Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Fuzzy Logic Concatenation in Fingerprint and Iris Multimodal Biometric Identification System

Prof. Kankrale R.N. , Prof. Mrs. Jawale M.A

Department of IT

SRESCOE Kopargaon,

Dist. Ahmednagar, Maharashtra, India

Abstract— This paper aims at concatenating two biometric features namely iris and fingerprint at decision level using Fuzzy logic. Multimodal biometric identification system to concatenate two or more physical traits to minimize False Accept Rate(FAR)and False Reject Rate (FRR). In greater detail, fuzzy logic based approach at decision level is used for concatenation and each biometric result is weighted for participate in final decision. Fuzzy logic is used for the effect of each biometric result combination. The proposed multimodal system achieves interesting results with several commonly used databases. For example, we have obtained an interesting working point with FAR = 0% and FRR=3.43% using entire CASIA Fingerprint and a randomly extracted same size subset of the CASIA Iris database.

Keywords— Fusion techniques, Fuzzy logic, Identification systems, Iris and Fingerprint biometry, Multimodal biometric systems.

I. INTRODUCTION

Biometric-based authentication systems represent a valid alternative to conventional approaches. Traditionally biometric systems, operating on a single biometric feature, have many limitations, which are as follows [1]. Trouble with data sensors: Captured sensor data are often affected by noise due to the environmental conditions (insufficient light, powder, etc.) or due to user physiological and physical conditions (cold, cut fingers, etc.). Distinctiveness ability: Not all biometric features have the same distinctiveness degree (for example, hand geometry-based biometric systems are less selective than the fingerprint-based ones). Lack of universality: All biometric features are universal, but due to the wide variety and complexity of the human body, not everyone is endowed with the same physical features and might not contain all the biometric features, which a system might allow.

Multimodal biometric systems are a recent approach developed to overcome these problems. These systems demonstrate significant improvements over unimodal biometric systems, in terms of higher accuracy and high resistance to spoofing. There is a sizeable amount of literature that details different approaches for multimodal biometric systems, which have been proposed [1]–[4]. Multibiometrics data can be combined at different levels: fusion at data-sensor level, fusion at the feature extraction level, fusion at the matching level, and fusion at the decision level. In this paper, a decision-level concatenation using fuzzy logic algorithm resulting in a unified biometric descriptor and integrating fingerprint and iris features is presented. At this kind of fusion, a separate decision is taken for each biometric type and then with weighting for each type result, final decision is accepted for final result. The paper is organized as follows. Section II illustrates the main techniques for multimodal biometric authentication systems. Section III describes the proposed multimodal authentication system. Section IV shows the achieved experimental results. Finally, a conclusion is reported in Section V.

II. MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEMS

Fusion strategies can be divided into two main categories: premapping fusion (before the matching phase) and post mapping fusion (after the matching phase). The first strategy deals with the feature-vector fusion level [8]. Usually, these techniques are not used because they result in many implementation problems [1]. The second strategy is realized through fusion at the decision level, based on some algorithms, which combine single decisions for each component of the system. Furthermore, the second strategy is also based on the matching-score level, which combines the matching scores of each component system. The biometric data can be combined at several different levels of the identification process. Input can be fused in the following levels [1], [5].

- *Data-sensor level:* Data coming from different sensors can be combined, so that the resulting information are in some sense better than they would be possible when these sources were individually used. The term better in that case can mean more accurate, more complete, or more dependable.
- *Feature-extraction level*: The information extracted from sensors of different modalities is stored in vectors on the basis of their modality. These feature vectors are then combined to create a joint feature vector, which is the basis for the matching and recognition process. One of the potential problems in this strategy is that, in some cases, a very high-dimensional feature vector results from the fusion process. In addition, it is hard to generate homogeneous feature vectors from different biometrics in order to use a unified matching algorithm.

- *Matching-score level*: This is based on the combination of matching scores, after separate feature extraction and comparison between stored data and test data for each subsystem have been compiled. Starting from the matching scores or distance measures of each subsystem, an overall matching score is generated using linear or nonlinear weighting.
- *Decision level:* With this approach, each biometric subsystem completes autonomously the processes of feature extraction, matching, and recognition. Decision strategies are usually of Boolean functions, where the recognition yields the majority decision among all present subsystems. Fusion at template level is very difficult to obtain, since biometric features have different structures and distinctiveness.

