A Correlation-Based Fingerprint Verification System

Asker M. Bazen, Gerben T.B. Verwaaijen, Sabih H. Gerez, Leo P.J. Veelenturf and Berend Jan van der Zwaag

University of Twente, Department of Electrical Engineering, Laboratory of Signals and Systems, P.O. box 217 - 7500 AE Enschede - The Netherlands
Phone: +31 53 489 3827 Fax: +31 53 489 1060

E-mail: a.m.bazen@el.utwente.nl

Abstract— **In this paper, a correlation-based fingerprint verification system is presented. Unlike the traditional minutiae-based systems, this system directly uses the richer gray-scale information of the fingerprints. The correlation-based fingerprint verification system first selects appropriate templates in the primary fingerprint, uses template matching to locate them in the secondary print, and compares the template positions of both fingerprints.**

Unlike minutiae-based systems, the correlation-based fingerprint verification system is capable of dealing with bad-quality images from which no minutiae can be extracted reliably and with fingerprints that suffer from non-uniform shape distortions. Experiments have shown that the performance of this system at the moment is comparable to the performance of many other fingerprint verification systems.

Keywords— **fingerprint verification, image processing, template matching.**

I. Introduction

This paper discusses a fingerprint verification system. As illustrated in Figure 1, a fingerprint is consists of *ridge-valley* structures [1]. In this figure, the ridges are black and the valleys are white. When using fingerprints for recognition systems, the ridge-valley structures are the main source for the information to be extracted from the fingerprints. It is possible to identify two levels of detail in a fingerprint.

- The *directional field* describes the coarse structure, or basic shape, of a fingerprint. The directional field is defined as the local orientation of the ridge-valley structures at each position in the fingerprint. The directional field is for instance used for *classification* of fingerprints.
- The *minutiae* provide the details of the ridge-valley structures, like ridge-endings and bifurcations. Minutiae are for instance used for *matching*, which is a one-to-one comparison of two fingerprints.

Two kinds of fingerprint recognition systems exist. In a fingerprint *identification* system, a user only offers his finger. Then, the system searches its internal database for a matching print. If a matching print is found, this identifies the person.

Fig. 1. Example of a fingerprint. The ridges are black and the valleys are white in this figure.

A fingerprint *verification* system, on the other hand, checks whether a person really is who he claims to be. A person first identifies himself by e.g. an ID-card or a username. Then, instead of entering a personal identification code or a password, the user puts his or her finger on a sensor. The system retrieves a fingerprint of that person, called the *primary* fingerprint, from its database, and checks whether it matches the live-scanned finger, which is called the *secondary* fingerprint. If they match, the user is classified as genuine, and gets access to the system. If the fingerprints don't match, the user is classified as impostor. The performance of a fingerprint matching system can be shown in a confusion matrix, in which the probabilities of all possible situations are shown:

	ω_0	ω_1
$\hat{\omega}_0$	TRR	FRR
$\hat{\omega}_1$	FAR	TAR

(1)

In this matrix, ω_0 is the impostor class, ω_1 the genuine class, $\hat{\omega}_0$ and $\hat{\omega}_1$ the corresponding assigned classes, TRR the true rejection rate, FRR the false rejection rate, FAR the false acceptance rate and TAR the true acceptance rate.

ISBN: 90-73461-24-3

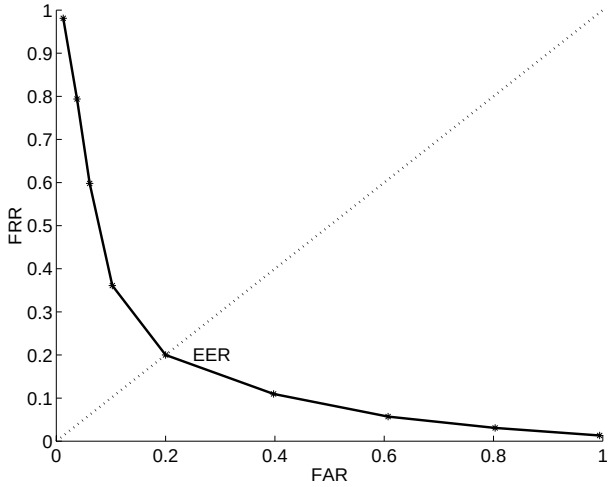


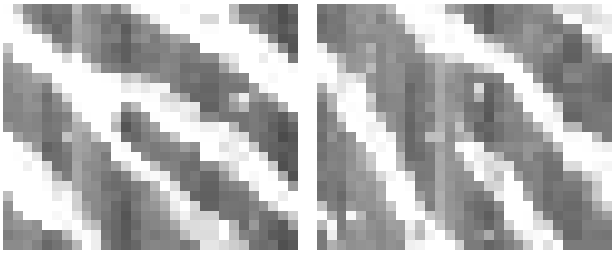
Fig. 2. Example of a receiver operating curve (ROC), in which the possible operating modes are indicated by the stars.

