Fingerprint Verification by Fusion of Optical and Capacitive Sensors

Gian Luca Marcialis[1] and Fabio Roli

Department of Electrical and Electronic Engineering - University of Cagliari

Piazza d'Armi - 09123 Cagliari (Italy)

Phone: +39 070 675 5776 - Fax: +39 070 675 5782

{marcialis,roli}@diee.unica.it

Abstract. A few works have been presented so far on information fusion for fingerprint verification. None, however, have explicitly investigated the use of multi-sensor fusion, in other words, the integration of the information provided by multiple devices to capture fingerprint images. In this paper, a multi-sensor fingerprint verification system based on the fusion of optical and capacitive sensors is presented. Reported results show that such a multi-sensor system can perform better than traditional fingerprint matchers based on a single sensor.

Key Words. Automatic Fingerprint Verification Systems, Multi Sensor Fusion, Fusion of Multiple Classifiers, Pattern Recognition, Image Analysis.

1 Introduction

Personal authentication through biometrics is aimed at granting or denying access to restricted resources (e.g., computer, ATM, or a restricted area in a building). The person accessing a certain resource submits her/his identity and biometrics to the automatic verification system. The system matches the given biometric with the one stored in its database associated with the claimed identity.

[1] Corresponding author

A degree of similarity, named “score”, is computed. If the score is higher than a certain acceptance threshold, the person is classified as “genuine” (i.e., the claimed identity is accepted), if not, he/she is classified as an “impostor”, and access to the required resource is denied.

Fingerprints are one of the most widely used biometrics in personal authentication. Their widespread use in both civil and forensic applications has been largely due to the fact that fingerprints are very difficult to steal and reproduce, and cannot be left behind. So far, many algorithms (Jain et al., 1997; Jain et al., 2000; Prabhakar and Jain, 2002) have been proposed to match two fingerprints. However, it is very difficult to design a matching algorithm capable of satisfying the stringent requirements of many real applications in terms of verification errors, especially when very low false acceptance (FAR) and false rejection (FRR) rates are required. Therefore, recent works have argued in favour of information fusion to improve current performances of fingerprint verification systems. So far, fusion of multiple matching algorithms, different fingerprints, and multiple impressions of the same fingerprint have been investigated experimentally (Jain et al., 1999; Prabhakar and Jain, 2002; Marcialis and Roli, 2003a; Marcialis and Roli, 2003b; Ross et al., 2003).

However, to the best of our knowledge, no work has investigated fusion of different imaging sensors. We believe this topic deserves attention, as multi sensor fusion offers some important potentialities for fingerprint verification. First, information fusion theory and the results achieved in other application fields support the hypothesis that by combining information from different physical sensors the performance of fingerprint verification can be improved substantially (Roli and Kittler, 2002). Secondly, fusion of different sensors can improve population coverage by reducing enrolment and verification failures (Ross et al., 2003). Persons with fingerprints that are poorly captured by one sensor could be enrolled satisfactorily by another. Finally, multi-sensor fusion may discourage fraudulent attempts to deceive personal identity verification systems. Deceiving a multi-sensor system by submitting fake fingers would require different kinds of fake fingers for each sensor.

On the other hand, increases in system cost and user co-operation in the enrolment and verification phases are the main drawbacks of multi sensor fusion. It should be noted, however, that similar drawbacks are observed in "multi-modal" verification systems combining multiple biometrics (e.g., fingerprint and face) (Ross and Jain, 2003). In the case of fingerprint verification, the ultimate choice will depend on the performance improvements that can be achieved by the fusion of different sensors, whose analysis is precisely the aim of this work, and on the related trade-off with increases in system cost and the required user co-operation.

In this paper, a multi-sensor fingerprint matcher based on optical and capacitive sensors is presented. A specific matching algorithm is used for fingerprint images captured by each sensor. Verification scores provided by each matcher are fused by score transformation. Reported results show that with this multi-sensor fusion, it is possible to outperform verification performances of the best matcher based on a single sensor. Moreover, analysis of the "complementarity" between optical and capacitive sensors clearly supports the potentialities of their fusion.

