in smudge areas with low contrast.

The design of the minutiae reliability measure was primarily based on the information gained from the police. This means that a true minutiae can have one of five different reliability values. Since also false minutiae should be identified by the minutiae reliability measure, a sixth reliability value, 0, was defined. From the 10 fingerprint images from which the minutiae reliability measure was designed, false minutiae were defined as those minutiae accepted as true by the pre-processing that had not been marked by the police.

3.1 Minutiae Position

The reliability of a minutiae depends upon its position in the fingerprint in the sense that a reliable minutiae should neither be close to the fingerprint border nor to the core point.

The first information, *the distance to the border* [4], was readily available from the localization estimate calculated during the image pre-processing. By using the 3-4 chamfer transform described in [1], a distance image was created in which the gray-level at the minutiae position of interest corresponded directly to its distance to the fingerprint border. To acquire the second type of information regarding the distance to the core point, the fact that the core point is located at the point of maximum curvature was used. To avoid the difficult estimation of the position of the core point and calculating the distance to it, it was decided to base the measure on *the local curvature* [4], as reliable minutiae lie in areas with low curvature.

3.2 Image Quality

The local image quality is closely connected to the reliability of a minutiae. From the original image *the local gray-level variance* [4] was measured. The gray-level variance was used because the low contrast areas in which less reliable minutiae are detected will have a lower gray-level variance than high contrast areas. In addition to the information which is available from the original image, the image manipulations performed during the pre-processing can also provide useful information about the minutiae reliability.

The first type of information used from the pre-processing was *the certainty of the orientation estimate* [4]. This knowledge is useful due to the fact that in areas where the orientation estimate is uncertain, the enhancement filtering - and thus the binarization - is more likely to fail. The certainty of the orientation estimate could be obtained by calculating the variance of the output from the three measurement kernels, used for the orientation estimation, since a large variance indicates that no dominant orientation could be estimated.

As a second type of information from the pre-processing, *the gray-level values in the enhanced image* [4] were measured. The contrast enhanced image can provide useful information because areas of high contrast are characterized by higher gray-level values.

3.3 Minutiae Reliability Measure

The reliability measure should be designed in such a way that it supports a classification of the minutiae similar to the one done by the police for the 10 fingerprints. To obtain the desired measure, the five types of information were combined into one measure as a sum weighted in such a way that the overlap between minutiae of different reliability was minimized in a least squares sense. The approach taken for doing this was to minimize the variance of distribution defined for each of the six reliability groups:

$$\text{minimize}(\text{var}(X^0) + \dots + \text{var}(X^5)) \Leftrightarrow \text{minimize}\left(\sum_{i=0}^5 \frac{1}{n_i} \sum_m (X_m^i - \mu_i)^2\right)$$

where X_m^i is the m th value of the stochastic variable representing the group of minutiae with reliability value i , n_i is the number of minutiae in the i th group and μ_i denotes the mean value. Due to the normalization factor, n_i , each group will contribute equally to the minutiae reliability measure. This is not desirable as the number of minutiae in some groups is considerably larger than the number of minutiae in other groups. Therefore, the minimization is performed without the use of the normalization factors.

Each value of X_i will be a weighted sum of the five measures described above. Letting x_i be a sample from X_i , this can be written as $x_i = m_1 h_1 + m_2 h_2 + \dots$ where m_i denotes the output of the i th measure and h_i is the corresponding weight that needs to be found. If all the sample measures for each group are gathered in one matrix, \mathbf{X} , and the weight in the vector \mathbf{h} , the equation and its solution can be written as:

$$\text{minimize}\left(\sum_i (\mathbf{X} \cdot \mathbf{h} - \mathbf{c})^2\right) \Leftrightarrow \mathbf{h} = (\mathbf{X}^T \mathbf{X})^{-1} \mathbf{X}^T \mathbf{c}$$

where \mathbf{c} is a vector containing the mean values for the six reliability groups.

To visualize the separation between the minutiae of different reliability provided by the combined minutiae reliability measure, a 3D histogram and a contour map is shown in figure 3. As it can be seen, especially from the contour plot, minutiae with a high value from our combined minutiae reliability measure are also those minutiae that were marked with a reliability value of 5 by the police. Similarly, the minutiae with the lowest value are primarily those that were interpreted as false (i.e. those not marked by the police). There are, however, some problems in connection with the separation of minutiae that were not marked as either very reliable (5) or false (0).