For most fingerprint matching systems, these rates can be controlled by a parameter. The receiver operating curve (ROC), of which an example is shown in Figure 2, is a plot in which FRR is plotted against FAR for the different operating modes. The closer the curve approaches the point where $FRR = 0$ and $FAR = 0$, the better is the performance of the system. The operating mode where $FRR = FAR$ is called the equal error rate (EER).

Fingerprints are slightly different each time they are captured. Therefore, matching cannot be carried out by simply calculating the crosscorrelation of two prints. There are two types of distortions when comparing one fingerprint to another print of the same finger.

- *Noise* is caused by the capturing device or by e.g. dirty fingers. This noise can be reduced by application of appropriate filters.
- *Shape distortions* are caused by pressing the convex elastic fingerprint surface on a flat sensor. This may result in stretch, rotation and shear, which also might be present only in certain parts of the fingerprint due to non-uniform finger pressure. Shape distortions cannot be compensated easily.

Most fingerprint recognition systems first extract the minutiae from fingerprints, and then compare the minutiae sets of two prints. The standard minutiae-based fingerprint verification system is discussed in Section II. To eliminate some of the drawbacks of the minutiae based systems, we have chosen to design a system that directly uses the gray-level information. This *correlation-based fingerprint verification system* is discussed in Section III. In Section IV, some experimental results of the application of this system to fingerprint databases are discussed, and in Section V, the conclusions of this paper are given.



(a) Ridge-ending (b) Bifurcation

Fig. 3. Examples of minutiae.

II. Minutiae-Based Approach

Most fingerprint verification systems follow a minutiae-based approach, see e.g. [1]. Minutiae-based fingerprint verification systems first extract the minutiae, shown in Figure 3, from the fingerprint images. Then, the decision is based on the correspondence of the two sets of minutiae locations.

Minutiae-based fingerprint verification systems use a large number of successive processing steps. In general, the following steps can be identified in a minutiae-based system:

- directional field estimation,
- adaptive filtering for noise reduction,
- thresholding to obtain a binary fingerprint image,
- morphological operations like thinning to obtain ridges that are only one pixel wide,
- minutiae extraction from the thinned image,
- application of heuristics to reduce the number of false minutiae,
- registration of minutiae templates by Hough transform,
- matching score computation.

The main drawback of the minutiae-based approach is the error propagation from the minutiae extraction to the decision stage. In general, the extracted minutiae templates contain a number of false minutiae, while also some minutiae will be missed. This is especially the case when using bad-quality fingerprints. The heuristics do not catch all spurious minutiae, while they might reject some of the genuine minutiae. As a result, the decision stage has to compare two affected sets.

The minutiae sets of the primary and secondary fingerprints are *registered*, which means aligned, by means of a Hough transform. This transform searches for the parameter set (T_x, T_y, φ, S) that aligns the minutiae sets as well as possible. For this purpose,

the number of matching minutiae pairs is used as an evaluation measure. In the parameter set, T_x and T_y are translations in x and y direction, φ is rotation and S is scale.

Minutiae sets of prints that originate from the same finger do in general not contain the same minutiae, due to errors in the first stages of the algorithm. Because of false and missed minutiae, it is even possible that both sets do not even contain the same number of minutiae. Obviously, this decreases the performance of registration and matching. Shape distortions decrease the performance even more. In the presence of these distortions, the perfectly registering transformation does not exist, even for sets that only contain corresponding minutiae.

III. Correlation-Based Fingerprint Matching

In order to deal with some of the problems of the minutiae-based approach, we have chosen an alternative approach. Instead of only using the minutiae locations, our method directly uses the gray-level information from the fingerprint image, since a gray-level fingerprint image contains much richer, more discriminatory, information than only the minutiae locations. Those locations only characterize a small part of the local ridge-valley structures [2, 3, 4].

The correlation-based fingerprint verification system is inspired by [5]. It first selects characteristic templates in the primary fingerprint. Then, template matching is used to find the positions in the secondary fingerprint at which the templates match best. Finally, the template positions in both fingerprints are compared in order to make the decision whether the prints match.

A. Template Selection

The first step in the template matching algorithm is the selection of appropriate templates. This is a crucial step, since good templates will be easily localized in the secondary print at the right position, while bad templates will not. More generally, the templates should be uniquely localized in the secondary fingerprint. The template should fit as well as possible at the same location, but as badly as possible at other locations.