Section 2 describes the proposed system in detail. Section 3 reports experimental results. Section 4 draws some preliminary conclusions.

2 A Multi-sensor System for Fingerprint Verification

Figure 1 shows the architecture of our multi-sensor verification system. The first stage of the system is made up of two fingerprint capture devices, namely, an optical and a capacitive sensor. In the second stage features from the fingerprint images provided by each sensor are processed and extracted. The third stage is made up of the matching algorithm applied separately to the two sets of features. This stage produces two matching scores, which are combined to obtain a "fused" matching score. Finally, an acceptance threshold is applied to make the final decision (the claimed identity is accepted or rejected).

The following sections give a detailed description of the various modules of the system.

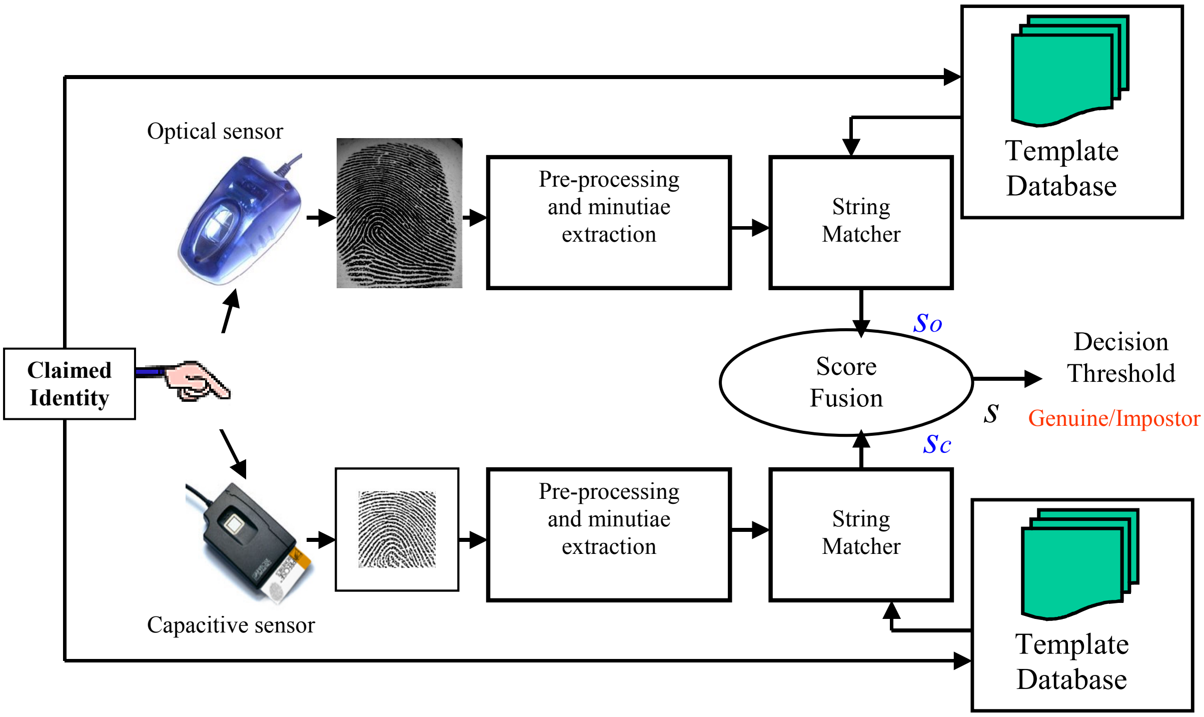

Figure 1. Architecture of the proposed multi-sensor fingerprint verification system.

2.1 Optical and capacitive sensors

We have chosen two well-known capture devices for fingerprint acquisition: an optical sensor and a capacitive sensor, because they are used extensively to test fingerprint matching algorithms (Maio et al., 2002). Moreover, their physical principles of acquisition are so different that it is reasonable to expect that "fusion" of the information provided by each of them can be effective (Xia and O'Gorman, 2003).