III. PROPOSED MULTIMODAL BIOMETRIC SYSTEM

In this paper, a multimodal biometric system, based on fingerprint and iris characteristics, is proposed [4]. As shown in Fig. 1, the proposed multimodal biometric system is composed of two main stages: the preprocessing stage and matching stage. Multibiometric offers many advantages like 1)significantly improving the accuracy of biometric identification or verification;2)providing certain degree of flexibility for some unusable biometric traits; and 3)resisting proof attacks due to difficulty in spoofing multiple biometric sources. The system is composed of number of subsystems, which corresponds to fingerprint recognition and iris recognition, matching using hamming distance. Once matching scores are generated they are normalized using max- min method and then fused by sum rule based fusion. Fuzzy logic is used as decision level.

A. Individual Recognizers

Iris and fingerprint biometric perform better as compared to other available traits due to their accuracy, reliability and simplicity. These properties make iris and fingerprint recognition particularly promising solution to the society. The process starts with preprocessing of the acquired images which removes the effect of noise. Further, feature are extracted for the training and testing images and matched to find the similarity between two feature sets. The matching scores are generated from the individual recognizer are passed to the decision module where person is declared as genuine or an imposter.

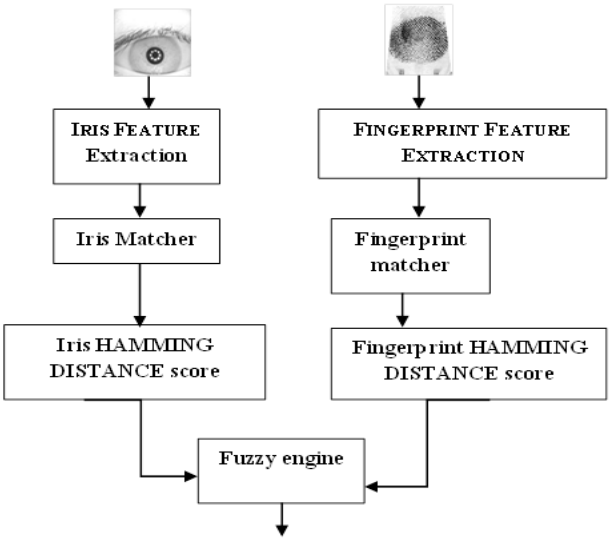

Fig: 1. Proposed Multimodal System

B. Iris Recognition

Iris is unique to each individual and remains constant over the life of a person. The eyeball has a circular black disk in the center known as pupil. The pupil dilates when exposed to light and contracts in dark. Thus the size of pupil varies with respect to light it is exposed to. The iris is the annular ring between the sclera and pupil boundary and contains the flowery pattern unique to each individual. This texture information unique to each individual is extracted from rest of the eye image and is transformed into strip to apply pattern matching algorithm between the database and query images of iris. Automated iris recognition system has been proposed by Flom and Safir [10]. The concept of multi-scale quadrature wavelets is used to extract texture phase structure information of the iris, to generate a 2048 bit iriscode and compares the difference between a pair of iris representations by computing their Hamming distance using XOR operator [4]. The important steps involved in iris recognition are:

1. Pupil Detection
2. Iris Detection
3. Normalization
4. Feature Extraction
5. Matching

1. Pupil Detection

Pupil is the darkest portion of the eye and is detected and removed from the rest of the eye image so that only iris pattern can be used for matching. The first step involved in pupil detection is to find the contours of the acquired iris image. Since the pupil region contains the lowest intensity values its edges can be formed easily. After edge detection the next step is to find the center of the pupil. Thus the process starts with dilating the edge detected image and the dilated image with filled pupil circle is used to find the Euclidean distance between the non-zero points. By computing the distance between non-zero points the spectrum showing the largest filled circle can be formed within the set of pixels. Since the pupil is the largest filled circle in the image the overall intensity of the spectrum peaks in at the center. This spectrum image can be used to compute the center of the pupil. The pixel position having the maximum value in the spectrum image corresponds to the pupil center. The radius of the pupil is the distance between the pupil center and nearest non-zero pixel.

2. Iris Detection

To find the outer iris boundary intensity variation approach is used. In this approach concentric circles of different radii are drawn from the detected center. The circle having maximum change in intensity with respect to previous drawn circle is iris circle. The approach works fine for iris images having sharp variation between iris boundary and sclera. The radius of iris and pupil boundary is used to transform the annular portion to a rectangular block, known as strip.