The first template property to consider is the size of the templates. There must be an optimal template size, as can be seen from two extreme situations. When the entire fingerprint is taken as template, any attempt to align specific corresponding positions will lead to misalignments at other positions due to shape distortions. On the other hand, if templates of only 1 by 1 pixel are chosen, it is clear that the templates do not offer enough distinction. Experiments have shown that a template size of 24 by 24 pixels is a good compromise.

The second problem in selecting the right templates is which template positions to chose. Research has shown for instance, that a template that contains only parallel ridge-valley structures cannot be located very accurately in the secondary fingerprint. In this paper, three template selection criteria are proposed, being *minutiae-based*, *coherence-based* and *correlation-based*.

A.1 Minutiae-Based Template Selection

As mentioned before, templates that only contain parallel ridge-valley structures do not offer much distinction. On the other hand, when a template contains one or more minutiae, it will be much easier to find the correct location in the secondary print. Using this assumption, one possible approach to select template locations is to extract minutiae from the fingerprint image and to define templates around the minutiae locations.

A drawback of this technique is that it suffers from most of the problems of minutiae-based systems. Still, many false minutiae are extracted, causing at least a part of the templates to be rather unreliable.

A.2 Coherence-Based Template Selection

The coherence of an image area is a measure that indicates how well the local gradients are pointing in the same direction. In areas where the ridge-valley structures are only parallel lines, the coherence is very high, while in noisy areas, the coherence is low [6, 7].

Templates that are chosen in regions of high coherence values cannot be located reliably in a second fingerprint [8]. However, at locations around minutiae, more gray-scale gradient orientations are present, resulting in a significantly lower coherence. Therefore, the coherence can be used as an appropriate measure that indicates the presence of minutiae as well as a measure that indicates how well a template can be located in the secondary fingerprint.

At first sight, this template selection criterion seems to conflict with segmentation [6]. While segmentation chooses the regions of low coherence values as noise or background areas, now the regions that have low coherence values have to be chosen as reliable templates. However, this contradiction is solved by the notion of scale [9]. Segmentation selects a large, closed area as foreground, in which holes and other irregularities are filled by means of morphology. Instead, the coherence based template selection only searches for local coherence dips in this foreground area.

The drawback of this method is that noisy areas

show coherence dips as well, while these are certainly not reliable templates. This problem may be solved by using appropriate filters.

A.3 Correlation-Based Template Selection

The third method satisfies the template requirements most directly. In this method, templates are selected by checking how well they fit at other locations in the same fingerprint. If a template fits almost as well at another location as it does at its original location, it is not a useful template. However, if a template fits much worse at all other locations in the fingerprint, it is a template that offers a lot of distinction. Therefore, the ratio of fit at a template's original location to the fit at the next best location can be used as a template selection criterion.

Since the correlation-based checking is carried out by means of template matching, this method consumes a lot of computational power. This makes it a less attractive method to use. However, it is for instance possible to combine this approach with the previous two methods. In that case, possible template locations are extracted by one of the methods of the previous subsections. Then, the correlation characteristics of those locations are checked as an additional selection criterion.

B. Template Matching

Once the templates have been selected in the primary fingerprint, their corresponding positions in the secondary fingerprint have to be found. This can be done using standard template matching techniques.

The template is shifted pixelwise over the secondary print. At each position, the gray-level distance between the template and the corresponding area in the secondary print is determined by summing the squared gray-level differences for each pixel in the template. After having shifted the template over the entire finger, the location where the distance is minimal is chosen as the corresponding position of the template in the second fingerprint.

This is a very computationally demanding technique. However, there are possibilities to speed up the process. When both the template and the fingerprint are normalized (we have chosen: $E[I_{x,y}] = 0$ and $Var[I_{x,y}] = 1$, where $I_{x,y}$ is the gray-scale image at pixel (x, y)), a convolution, or filter, can be used instead. For this method, it is required that these conditions do not only hold globally for the whole image, but also locally for each area in the image. If the size of the fingerprint is chosen appropriately, a 2-dimensional FFT can be used for even more efficiency [10].

As result of the template matching, for each template position in the primary fingerprint, the corresponding, or best matching, template position in the secondary print is obtained.

C. Classification of Template Positions

The fingerprint matching algorithm, based on two sets of template positions, uses two decision stages. First, elementary decisions are made by classifying the individual template position pairs to be matching or not. Then, the information of all template pairs is merged in order to make a final decision whether the primary and secondary fingerprint match or not.