Optical sensors are characterised by a LED light source and a CCD placed on the side of a glass platen, on which the fingerprint to be acquired is placed. The LED illuminates the fingerprint and the CCD captures the light reflected from the glass, enhancing the ridges and valleys of the fingerprint.

The core of the capacitive sensors is the sensing surface, which is made up of a two-dimensional array of capacitor plates. The second plates are considered to be the finger skin. The capacitance is dependent on the distance between the finger skin (i.e. ridges and valleys) and the plates. The captured image is derived from the capacitance measures from each array element.

2.2 Feature extraction

The fingerprint images acquired from the optical and the capacitive sensors are processed with the same algorithms to enhance the quality of the images and to extract features. We have chosen to use only one kind of feature, namely, the minutiae-points, in order to reduce the complexity of our system as much as possible.

The enhancement process is made up of a Fourier enhancement algorithm (Candela et al., 1995) followed by a rank-order transformation to improve the result of the enhancement further (Kette and Zamperoni, 1996). Thinning and skeletonization processes are then applied through morphological operators to reduce each ridge line to 1 pixel of width (Maltoni et al., 2003). Finally, the so-called minutiae-points are extracted (Maltoni et al., 2003). The minutiae-points consist of the bifurcation and termination of each ridge line. Each minutia is represented by its location in the fingerprint image and its orientation, computed on the basis of the local orientation of the ridge the minutia belongs to. These features are widely used for fingerprint matching (Jain et al., 1997). In particular, they have been shown to be the most effective features in fingerprint verification (Prabhakar and Jain, 2002; Marcialis and Roli, 2003a).

2.3 The matching algorithm

In order to compare two fingerprints based on their minutiae points, we have used the so-called “String” algorithm (Jain et al., 1997). The score produced by the String algorithm is a real value between 0.0 and 1.0, which represents the similarity degree of two sets of minutiae-points. The maximum value indicates that the compared minutiae-points belong to the same finger, the minimum value indicates that the fingerprints are definitely different.

Details about the String algorithm can be found in Jain et al. (1997). Briefly, let X be the template minutiae set. Let Y be the input minutiae set. For each minutia $x \in X$, the following algorithm is performed. For each $y \in Y$, x is aligned to y. After this alignment, x and y match perfectly. Let $A(x, y) = \{(x_i, y_i), x_i \in X, y_i \in Y : aligned(x_i, y_i) = true\}$ be the set of other couples of aligned minutiae. x_i and y_i are considered as aligned on the basis of a pre-defined "minutiae distance" not exceeding a certain fixed threshold. At the end of these loops, the value $\max_{x,y}\{|A(x,y)|\}$ is converted to the matching score by the formula:

$$score = \frac{\left(\max\{|A(x,y)|\}\right)^2}{|X| \cdot |Y|} \qquad \textbf{(1)}$$

It is worth noting that, in our system, the String algorithm is applied separately to the input-template minutiae extracted from the images provided by the optical and the capacitive sensors.

2.4 Fusion of the scores

Given the input fingerprint image associated with the claimed identity *i*:

1) Compute the matching score between the given fingerprint and the "template" fingerprint stored in the database and associated with the identity *i*. Let s_o and s_c be the matching scores provided by the matching algorithm applied to the images acquired from the optical and the capacitive sensors, respectively (Figure 1).
2) Apply the following transformation to the above scores s_o and s_c to implement the fusion:

$$s = f(s_o, s_c) \qquad \textbf{(2)}$$

3) Compare the obtained score value s with a threshold. The claimed identity is classified as "genuine user" if:

$$s > threshold \qquad (3)$$

otherwise it is classified as "impostor".

It is easy to see that the above methodology can also be used in the case of more than two matchers based on multiple sensors.

We used various score transformations according to eq. (1) to implement the fusion rule. In particular, the investigated fusion rules were: mean of the scores (Mean), product of the scores (Product), logistic transformation (Logistic).