4 Representation

To allow for describing a fingerprint uniquely, the feature information used should be minutiae based. The fingerprint representation was based on the combined use of features characterizing minutiae individually, called attributes, and features describing a minutiae relative to other minutiae, called relations. The relative minutiae information was used because it allows for storing contextual information in the fingerprint description. In noisy regions of a fingerprint the use of contextual information is especially valuable because it can provide useful information about a minutiae, even if it lies in an area in which no descriptive information can be gained locally. The use of contextual information formulated as relations has not been encountered in previous approaches to fingerprint identification.

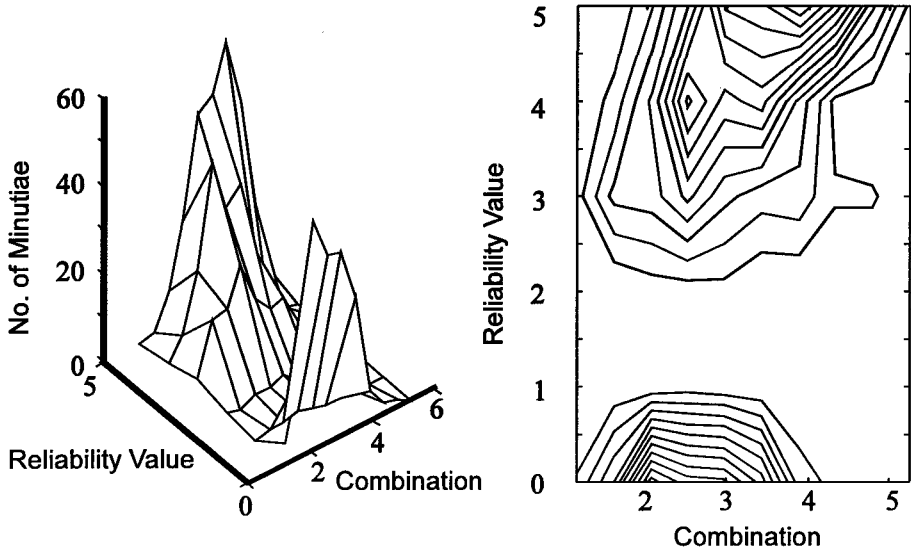


Fig. 3. The plot to the left is a 3D histogram showing the dependency between the values calculated by the combined minutiae reliability measure and the reliability values given by the police. The plot to the right is a contour plot based on the same data.

A total of four features was used. Of these two were attributes, the minutiae type and the minutiae curvature, and two were relations, the distance to other minutiae and the minutiae orientation difference. The minutiae type is a discrete, symbolic feature that can take on two different values: ridge ending and bifurcation.

The minutiae curvature is a continuous feature. This feature can be used for obtaining information about the minutiae position, due to the typical ridge flow in a fingerprint.

The distance to other minutiae is a binary relation. Its extraction involves calculation of the distance from the minutiae of interest to all other minutiae in the fingerprint. As the distance measure the Euclidean distance was used, thus implying that the feature is continuous.

The minutiae orientation difference is also a binary relation and it is based on measuring the orientation difference between any two minutiae. The minutiae orientation difference is a continuous feature.

In the data used in this paper only two impressions of each finger were available, and therefore it was not possible to test the robustness of the features by analyzing the feature values in a large series of the same minutiae. Instead 435 pairs of corresponding minutiae were pointed out manually, and the difference between the feature values was found. To be able to compare the 435 attribute differences and 6173 relation differences, they were analyzed relative to the average of the feature values. The evaluation showed that especially the two relations were very robust [4].

5 Matching

The matching in fingerprint identification has two parts: The fingerprint to be identified has to be matched to a fingerprint in the database (hereafter called the unit and label fingerprint, respectively) to find the best possible match between the two. When the best match between these two fingerprints is found, the goodness of the match, i.e. the matching score, must be evaluated and compared to similar matches with all the other fingerprints in the database. The result of the comparison is a ranked list of possible matches.

The matching of the two fingerprints is based on a tree search guided by an evaluation function. Since all fingerprints contain a large number of minutiae a fully expanded search will be very comprehensive. Therefore the evaluation function is calculated every time a label is assigned to a unit (i.e. a minutiae in the label and unit fingerprint) and if an assignment is found to be non valid the search backtracks. This happens very often due to the very discriminant relations used in the fingerprint representation, and therefore only a small part of the tree is expanded. Since the matching in this approach is inexact, wild cards are used to cope with the cases where no label can be assigned due to none-overlapping parts of the fingerprints, smudged regions, etc.

In the tree search the minutiae reliability measure is used to rank the minutiae so that the most reliable minutiae are matched first. In this way it is expected that a reduced number of minutiae can be used in the matching, and still be able to identify the fingerprint. Using a reduced number of minutiae the matching tree will only be expanded to the necessary depth, and thus reduce the matching time.