C.1 Elementary Decisions

After template matching, there are two sets of corresponding template locations $(\boldsymbol{x}^p, \boldsymbol{y}^p)$ and $(\boldsymbol{x}^s, \boldsymbol{y}^s)$, where $\boldsymbol{x} = [x_1, \ldots, x_n]^T$ and $\boldsymbol{y} = [y_1, \ldots, y_n]^T$ are the coordinates of the templates and the superscripts p and s refer to the primary and secondary fingerprints. Now, for all n template pairs, a decision has to be made whether the positions correspond to each other:

$$(x_i^s, y_i^s) \stackrel{?}{\approx} (x_i^p, y_i^p) \qquad \text{for } 1 \le i \le n \tag{2}$$

Directly examining the difference of both template coordinate pairs would only allow some fixed translation in x and y directions. Template pairs that are some more translated with respect to each other would be classified as non-matching. In order to deal with the translations, relative template positions (RTPs) are used instead. Now, the test becomes:

$$\left[(x_i^s, y_i^s) - (x_j^s, y_j^s)\right] \stackrel{?}{\approx} \left[(x_i^p, y_i^p) - (x_j^p, y_j^p)\right] \qquad \text{for } 1 \le i, j \le n,\ i \ne j \tag{3}$$

or

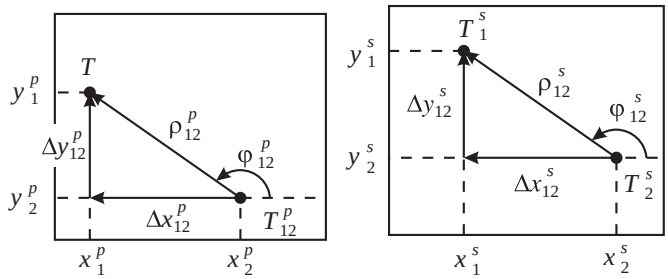
$$(\Delta x_{ij}^s, \Delta y_{ij}^s) \stackrel{?}{\approx} (\Delta x_{ij}^p, \Delta y_{ij}^p) \qquad \text{for } 1 \le i, j \le n,\ i \ne j \tag{4}$$

using the notations that are illustrated in Figure 4. Instead of comparing n template positions, now $n(n-1)/2$ RTPs are classified, of which $n-1$ are independent.

Direct application of this test allows for some fixed displacement of the templates in x and y direction, which is set by a threshold (x_T, y_T). However, to allow rotation and scaling as well, the RTPs are converted to polar coordinates, as illustrated in Figure 4:

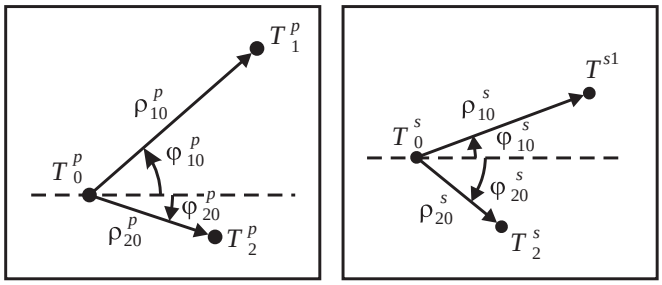
$$\rho = \sqrt{(\Delta x)^2 + (\Delta y)^2} \tag{5}$$

$$\varphi = \angle(\Delta x, \Delta y) \tag{6}$$



(a) Primary fingerprint (b) Secondary fingerprint

Fig. 4. Relative template positions, tolerating translations.



(a) Primary fingerprint (b) Secondary fingerprint

Fig. 5. Use of 3 templates to allow rotation and scaling.

where $\angle(x, y)$ is defined as:

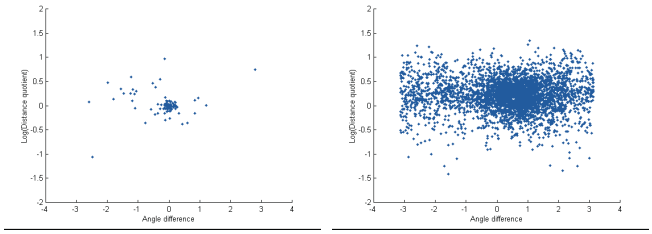
$$\angle(x,y) = \begin{cases} \tan^{-1}(y/x) & x \geq 0 \\ \tan^{-1}(y/x) + \pi \quad \text{for} & x < 0 \wedge y \geq 0 \\ \tan^{-1}(y/x) - \pi & x < 0 \wedge y < 0 \end{cases} \tag{7}$$

This leads to the classification test:

$$(\rho^s_{ij}, \varphi^s_{ij}) \stackrel{?}{\approx} (\rho^p_{ij}, \varphi^p_{ij}) \qquad \text{for } 1 \leq i,j \leq n,\ i \neq j \tag{8}$$

which tolerates some fixed amount of rotation and scaling, especially when ρ_s and ρ_p are compared by division instead of subtraction. This tolerates more displacement for templates that are further away from each other, which is a much more natural restriction than fixed x and y displacements. This kind of tolerance is capable of handling some amount of non-uniform shape-distortion, caused by the fingerprint elasticity. Again, the degree of tolerance can be set by thresholds ρ_T and φ_T.