The Logistic transformation is as follows:

$$s = \frac{1}{1 + \exp\left[-\left(w_0 + w_1 s_o + w_2 s_c\right)\right]} \qquad \textbf{(4)}$$

The "weights" of the logistic transformation were computed by a gradient descent algorithm with a cross-entropy loss function (Bishop, 1995), and by a class-separation loss function recently proposed in Marcialis and Roli (2003b). This class-separation loss function is the so-called "Fisher Distance" (FD):

$$FD = \frac{\left(\mu_g - \mu_i\right)^2}{\sigma_g^2 + \sigma_i^2} \qquad \textbf{(5)}$$

Where μ_g and μ_i are the mean values of the genuine and impostor matching scores, and σ_g^2 and σ_i^2 the related variances. It can be seen intuitively that *FD* allows to obtain a fusion rule explicitly aimed at increasing the separation between genuine and impostor classes (Marcialis and Roli, 2003b).

In the following, we have indicated the logistic fusion rule trained with the cross-entropy loss function as "Logistic-CE", and the logistic rule trained with FD as "Logistic-FD".

3 Experimental Results

3.1 Data Set

According to the FVC protocol (Maio et al., 2002), we created a data set containing 1,200 multisensor fingerprint images from 20 volunteers. We used the Biometrika FX2000 (312x372 pels images at 569 dpi) and the Precise Biometrics MC100 (250x250 pels images at 500 dpi) as optical and capacitive sensors. The forefingers, ringfingers and middle-fingers of both hands were acquired (six classes per person). According to the FVC protocol (Maio et al., 2002), the total number of classes (different fingerprints) is 6*20 = 120. Ten impressions of each finger were acquired, thus creating a data base containing 1,200 multi-sensor fingerprint images. Figure 1 also shows an example of optical and capacitive images of the same fingerprint.

3.2 The Evaluation Protocol

In our experiments, the following evaluation protocol was used:

- For each verification algorithm we computed two sets of scores. The first is the so-called "genuine-matching scores" set ***G***, made up of all matches among fingerprints of the same identity. A score from set ***G*** belongs to the "genuine user" class. The second set is the "impostor matching scores" set ***I***, made up of all matches among fingerprints of different identities. A score from set ***I*** belongs to the "impostor" class. The total number of genuine and impostor comparisons was 5,400 and 714,000, respectively[2].
- We randomly subdivided the above sets into two parts of the same size, so that: ***G***=***G1***U***G2***, ***I***=***I1***U***I2***. Sets ***G1*** and ***G2***, as well as ***I1*** and ***I2***, are disjoined.
- The training set ***Tr***={***G1***, ***I1***} was used to compute the weights of the logistic fusion rules.
- The test set ***Tx***={***G2***, ***I2***} was used to evaluate and compare the performances of algorithms
- Performances were assessed and compared in terms of:
    - o Equal Error Rate (EER), corresponding to the error rate computed at the threshold value for which the percentage of genuine users rejected by the system (FRR) is equal to the percentage of impostors accepted by the system (FAR);
    - o 1%FAR, which is the FRR when the FAR is fixed to 1%;

[2] For each class, the number of genuine comparisons is (10x9)/2=45. Therefore, we have 45*120=5,400 genuine comparisons. The number of impostors comparisons is 10x10x(120*119)/2=714,000.

- 1%FRR, which is the FAR when the FRR is fixed to 1%;
- Receiver Operating Characteristic (ROC) curves, which show FAR and FRR for various threshold values, according to Eq. (2).

1%FAR and 1%FRR measures were used to assess and compare the verification algorithms under the stringent requirements of many real applications. For example, with the 1%FRR performance measure it is possible to assess the degree of security of the system (i.e., the FAR of the system) when only 1% of genuine users can be rejected.

We also investigated “complementarity” among results provided by optical and capacitive sensors, in order to analyse to what extent the fingerprints wrongly recognized by one sensor can be recovered by fusion. This analysis pointed out the potentialities of optical and capacitive sensor fusion.