3. Normalization

The localized iris image is transformed into strip. The mapping is done after transforming the Cartesian coordinates into its polar equivalent using

$$I(x(\rho,\theta), y(\rho,\theta)) \rightarrow I(\rho,\theta)$$

with

$$\begin{cases} x_p(\rho,\theta) = x_{\rho 0}(\theta) + r_p * \cos(\theta) \\ y_p(\rho,\theta) = y_{\rho 0}(\theta) + r_p * \sin(\theta) \\ x_i(\rho,\theta) = x_{i0}(\theta) + r_i * \cos(\theta) \\ y_i(\rho,\theta) = x_{i0}(\theta) + r_i * \sin(\theta) \end{cases} \quad (1)$$

where rp and ri are respectively the radius of pupil and the iris in equation (1), while (xp(θ), yp(θ)) and (xi(θ), yi(θ)) are the coordinates of the pupillary and limbic boundaries in the direction θ. The value of θ belongs to [0; 2π], ρ belongs to [0; 1].

The transformed iris image consists of points taken from the pupil boundary to the outer iris boundary. Thus the same set of points is taken for every image. The iris image is normalized so that the size of strip does not vary for different images. The size of same iris image may vary due to expansion and dilation of pupil. Thus the size of iris strip is fixed for every iris image. In this experiment the size of strip is 80×360 pixels.

4. Feature Extraction

Features are the attributes or values extracted to get the unique characteristics from the image. Features from the iris image are extracted using Haar Wavelet decomposition process [9]. In the wavelet decomposition the image is decomposed into four coefficient i.e., horizontal, diagonal, vertical and approximation. The approximation coefficients are further decomposed into four coefficients. The sequences of steps are repeated for five levels and the last level coefficients are combined to form a vector. The combined vector is binarized to allow easy comparisons between the iris codes for database and query image.

$$IC(i) = \begin{cases} 1 & FV(i) \geq 0 \\ 0 & FV(i) < 0 \end{cases} \quad (2)$$

The binarized feature vectors are passed to the matching module to allow comparisons.

5. Matching

The comparison is done between iris codes (IC) generated for database and query images using hamming distance approach. In this approach the difference between the bits of two codes are counted and the number is divided by the total number of comparisons.

$$MS_{Iris} = \frac{1}{N} \sum_{i=1}^{N} A_i \oplus B_i \quad (3)$$

where A is the binary vector (iris code) for database image and B is the binary vector for query image while N is the number of elements. After comparing extracted code of a new iris image with codes in database and hamming distance algorithm, the code with minimum difference can be found which can be accepted consequently and save the difference number for an input in our fuzzy logic engine.

C. Fingerprint Recognition

Fingerprint is one of the most widely used biometric modality. The main reason behind the use of fingerprint biometric is that it is the most proven technique to identify the individual. The fingerprint is basically the combination of

ridges and valleys on the surface of the finger. The systematic study on the ridge, furrow, and pore structure in fingerprints has been published in [5]. The use of minutiae feature for single fingerprint classification has been introduced in [4]. A system on fingerprint classification is discussed in [2] [3]. The major steps involved in fingerprint recognition using minutiae matching approach after image acquisitions are:

1. Image Enhancement
2. Minutiae Extraction
3. Matching

1. Image Enhancement

A fingerprint image is corrupted due to various kinds of noises such as creases, smudges and holes. It is almost impossible to recover the true ridge/valley structures from the unrecoverable regions; any effort to improve the quality of the fingerprint image in these regions may be futile. Therefore, any well-known enhancement algorithm may be used to improve the clarity of ridges/valley structures of fingerprint images in recoverable regions and to mask out the unrecoverable regions. The steps involved in image enhancement are given in [3]. The process starts with normalization of input fingerprint image so that it has pre-specified mean and variance. The orientation image is estimated from the normalized input fingerprint image. Further, frequency image is computed from the normalized input fingerprint image and the estimated orientation image. After computation of frequency image the region mask is obtained by classifying each block in the normalized input fingerprint image into a recoverable or unrecoverable block. Lastly, a bank of Gabor filters which is tuned to local ridge orientation and ridge frequency is applied to the ridge and valley pixels in the normalized input fingerprint image to obtain an enhanced fingerprint image.