The next step is to allow any rotation and scaling instead of only some fixed amount. As illustrated in Figure 5, a third template is used to obtain the test that is not only fixed for translation of the template positions, but for rotation and scaling as well:



(a) Matching fingerprints (b) Non-matching fingerprints

Fig. 6. Scatter diagrams of the $(\ln \rho_s/\rho_p,\ \phi_s - \phi_p)$ pairs.

$$(\varphi^s_{ji} - \varphi^s_{ki},\ \rho^s_{ji}/\rho^s_{ki}) \stackrel{?}{\approx} (\varphi^p_{ji} - \varphi^p_{ki},\ \rho^p_{ji}/\rho^p_{ki}) \\ \text{for } 1 \leq i,j,k \leq n,\ i \neq j \neq k \tag{9}$$

However, there is one practical drawback to this method. The template locations are obtained by means of template matching. If a template is scaled or rotated more than some constant, it is not possible anymore to localize it in the secondary image. Furthermore, the same holds, to some extent, for scaling. This makes the tolerance of any amount of rotation and scaling less useful.

Since the test of Expression 8 uses one more independent classification than the test of Expression 9, and the last step does not add much value, we adopt the test of Expression 8 for the rest of the paper. The scatter diagrams of the $(\ln \rho^s_{ij}/\rho^p_{ij},\ \varphi^s_{ij} - \varphi^p_{ij})$ pairs, both for matching fingerprints and for non-matching prints, are given in Figure 6. These pairs are classified by applying an elliptical threshold:

$$\left(\frac{\ln \frac{\rho^s_{ij}}{\rho^p_{ij}}}{\rho_T}\right)^2 + \left(\frac{\varphi^s_{ij} - \varphi^p_{ij}}{\varphi_T}\right)^2 < 1 \tag{10}$$

where ρ_T and φ_T are the parameters determining the shape of the ellipse.

The result of this procedure is a match or non-match classification for all $n(n-1)/2$ template combinations. The probability that an RTP is classified non-matching while the prints match, is given by $p(\hat{\omega}_{0,T}|\omega_{1,F})$, while the probability that a template distance is classified matching while the prints don't match is denoted by $p(\hat{\omega}_{1,T}|\omega_{0,F})$. Here, the subscripts T and F denote template and fingerprint respectively.

The thresholds that provide the best discrimination of matching and non-matching RTPs, give for this database:

$$p(\hat{\omega}_{0,T}|\omega_{1,F}) = 0.2 \quad (11)$$
$$p(\hat{\omega}_{1,T}|\omega_{0,F}) = 0.02 \quad (12)$$

C.2 Combining Elementary Decisions

We now have to classify the two fingerprints as being a match or not. This decision is based on $n(n-1)/2$ relative template positions. This can be solved using the theory of Bernoulli experiments, which combine n independent experiments using binominal distribution. The probability $P(X = k)$ for k positive outcomes when doing n independent experiments that all have a probability of success p is given by:

$$P(X = k) = \binom{n}{k} p^k (1-p)^{n-k} \quad (13)$$

where

$$\binom{n}{k} = \frac{n!}{k!\ (n-k)!} \quad (14)$$

is the binominal coefficient and $n!$ denotes factorial.

The $n(n-1)/2$ RTPs are certainly not independent. If we choose one template as reference, all template positions are fixed by only $n-1$ distances, while all other distances can be calculated. Therefore, only $n-1$ independent RTPs are available.

The choice of the reference template is rather important. If one template is not localized at the right position in the secondary fingerprint, and this template is chosen as reference template, all RTPs will be classified non-matching. This results in a false rejection of the fingerprint. Therefore, we chose the reference template as the one that has the most RTP matches.

Once the reference template has been chosen, there are $n-1$ RTPs that are in principle independent. This means that the combination of all RTP matches can be considered as a Bernouilli experiment, and Expression 13 can be applied. A threshold k_T is set for the final fingerprint match or non-match classification, resulting in:

$$\begin{aligned} FAR &= p(\hat{\omega}_{1,F}|\omega_{0,F}) \\ &= P(X \geq k_T \mid \text{non-match}) \\ &= \sum_{k=k_T}^{n-1} \binom{n-1}{k} p(\hat{\omega}_{1,T}|\omega_{0,F})^k \cdot \\ &\quad (1 - p(\hat{\omega}_{1,T}|\omega_{0,F}))^{n-k-1} \end{aligned} \quad (15)$$

and

$$\begin{aligned} FRR &= p(\hat{\omega}_{0,F}|\omega_{1,F}) \\ &= P(X < k_T \mid \text{match}) \\ &= \sum_{k=0}^{k_T-1} \binom{n-1}{k} p(\hat{\omega}_{0,T}|\omega_{1,F})^{n-k-1} \cdot \\ &\quad (1 - p(\hat{\omega}_{0,T}|\omega_{1,F}))^k \end{aligned} \quad (16)$$