3.3 Results

The first two rows of Table 1 show the performances of matchers based on optical and capacitive sensors in terms of EER, 1%FAR, and 1%FRR. As can be expected, the optical sensor strongly outperformed the capacitive sensor. For the considered data set, this result is probably due to the fact that the acquisition area of the capacitive sensor is small, and it was not possible to characterise each fingerprint with a sufficient number of minutiae. For fusion purposes, such a large difference in performances among sensors is known to be an issue, as complex trainable fusion rules are usually required to obtain similar or higher performances than those of the best single sensor (Roli et al., 2002). Simple fusion rules, such as mean and product, suffer from differences in sensor accuracy, and usually provide worse results than the best single sensor, except for the case of sensors that are so “complementary” that errors in individual sensors can easily be compensated by fusion (Roli and Kittler, 2002; Roli et al., 2002). It is worth noting that fusion with mean and product rules therefore provided similar or slightly higher performances than those of the optical sensor (Table 1). This result suggests that optical and capacitive sensors are strongly complementary, and, remarkably, their complementarity can be exploited by simple fusion rules. In Section 3.4, we will analyse further the complementarity of the two sensors for decision fusion purposes. Improvements in EER over the optical sensor, of around 1%, were obtained with the two trainable fusion rules, Logistic-CE and Logistic-FD (Table 1). 1%FAR was decreased by 2% over the optical sensor by trainable fusion rules. Relevant improvements were obtained in terms of 1%FRR (more than 20% using the Logistic-FD fusion rule). It should be noted that these improvements in terms of 1%FAR and 1%FRR are particularly important for high security applications, and can justify the increases in cost and user cooperation required by multi sensor fusion.

Table 1. Error rates of individual and combined matchers in terms of EER, 1%FAR, and 1%FRR. The terms "Optical" and "Capacitive" refer to the matchers based on optical and capacitive sensors, respectively. The other terms (Product, Mean, Logistic-CE, Logistic-FD) indicate the fusion rules used to combine the optical and capacitive matchers.

	EER	**1%FAR**	**1%FRR**
Optical	3.4%	5.3%	33.0%
Capacitive	18.5%	39.2%	92.8%
Product	3.3%	5.5%	28.4%
Mean	2.9%	5.0%	22.5%
Logistic-CE	2.3%	3.2%	14.1%
Logistic-FD	2.2%	3.0%	12.9%

Figure 2 shows the ROC curves of the matcher based on the optical sensor (Optical), the best fixed fusion rule (Mean), and the best trainable fusion rule (Logistic-FD). The ROC curves of combined matchers are always better than those of the matcher based on an optical sensor. In particular, the ROC curve of the combined matcher based on the Logistic-FD fusion rule is significantly lower than those of the other matchers.

3.4 Complementarity between optical and capacitive sensors

In this section, we analyse complementarity between optical and capacitive sensors by investigating:

(a) the maximum "theoretical" verification accuracy, in terms of FAR and FRR, achievable by fusion of the two sensors;

(b) the degree of sensor complementarity in terms of percentages of fingerprints wrongly recognized by one of the sensors and "recovered" (i.e., correctly recognized) thanks to multi-sensor fusion.

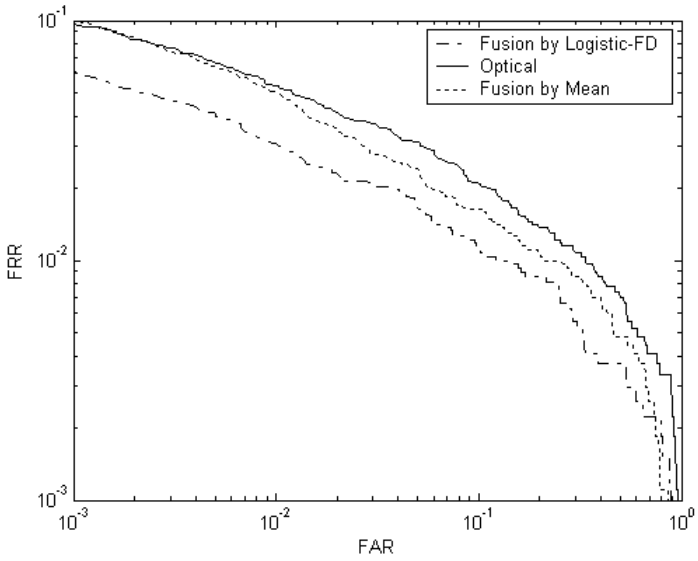

Figure 2. ROC curve of the matcher based on the optical sensor (Optical) and those of the combined matchers based on the Mean and Logistic-FD fusion rules.