The evaluation function used in the matching is inspired by Boyer & Kak [2] and Vosselman [7] who suggested to use information theory instead of formulating a heuristic evaluation function [5]. The evaluating function is based on mutual information as it allows for using both symbolic and numeric features and both attributes and relations at the same time. Furthermore wild cards are easily coped with, because it can be shown that the mutual information in assigning a wild card is zero [7]. The evaluation function is based on measuring the mutual information in assigning the label minutiae, L to the unit minutiae U . If the mutual information is split up into the information which originates from the attributes and the relations respectively, the matching score (MS) can be written as;

$$MS = I_a(U; L) + I_r(U; L) = \sum_{(i,j)} \sum_{l=1}^N I(a(p_i); a(q_j)) + \sum_{k=1}^K \sum_{(i,j)} \sum_{l=1}^{N_k} I(a(r_{k_i}); a(s_{k_j}))$$

where (i, j) are corresponding minutiae pairs and $a(p_i)$ and $a(q_j)$ are attribute vectors of length N in the unit and label fingerprints respectively. $a(r_{k_i})$ and $a(s_{k_j})$ are the relation vectors of length N_k which are defined for pairs of corresponding minutiae (i, j) and for all tuples (in this case pairs as the relation is binary) of minutiae within each fingerprint. There exist K such tuples. The mutual information is defined as $I(a; b) = -\log(\text{prob}(a)) + \log(\text{prob}(a | b))$.

In order to use the evaluation function the a priori and the conditional probability distributions have to be estimated. Since some of the features are continuous, either a polynomial approximation can be used or the features can be discretized. Discretized features are much faster in an implementation, and it is therefore chosen to use these with as many intervals as possible, while it is still possible to estimate the probabilities properly. The 435 minutiae pairs used for the feature evaluation were also used to estimate the probabilities. Since the feature values in the two impressions of the same finger can be assumed independent the probability estimation is based on 870 attribute values and 12.346 relation values.

The minutiae reliability is also included in the evaluation function so that more reliable minutiae are given a higher weight than the unreliable. This is done by multiplying the minutiae reliability of the involved minutiae by the information for each attribute and relation in an assignment. The matching score can then be calculated as

$$MS = \sum_{(i,j)} \sum_{l=1}^N m_a \cdot I(a(p_i); a(q_j)) + \sum_{k=1}^K \sum_{(i,j)} \sum_{l=1}^{N_k} m_r \cdot I(a(r_{k_i}); a(s_{k_j}))$$

where $m_a = m(p_i) \cdot m(q_j)$ and $m_r = m(p_{r_i}) \cdot m(q_{r_j}) \cdot m(p_{s_i}) \cdot m(q_{s_j})$. The notation $m(\cdot)$ denotes the minutiae reliability for a given minutiae.

Before the minutiae reliability is used it is scaled to lie about 1. Through the introduction of a scale factor, it can be controlled to which degree the minutiae reliability should be used.

6 Results

In the Introduction it was hypothesized that a more reliable and faster matching of finger prints can be obtained using weighted minutiae.

A more reliable matching is expected to be obtainable if the minutiae reliability is used to weight reliable minutiae higher than unreliable ones as described earlier. To obtain a faster matching we suggest to use a hierarchical matcher in which the initial match is based on a few of the most reliable minutiae (selected by the minutiae reliability measure) followed by a more complete match on the best of the initial matches using more minutiae. To make this approach faster it requires that matching few minutiae is faster than matching many, and that the number of matches that it is necessary to perform can be reduced significantly from the first to the second match.

Two series of experiments were performed to verify the hypothesis. In all tests 100 fingerprints were matched against a database of 250 fingerprints.

6.1 Matching using Weighted Minutiae

The effect of using the minutiae reliability measure for weighting the minutiae was tested by matching the fingerprints using 6 minutiae and an increasing scale factor. The results are evaluated by calculating the difference in matching score