In order to meet the commonly used requirements for fingerprint verification systems, being $FAR = 10^{-4}$ and $FRR = 10^{-2}$, and using the values given in Expressions 11 and 12, it can be calculated that the use of $n = 10$ templates with threshold $k_T = 4$ satisfies the required performance. For these parameters, the exact performance is given by:

$$FRR = p(\hat{\omega}_{0,F}|\omega_{1,F}) = 1.8 \cdot 10^{-5} \quad (17)$$
$$FAR = p(\hat{\omega}_{1,F}|\omega_{0,F}) = 3.1 \cdot 10^{-3} \quad (18)$$

An example of the results of this method, using only 5 templates, is given in Figure 7. The figure shows that for matching prints, indeed the relative template positions are about equal, while for non-matching prints, they are completely different.

D. Discussion of the Method

The correlation-based fingerprint verification that is proposed in this section, is compared to the traditional minutiae-based methods. The advantage of the correlation-based method are:

- The method uses the much richer gray-level information of the fingerprint image instead of only positions of minutiae.
- The method is also capable of dealing with fingerprints of bad image quality from which no minutiae can be extracted reliably.
- False and missed minutiae do not decrease the matching performance.
- Unlike the minutiae templates, the template locations are already paired, which results in much simpler matching methods. When registering minutiae sets, it is not known in advance which minutiae from both sets should correspond.
- The first decision stage only classifies relative template positions. This method tolerates non-uniform local shape distortions in the fingerprint, unlike the minutiae templates for which the optimal global transform is searched.

The disadvantages of the correlation-based fingerprint verification method are:

- Template matching is a method that demands a rather high computational power, which makes

(a) Primary fingerprint (b) Matching fingerprint (c) Non-matching fingerprint

Fig. 7. Template positions in primary and secondary fingerprints.

the method less applicable for real time applications.

- The method is at the moment not capable of dealing with rotations of more than about 10 degrees. This is caused by the fact that, for larger rotations, the templates don't match well anymore, causing incorrect positions to be found. A solution to this problem is rotating the templates and then performing the matching again. However, this is a solution that requires a lot of additional computational power.
- Problems might arise if the minutiae- or coherence-based template selection methods are used while 2 minutiae surroundings resemble a lot. In this case, there is a probability that template matching will find the incorrect template position, which degrades the matching performance. Use of the correlation-characteristic template selection will solve this problem.

IV. Experimental Results

The correlation based fingerprint verification system that is described in this paper has participated in FVC2000, a Fingerprint Verification Competition [11] which was part of the ICPR2000 conference. This section will present some of the results of this competition as well as a discussion how to interpret these results.

A. Experiment Setup

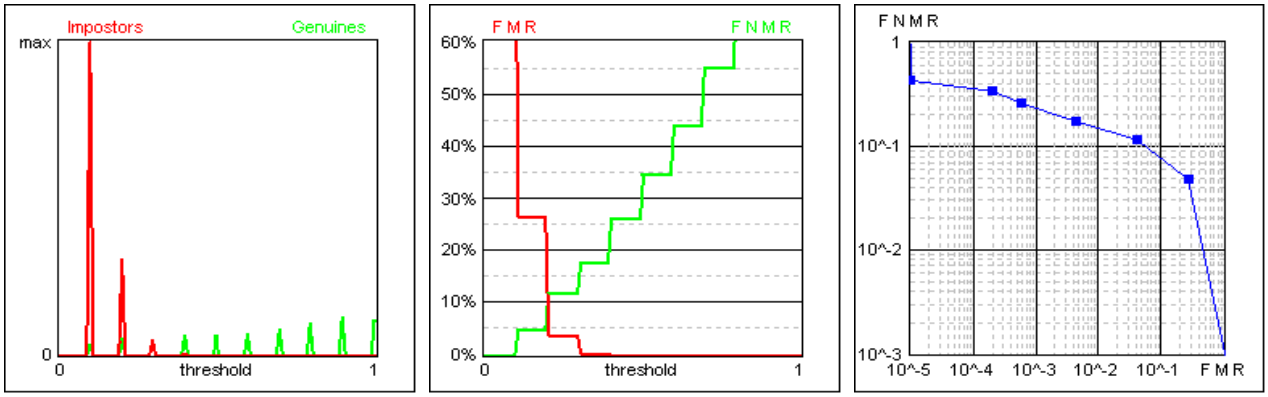
Although many research groups have developed fingerprint verification algorithms, only a few benchmarks are available. Developers usually perform tests over self-collected databases, since in practice, the only available sets are the NIST databases, containing thousands of scanned inked impressions of fingers. Since these images significantly differ from those acquired electronically, they are not well-suited for testing on-line fingerprint systems.