In order to investigate point (a), we computed the verification accuracy of each matcher in terms of FAR and FRR on the test set. FAR and FRR were computed using the acceptance threshold $s*$ estimated on the training set at the EER point. We then assessed the "ideal" FAR($s*$) and FRR($s*$) that can be achieved using an "oracle" like fusion rule. With the term "oracle" we indicate the ideal fusion rule capable of selecting the matcher, if any, that correctly recognizes the input fingerprint. Performances of fusion with oracle were compared with those of the matchers based on the optical and capacitive sensors. Table 2 reports the results of our analysis. The second column reports the overall accuracy defined as :

$$OverallAccuracy(s^*) = 1 - \frac{N_i \cdot FAR(s^*) + N_g \cdot FRR(s^*)}{N_i + N_g} \quad \textbf{(6)}$$

where N_i and N_g are the number of impostor and genuine fingerprints in the test set.

Table 2. Comparison of performances on the test set, in terms of FAR, FRR, and overall accuracy, of the matchers based on the optical and capacitive sensors (Optical and Capacitive) with the theoretical performances achievable by the "oracle" fusion rule (Oracle).The EER threshold $s*$ estimated on the training set was used.

	Overall accuracy(s^*)	FAR(s^*)	FRR(s^*)
Optical	96.8%	3.2%	3.6%
Capacitive	81.5%	18.2%	18.8%
Oracle	99.3%	0.7%	1.3%

The results reported in Table 2 point out the strong complementarity between optical and capacitive sensors. In particular, the results of the "oracle" point out that fusion of the two sensors can potentially bring the error rate close to zero. Obviously, this is only a theoretical possibility, since the real performances of fusion rules based on the dynamic selection of matchers can only approximate the ideal oracle (Giacinto and Roli, 2001). Nevertheless, the analysis in Table 2 shows that fusion of the optical and the capacitive sensor could provide significant improvements in fingerprint verification performance, especially if effective algorithms for the dynamic selection of fingerprint matchers were developed (Giacinto and Roli, 2001).

Table 3 reports the results of the analysis of sensor complementarity in terms of the percentages of fingerprints wrongly recognized by one of the sensors and recovered by multi-sensor fusion. In other words, for each sensor and for the genuine and impostor classes, the values in Table 3 indicate the percentages of fingerprints in the test set that were correctly recognized thanks to multi sensor fusion.

The results in Table 3 clearly show the capability of all fusion rules to recover (i.e., correctly recognize) fingerprints that were wrongly recognized by the individual sensors. As an example, thanks to the Logistic-FD fusion rule, 98.7% of genuine fingerprints wrongly classified by the capacitive sensor were correctly recognized (Table 3).

Table 3. Percentages of genuine and impostor fingerprints wrongly recognized by one of the considered sensors and recovered, i.e., correctly recognized, by the different fusion rules (the term "recovery" rate is used to indicate these percentages). For each sensor, recovery rates are computed with respect to the maximum number of wrongly recognized genuine patterns (second and fourth columns) and impostor patterns (third and fifth columns) in the test set.

	Recovery Rate Optical Sensor		**Recovery Rate Capacitive Sensor**	
	Genuine	**Impostor**	**Genuine**	**Impostor**
Product	80.7%	82.8%	91.9%	89.9%
Mean	87.1%	91.7%	93.6%	86.7%
Logistic-FD	74.2%	60.9%	98.7%	96.1%
Logistic-CE	75.8%	70.7%	97.9%	94.3%

4 Conclusions

Although some information fusion approaches have already been investigated to improve current performances of fingerprint verification systems (Jain et al., 1999; Prabhakar and Jain, 2002; Marcialis and Roli, 2003a; Marcialis and Roli, 2003b; Ross et al., 2003; Ross and Jain, 2003), no previous work has explicitly studied the possibility of fusing the information provided by different imaging sensors. As discussed in the introduction, the integration of multiple fingerprint sensors offers some potential advantages that deserve to be investigated.