2. Minutiae Extraction

The enhanced fingerprint image is binarized and submitted to the thinning algorithm which reduces the ridge thickness to one pixel wide. The skeleton image is used to extract minutiae points which are the points of ridge endings and bifurcations. The location of minutiae points along with the orientation is extracted and stored to form feature set. For extraction of minutiae points eight connected pixels are used [3]. The Crossing Number (CN) method is used to perform minutiae extraction. This method extracts the ridge endings and bifurcations from the skeleton image by examining the local neighborhoods of each ridge pixel using a 3×3 window. The CN for a ridge pixel P is given by

$$CN = 0.5\sum_{i=1}^{8} | P_i - P_{i+1} | \qquad (4)$$

P9 = P1

where Pi is the pixel value in the neighborhoods of P. After the CN for a ridge pixel has been computed, the pixel can then be classified according to its CN value. A ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation. For each extracted minutiae point, the following information is recorded:

- x and y coordinates,
- Orientation of the associated ridge segment, and
- Type of minutiae (ridge ending or bifurcation)

3. Matching

In identification phase after obtaining 128 bits code from new fingerprint image, and comparing it against hamming distance with codes in database and finding the code with minimum difference, it is accepted consequently and saves the difference number for one input in our fuzzy logic engine.

D. Multi-Biometric Method

This paper presents a novel fusion strategy for personal identification using fingerprint and iris at the decision level fusion scheme. It is also shown that integration of fingerprint and iris biometrics can achieve higher performance than using each single biometric alone. A fuzzy logic method is used for fusion which is given better performance and accuracy. Hamming distance and fuzzy logic are used for comparing and deciding to verification.

1. Fuzzy logic (FL)

Fuzzy logic is a kind of soft computing, which mimics human decision making. In this paper, fuzzy logic decision fusion is used and gives reasonable results. The general block diagram for FL is shown in figure 2. Fuzzification is the process of each input convert to linguistic variable. One or more membership function with a degree of membership function is obtained from linguistic variables. The degrees of membership function based on predefined rules and rule weights are combined and the output is produced. Each rule can be given a weight to show the influence of the particular rule on the output.

Fig. 2. Fuzzy logic block diagram

In this paper, fuzzy logic is used for fusion at decision level. The fuzzy engine has two inputs, one of them named fig and the other iris. Fig considered as fingerprint results in identification and iris considered as iris result identification. The figure below shows them:

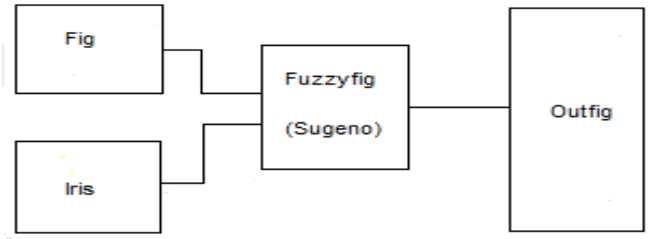

Fig. 3. Membership function

In the previous fusion methods, each single biometrics has same weight, but some biometrics have more features and more stability. It is better that biometric with more features will have more chance to participate. Iris has more features than fingerprint and also more stability. It is also more resistant against cheating and copying. So in this paper, iris has more weight in fusion with fingerprint and this is one of the reasons that we get better results.

2. Fusion by Fuzzy Logic Decision

Fuzzy logic enables us to process iambuses information in a way like human thinking, i.e. big versus small or high versus low. It makes intermediate values to be defined between true and false by partial set memberships. As an initial step, we consider fuzzy variables and fuzzy sets in a fuzzy inference system for iris and fingerprint images. Using fuzzy logic for fusion at decision level has many advantages like soft inputs while the crisp outputs are achieved. Fuzzy system used in this paper with simplest way gives an excellent result. This system gives an acceptable percentage output for every acceptable range of inputs for which using a threshold for the best states are accepted.

3. Fuzzy Inference System

The fuzzy inference system adjusts the weighting for each biometric as affected by the differences between hamming code. There are two input fuzzy variables, one for fingerprint (fig) and one for iris (iris).). Each input variable has a fuzzy set that defines each variable. As seen in figure 4 trapezoidal membership function is used. There is one output fuzzy variables (outfig), which corresponds to the weightings for iris and fingerprint verification. This MF accept %100 input number 0 to 3 and input number 15 with %0. This means that input fingerprint with 3 bits difference accepted with %100 and fingerprint with 15 bits difference accepted %0 and normalize numbers 3 to 15 with %100 to %0. For example, fingerprint with 5 bit difference is accepted by %84 and with 10 bit difference by %44. Now we normalize these acceptation rates (%0 … %100) to (%0 … %20). This is because of weighting fingerprint code as 20. Triangular membership function is used for input.