FVC2000 attempts to establish a first common benchmark, allowing companies and academic institutions to unambiguously compare performance and track improvement in their fingerprint recognition algorithms. However, the databases used in this contest have not been acquired in a real environment according to a formal protocol and the images originate from sensors that are not native to the participating systems. Therefore, FVC2000 is not an official performance certification of the participating systems, but it should be considered as a technology evaluation.

The system performance is evaluated on images from four different fingerprint databases. Three of these databases are acquired by various sensors, low-cost and high-quality, optical and capacitive. The fourth database is synthetically generated using the approach described in [12]. All databases contain 8 prints of 110 different fingers, so 880 fingerprints in total. All prints were captured by untrained volunteers, resulting in fingerprints ranging from high quality to very low quality.

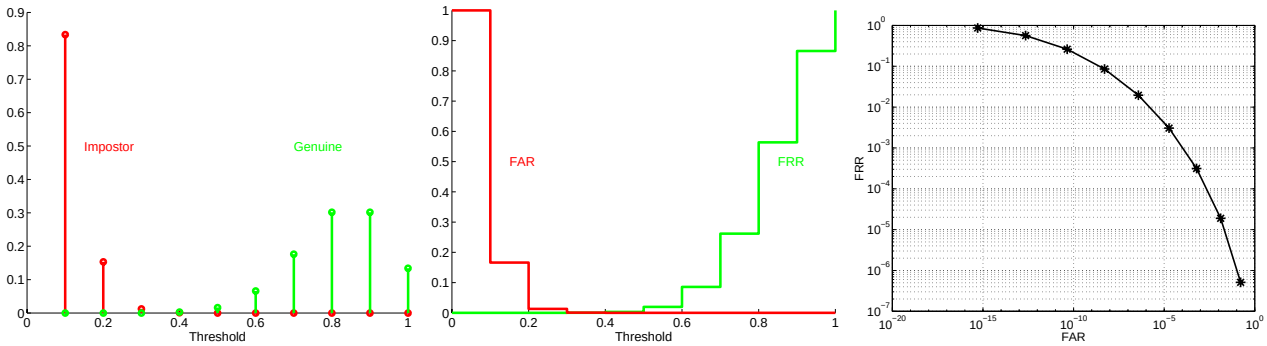
Of all fingerprints, 8 prints of 10 fingers were distributed to the participants to tune their algorithms to the databases. The algorithms were tested using the other 100 fingers.

For each database, an FAR and an FRR test is performed. For the FAR test, the first print of each finger is matched against the first print of all other fingers, leading to 4,950 impostor attempts. For the FRR test, each print of each finger is matched against all other prints of the same finger, leading to 2,800 genuine attempts.



(a) Distributions (b) FAR and FRR (c) ROC

Fig. 8. Results of the correlation based fingerprint verification system. In this figure, FAR is called false matching rate (FMR) and FRR is called false non-matching rate (FNMR).



(a) Distributions (b) FAR and FRR (c) ROC

Fig. 9. Theoretic results.

B. Experimental Results

The correlation based fingerprint verification system performed about halfway the best and the worst of the other 10 participating systems. Some charts, showing performance measures for the first database, are given in Figure 8. The discrete distribution is caused by the fact that the competition required a confidence measure between 0 and 1, indicating how well 2 fingerprints match. The confidence measure of our method is the quotient of the number of matching RTPs and the maximum number of matching RTPs that is possible, causing a distribution that consists of n discrete peaks.

One interesting measure is the equal error rate (EER) of the system, which is the operating mode of the system for which FAR and FRR are equal. For this database, the EER was 7.98%.

The correlation based fingerprint verification system consumes a lot of CPU time. The enrollment is the most time-consuming part of the algorithm. The version that was sent to FVC2000 takes 10 seconds, which was the maximum time allowed. The enrollment time can be reduced by evaluating fewer candidate templates, but this will decrease the overall template quality and therefore also the system performance. The average matching time was 2 seconds.

C. Comparison to Theoretic Results

In order to compare the experimental results to the theory, Figure 9 shows the same performance measures, according to the theory of Expressions 11, 12, 15 and 16. Using these expressions, the theoretic EER is given by $4.6 \cdot 10^{-4}$.