In this paper, a multi-sensor fingerprint verification system, based on the fusion of optical and capacitive sensors, has been presented. The reported results show that this multi-sensor system can improve the performances of the best individual sensor (the optical sensor). In particular, improvements in terms of 1%FAR and 1%FRR could justify the increase in system cost and user cooperation required by multi sensor fusion, especially for high security applications. The analysis of sensor complementarity reported in Section 3.4 points out the potentialities of this kind of multi-sensor fusion for fingerprint verification. Most verification errors made by individual sensors can be corrected by fusion (Table 3), and there is still room for further improvement (Table 2)

To sum up, we believe that this first work on multi-sensor fusion has shown the potentialities of this approach to fingerprint verification. Further theoretical work and experiments with other data bases are obviously necessary to investigate the conditions under which performance improvements provided by this kind of fusion can justify the increase in system cost and user cooperation.

References

Bishop, C.M., 1995. Neural Networks for Pattern Recognition. Oxford University Press.

Candela, G.T., Grother, P.J., Watson, C.I., Wilkinson, R.A., Wilson, C.L., 1995. PCASYS - A Pattern-Level Classification Automation System for Fingerprints, NIST tech. Report NISTIR 5647.

Giacinto G., Roli, F., 2001. Dynamic Classifier Selection Based on Multiple Classifier Behaviour.

Pattern Recognition 34 (9) 179-181.

Jain, A.K., Hong, L., Bolle, R., 1997. On-line Fingerprint Verification. IEEE Transactions on Pattern Analysis and Machine Intelligence 19 (4) 302-314.

Jain, A.K., Prabhakar, S., Chen, S., 1999. Combining Multiple Matchers for a High Security Fingerprint Verification System. Pattern Recognition Letters 20 (11-13) 1371-1379.

Kette, R., Zamperoni, P., 1996. Handbook of image processing operators. John Wiley and Sons.

Jain, A.K., Prabhakar, S., Hong, L., Pankanti, S., 2000. Filterbank-based Fingerprint Matching. IEEE Transactions on Image Processing 9 (5) 846-859.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L., Jain, A.K., 2002. FVC-2000: Fingerprint Verification Competition. IEEE Transactions on Pattern Analysis and Machine Intelligence 24 (3) 402-412.

Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S., 2003. Handbook of fingerprint recognition. Springer.

Marcialis, G.L., Roli, F., 2003a. Experimental results on Fusion of Multiple Fingerprint Matchers. Proc. 4th Int. Conf. on Audio and Video-Based Person Authentication AVBPA03, J. Kittler and M.S. Nixon Eds., Springer LNCS2688, pp. 814-820.

Marcialis, G.L., Roli, F., 2003b. Perceptron-based Fusion of Multiple Fingerprint Matchers. Proc. First Int. Work. on Artificial Neural Networks in Pattern Recognition ANNPR03, M. Gori and S. Marinai Eds., pp. 92-97.

Prabhakar, S., Jain, A.K., 2002. Decision-level Fusion in Fingerprint Verification. Pattern Recognition 35 (4) 861-874.

Roli, F., Kittler, J., 2002. Multiple Classifier Systems. Springer-Verlag, Lecture Notes in Computer Science, Vol. 2364.

Roli, F., Fumera, G., Kittler, J., 2002. Fixed and Trained Combiners for Fusion of Unbalanced Pattern Classifiers, Proc. Fifth Int. Conference on Information Fusion, pp. 278-284.

Ross, A., Jain, A.K., 2003. Information Fusion in Biometrics. Pattern Recognition Letters, 24 (13) 2115-2125.

Ross, A., Jain, A.K., Reisman, J., 2003. A Hybrid Fingerprint Matcher. Pattern Recognition, 36 (7) 1661-1673.

Xia, X., O'Gorman, L., 2003. Innovations in fingerprint capture devices. Pattern Recognition, 36 (2) 361-369.