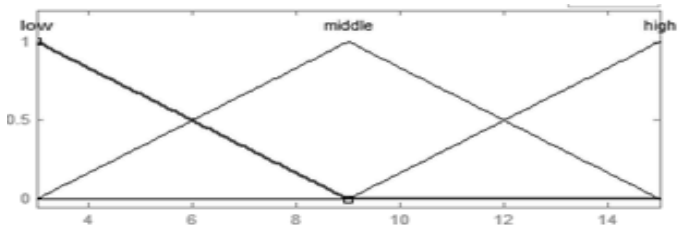

Fig. 4. Triangular membership functions for fingerprint code.

4. Fuzzy Rules

The conditions that comprise the fuzzy logic are formulated by two groups of fuzzy IF-THEN rules. One group controls the output variable finger (weighting for the fingerprint biometric) according to values of the input variables. The other group controls the output variable iris (weighting of iris biometric) according to the values of the input variables. We could find the experimental numbers (3) for high level and (15) for low level acceptation. These numbers are the differences between acquired code and the code in database with hamming distance. Number (3) means that fingerprint code has three bits differences with the code in database and Number (15) means code with 15 bits differences. Numbers 0 to 3 are accepted as real and numbers 15 and up is not acceptable fingerprint code. Now normalize these acceptation rates(%0 … %100) to (%0 … %20). This is because of weighting fingerprint code as 20. The other MF used for iris accepts % 100 input numbers 0 to 40 and input number 400 with %0. This means that input iris to 40 bits difference is accepted with %100 and iris with 400 bits difference is accepted %0 and normalizes numbers 40 to 400 with %100 to %0. Now normalize these acceptation rates (%0 … %100) to (%0 … %80). This is because of weighting iris code as 80. Triangular membership function and sugeno fazzification are used in this fuzzy system.

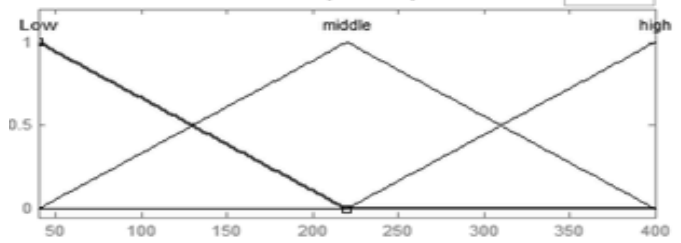

Fig. 5. Triangular membership function for iris code

The main properties in the fuzzy rules are: If (fig is low) and (iris is low) then (OR is Very Low) If (fig is low) and (iris is middle) then (OR is middle) If (fig is low) and (iris is high) then (OR is Very Good) If (fig is middle) and (iris is low) then (OR is Low) If (fig is middle) and (iris is middle) then (OR is Good) If (fig is middle) and (iris is high) then (OR is Very Good) If (fig is high) and (iris is low) then (OR is Middle) If (fig is high) and (iris is middle) then (OR is Very Good) If (fig is high) and (iris is high) then (OR is Excellent) It is also the same for iris code and the experimental numbers we found (40) for high level and (400) for low level acceptation. These numbers are the differences between acquired code and the code in database with hamming distance. Number (40) means iris code has forty bits differences with the code in database and Number (400) means code with 400 bits differences. Numbers 0 to 40 are accepted as real and number 400 and up is not acceptable iris code.