From these performance measures, it is clear that the correlation-based fingerprint verification system does not perform as well as it was supposed to. When comparing Figure 8(a) to Figure 9(a), is can be seen that the experimental impostor distribution approximately equals the theoretic one, but that the genuine distribution is much flatter than it is in theory.

The deviation of the genuine distribution can be explained by the fact that the RTPs are not independent for genuine matches, while this was assumed

by using the binominal distribution of Expression 13. The most probable cause of the lower genuine scores is the rotation of fingerprints. If two fingerprints are rotated more than about 10 degrees with respect to each other, template matching cannot localize some of the templates correctly. This causes the dependent RTPs to be classified incorrectly.

This situation certainly exists for some pairs of fingerprints in the databases. The fingerprints are specified to have a rotation of -15 to +15 degrees from normal, which means that relative rotations up to 30 degrees might appear in these databases.

A possible solution to this problem is the determination of the relative rotation of two fingerprints, using for instance the singular points. Once the rotation is known, it can be compensated, after which the correlation based fingerprint verification algorithm can be applied directly.

V. Conclusions

This correlation-based fingerprint verification system provides a very simple and direct solution to the fingerprint matching problem. Unlike the minutiae-based systems, this approach does not require much preprocessing. As a consequence, there will be no errors introduced in these steps.

The system uses the much richer gray-level information of a fingerprint image. It is capable of dealing with bad image quality fingerprints and missed and spurious minutiae. Due to the paired templates, the decision stage is much simpler and it is able to deal with some non-uniform shape-distortion problems.

Experiments have shown that the correlation based fingerprint verification system performs approximately as well as other types of systems. The performance of the system can be enhanced by solving the problem of fingerprints that show more than some amount of rotation with respect to each other.

Acknowledgement

This research has been carried out within the *Euregio Computational Intelligence Center* (ECIC), subsidized by the European Commission, The Netherlands and Nordrhein-Westfalen, in the scope of the Interreg Program.

References

[1] A.K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity-authentication system using fingerprints," *Proc. of the IEEE*, vol. 85, no. 9, pp. 1365–1388, Sept. 1997.

[2] S. Prabhakar, A.K. Jain, J. Wang, S. Pankanti, and R. Bolle, "Minutia verification and classification for fingerprint matching," in *Proceedings of ICPR2000, 15th Int. Conf. Pattern Recognition*, Barcelona, Spain, Sept. 2000.

[3] A.K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Transactions on Image Processing*, vol. 9, no. 5, pp. 846–859, May 2000.

[4] D. Maio and D. Maltoni, "Minutiae extraction and filtering from gray-scale images," in *Intelligent Biometric Techniques in Fingerprint and Face Recognition*, L.C. Jain et al., Ed., pp. 155–192. CRC Press LLC, 1999.

[5] A.R. Roddy and J.D. Stosz, "Fingerprint feature processing techniques and poroscopy," in *Intelligent Biometric Techniques in Fingerprint and Face Recognition*, L.C. Jain, U. Halici, I. Hayashi, S.B. Lee, and S. Tsutsui, Eds., pp. 37–105. CRC Press, 1999.

[6] A.M. Bazen and S.H. Gerez, "Directional field computation for fingerprints based on the principal component analysis of local gradients," in *Proceedings of ProRISC2000, 11th Annual Workshop on Circuits, Systems and Signal Processing*, Veldhoven, The Netherlands, Nov. 2000, to be published.

[7] M. Kass and A. Witkin, "Analyzing oriented patterns," *Computer Vision, Graphics, and Image Processing*, vol. 37, no. 3, pp. 362–385, Mar. 1987.

[8] M. Schrijver, A.M. Bazen, and C.H. Slump, "On the reliability of template matching in biomedical image processing," in *Proceedings of SPS2000, IEEE Benelux Signal Processing Chapter*, Hilvarenbeek, The Netherlands, Mar. 2000.

[9] T. Lindeberg, *Scale-Space Theory in Computer Vision*, Kluwer Academic Publishers, Boston, 1994.

[10] G.T.B. Verwaaijen, "Fingerprint authentication," M.S. thesis, Faculty of Electrical Engineering, University of Twente, Enschede, The Netherlands, May 2000, EL-S&S-002N00.

[11] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, and A.K. Jain, "Fvc2000: Fingerprint verification competition," in *Proceedings of ICPR2000, 15th Int. Conf. Pattern Recognition*, Barcelona, Spain, Sept. 2000.

[12] R. Cappelli, A. Erol, D. Maio, and D. Maltoni, "Synthetic fingerprint-image generation," in *Proceedings of ICPR2000, 15th Int. Conf. Pattern Recognition*, Barcelona, Spain, Sept. 2000.