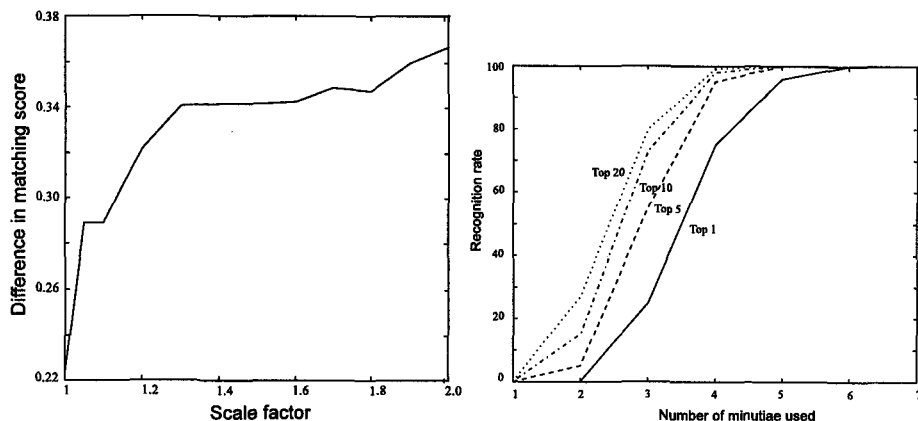


Fig. 4. (Left): The difference in matching score between the correctly matching fingerprints and the best of the other matches. (Right): The position of the correctly matching fingerprints in the ranked list using an increasing number of minutiae in the matching.

between the correctly matching fingerprints and the best match of the other 249 fingerprints. This way is used because all fingerprints are correctly identified using 6 minutiae, and because the larger the difference to the second best match in a small database, the higher is the correct match likely to be in a ranked list from a large database. The result is shown in figure 4(left). A scale factor of 1 equals the situation where no weights are used. The matching is improved when the minutiae reliability is used with higher weight. Most is, however, gained by increasing the scale factor to 1.3, after this point the improvement is minimal.

6.2 Hierarchical Matching

To investigate if a hierarchical matcher is faster, it is important to know how the matching time increases as the number of minutiae increase, and to verify that a matching based on only a very limited number of minutiae is able to select the true match for the second stage of the classification.

Measuring the average time spent on matching with 10 fingerprints with an increasing number of minutiae, showed an almost exponential growth in matching time [4]. To investigate the systems ability to select the true match 4 different ranked lists were calculated using different numbers of minutiae. The results are shown in figure 4(right). From the figure it can be seen that if four minutiae are used 99 % are in Top-20 and 75 % are number one in the ranked list. Increasing the number of minutiae to five, 95 % of the true matches are number one and using six all fingerprints are classified correctly. These results indicate that a hierarchical matcher can be based on very few minutiae.

Within the time frame of this project it has not been possible to set up a large test for measuring the performance of the hierarchical classifier. However, the two sets of experiments mentioned above strongly indicate that a considerable

reduction in the overall matching time can be obtained by using a hierarchical classifier when working on large databases. The exact improvements will depend on the quality of the prints and the type of matcher.

7 Conclusion

In this paper a minutiae reliability measure has been defined and methods for calculating the measure given. It is shown how it can be integrated in a fully automatic fingerprint identification system

It is shown that the matching can be improved by using the minutiae reliability in the evaluation function. This is especially important in a large database, because the chance of finding the correct match among the first in a ranked list is improved.

It is shown that good matching results can be obtained by matching a reduced number of minutiae chosen among the most reliable minutiae. This indicates that a faster matching can be obtained by using a hierarchical classifier. The advantage of a hierarchical matching is especially large in a tree search which is used in this paper. A tree search is, however, not fast enough for use in systems where fingerprints are to be matched against a larger database, but advantages in regard to speed will possibly be obtainable for other matching methods as well.

To summarize, we believe that the results documented in this paper clearly verify the hypothesis put forward in the introduction and that the results strongly suggest that the use of weighted minutiae in matching of fingerprints can improve the matching performance significantly.

References

1. G. Borgefors. Distance transformations in arbitrary dimensions. *Computer Vision, Graphics and Image Processing*, 27:321–345, 1984.
2. K.L. Boyer and A.C. Kak. Structural stereopsis for 3-d vision. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1988.
3. A. Datta and S.K. Parui. A robust parallel thinning algorithm for binary images. *Pattern Recognition*, 27(9):1181–1192, 1994.
4. F. Johannesen and S. Raaschou. Fingerprint identification using weighted minutiae. Master's thesis, Aalborg University, Laboratory of Image Analysis, Denmark, 1995.
5. Peter Jürgensen, Ole Vilhelm Larsen, and Lars H. Andersen. A model-based fingerprint verification system. In D. Dori and A. Bruckstein, editors, *Shape, Structure and Pattern Recognition*. World Scientific, 1995.
6. L. O'Gorman and J. V. Nickerson. An approach to fingerprint filter design. *Pattern Recognition*, 22(1):29–38, 1989.
7. G. Vosselman. *Relational Matching*. Lecture Notes in Computer Science. Springer-Verlag, 1992.
8. Q. Xiao and H. Raafat. Fingerprint image postprocessing: A combined statistical and structural approach. *Pattern Recognition*, 24(10):985–992, 1991.