IV. EXPERIMENTAL RESULTS

The proposed multimodal biometric system achieves interesting results on standard and commonly used databases. To show the effectiveness of our approach, the CASIA database [6] has been used for fingerprints and irises. The obtained experimental result of recognition rates is here outlined. Table I gives a brief description of the features and result of the used databases. The CASIA-Iris-Interval database has been generated with self-developed camera with 249 user and 395 classes (left eye and right eye image) in iris database [6]. The reduced CASIA-Iris-Interval-A1, CASIA-Iris-Interval-A2 and CASIA-Iris-Interval-A3 database has been generated with fifty user random extractions for each from the full iris database. For each user, the first ten iris acquisitions have been selected.CASIA-FingerprintV5 (000-009)-S1 database has been generated considering the first 10 users, CASIA-FingerprintV5 (000-009)-S2 database has been generated considering the users from 25 to 35 and CASIA-FingerprintV5 (000-009)-S3 database has been generated considering users from 75 to 85. The multimodal recognition system performance evaluation has been performed using the well-known FRR and FAR indexes. For an authentication system, the FAR is the number of times that an incorrectly accepted unauthorized access occurred, while the FRR is the number of times that an incorrectly rejected authorized access resulted. Several test sets considering the appropriate number of fingerprint and iris acquisitions have been generated to test the proposed multimodal approach. Table I shows the used test sets composition and the achieved results in terms of FAR and FRR indexes.

Table I: Recognition Analysis of Multimodal System

Unimodal System	FAR	FRR
S1	1.0%	11.00%
S2	1.0%	12.1%
S3	0.0%	10.00%
A1	2.0%	13.00%
A2	3.0%	11.00%
A3	0.0%	15.00%
Multimodal System	FAR	FRR
A1+S1	0%	4.14%
A2+S2	0%	8.27%
A3+S3	0%	3.43%

V. CONCLUSION

For an ideal authentication system, FAR and FRR indexes are equal to 0. The aforementioned result may be reached by online biometric authentication systems, because they have the freedom to reject the low-quality acquired items. On the contrary, official ready-to-use databases (FVC databases, CASIA, BATH, etc.) contain images with different quality, including low-, medium-, and high-quality biometric acquisitions, as well as partial and corrupted images. For this reason, these biometric authentication systems do not achieve the ideal result. To increase the related security level, system parameters are then fixed in order to achieve the FAR = 0% point and a corresponding FRR point. The multimodal biometric system has been tested on different congruent datasets obtained by the official CASIA database [6]. In this paper, a multi- modal biometric system (Fingerprint & Iris) is used after converting fingerprint and iris image to a binary code, with decision level fusion combining the results. Fingerprint code is weighed as 20% and iris code as 80%. Using fingerprint and iris as multi-modal gives better result than other modalities. Using fuzzy logic and weighted code gives flexible result. An efficient method in fingerprint encoding is used and the fuzzy logic framework incorporates iris and fingerprint .

REFERENCES

[1] A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems IEEE transactions on systems, man, and cybernetics—part c: applications and reviews, vol. 40, no.4,july2010.

[2] S.Vasuhi. V.Vaidehi, N.T.Naresh Babu, Teena Mary Treesa. An Efficient Multi-modal Biometric Person Authentication System Using Fuzzy Logic. IEEE 978-1-61284-260-8/10. 2010.
[3] Dr. Shubhamgi D C, Manohar Bali. "Multi-Biometric Approaches to Face and Fingerprint Biometrics", International Journal of Engineering Research & Technology. 2278-0181. 2012.pp
[4] Mohamad Abdolahi, Majid Mohamadi and Mehdi Jafari "Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013, pp.504-510.
[5] V. Conti, G. Milici, P. Ribino, S. Vitabile, and F. Sorbello, "Fuzzy fusion in multimodal biometric systems," in Proc. 11th LNAI Int. Conf. Knowledge.-Based Intell. Inf. Eng. Syst. (KES 2007/WIRN 2007), Part I LNAI 4692. B. Apolloni et al., Eds. Berlin, Germany: Springer-Verlag, 2010, pp. 108–115.
[6] http://biometric.idealtest.org/download/ CASIA Iris Image Database Version 4 and CASIA-FingerprintV5/,access date May 15, 2011.
[7] R. C. Gonzalez and R. E. Woods, Digital Image Processing. Englewood Cliffs, NJ: Prentice-Hall, 2008, pp. 362-458.
[8] A. Ross, & A. K. Jain, Information Fusion in Biometrics, Pattern Recognition Letters, 24(13), 2003, pp.2115-2125.
[9] A. K. Jain, K. Nandakumar, & A. Ross, Score Normalization in multimodal biometric systems. The Journal of Pattern Recognition Society, 38(12), 2005, pp.2270-2285.
[10] L. Flom, & A. Safir, Iris Recognition System, U.S. Patent No. 4641394, 1987.

