A SURVEY OF BIOMETRIC RECOGNITION METHODS

Kresimir Delac [1], Mislav Grgic [2]

[1] HT - Croatian Telecom, Carrier Services Department, Kupska 2, Zagreb, CROATIA
[2] University of Zagreb, FER, Unska 3/XII, Zagreb, CROATIA
E-mail: kresimir.delac@ht.hr

Abstract: *Biometric recognition refers to an automatic recognition of individuals based on a feature vector(s) derived from their physiological and/or behavioral characteristic. Biometric recognition systems should provide a reliable personal recognition schemes to either confirm or determine the identity of an individual. Applications of such a system include computer systems security, secure electronic banking, mobile phones, credit cards, secure access to buildings, health and social services. By using biometrics a person could be identified based on "who she/he is" rather then "what she/he has" (card, token, key) or "what she/he knows" (password, PIN). In this paper, a brief overview of biometric methods, both unimodal and multimodal, and their advantages and disadvantages, will be presented.*

Keywords: *Biometrics, Multimodal Biometrics, Recognition, Verification, Identification, Security*

1. INTRODUCTION

The term *biometric* comes from the Greek words *bios* (life) and *metrikos* (measure). It is well known that humans intuitively use some body characteristics such as face, gait or voice to recognize each other. Since, today, a wide variety of applications require reliable verification schemes to confirm the identity of an individual, recognizing humans based on their body characteristics became more and more interesting in emerging technology applications. Traditionally, passwords and ID cards have been used to restrict access to secure systems but these methods can easily be breached and are unreliable. Biometric can not be borrowed, stolen, or forgotten, and forging one is practically impossible.

2. BIOMETRIC SYSTEMS

A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses [1]. That feature vector is usually stored in a database (or recorded on a smart card given to the individual) after being extracted. A biometric system based on a physiological characteristics is generally more reliable than one which adopts behavioral characteristics, even if the latter may be more easy to integrate within certain specific applications. Biometric system can than operate in two modes: *verification* or *identification*. While identification involves comparing the acquired biometric information against templates corresponding to all users in the database, verification involves comparison with only those templates corresponding to the claimed identity. This implies that identification and verification are two problems that should be dealt with separately.

A simple biometric system consists of four basic components:

1) *Sensor module* witch acquires the biometric data;
2) *Feature extraction module* where the acquired data is processed to extract feature vectors;
3) *Matching module* where feature vectors are compared against those in the template;
4) *Decision-making module* in which the user's identity is established or a claimed identity is accepted or rejected.

Any human physiological or behavioral trait can serve as a biometric characteristic as long as it satisfies the following requirements:

1) *Universality*. Everyone should have it;
2) *Distinctiveness*. No two should be the same;
3) *Permanence*. It should be invariant over a given period of time;
4) *Collectability*.

In real life applications, three additional factors should also be considered: *performance* (accuracy, speed, resource requirements), *acceptability* (it must be harmless to users), and *circumvention* (it should be robust enough to various fraudulent methods).

3. OVERVIEW OF COMMONLY USED BIOMETRICS

Since there are number of biometric methods in use (some commercial, some "not yet"), a brief overview of various biometric characteristics will be given, starting with newer technologies and then progressing to older ones [2]:

Infrared thermogram (facial, hand or hand vein). It is possible to capture the pattern of heat radiated by the human body with an infrared camera. That pattern is considered to be unique for each person. It is a noninvasive method, but image acquisition is rather difficult where there are other heat emanating surfaces near the body. The technology could be used for covert recognition. A related technology using near infrared imaging is used to scan the back of a fist to determine hand vein structure, also believed to be unique. Like face recognition, it must deal with the extra issues of three-dimensional space and orientation of the hand. Set-back is the price of infrared sensors.

Gait. This is one of the newer technologies and is yet to be researched in more detail. Basically, gait is the peculiar way one walks and it is a complex spatio-temporal biometrics. It is not supposed to be very distinctive but can be used in some low-security applications. Gait is a behavioral biometric and may not remain the same over a long period of time, due to change in body weight or serious brain damage. Acquisition of gait is similar to acquiring a facial picture and may be an acceptable biometric. Since video-sequence is used to measure several different movements this method is computationally expensive.

Keystroke. It is believed that each person types on a keyboard in a characteristic way. This is also not very distinctive but it offers sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioral biometric; for some individuals, one could expect to observe large variations in typical typing patterns. Advantage of this method is that keystrokes of a person using a system could be monitored unobtrusively as that person is keying information. Another issue to think about here is privacy.

Odor. Each object spreads around an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. This would be done with an array of chemical sensors, each sensitive to a certain group of compounds. Deodorants and parfumes could lower the distinctiveness.

Ear. It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. Matching the distance of salient points on the pinna from a landmark location of the ear is the suggested method of recognition in this case. This method is not believed to be very distinctive.

Hand geometry. The essence of hand geometry is the comparative dimensions of fingers and the location of joints, shape and size of palm. One of the earliest automated biometric systems was installed during late 60s and it used hand geometry and stayed in production for almost 20 years. The technique is very simple, relatively easy to use and inexpensive. Dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy. Since hand geometry is not very distinctive it cannot be used for identification of an individual from a large population, but rather in a verification mode. Further, hand geometry information may not be invariant during the growth period of children. Limitations in dexterity (arthritis) or even jewelry may influence extracting the correct hand geometry information. This method can find its commercial use in laptops rather easy. There are even verification systems available that are based on measurements of only a few fingers instead of the entire hand. These devices are smaller than those used for hand geometry.

Fingerprint. A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy was very high [3]. Patterns have been extracted by creating an inked impression of the fingertip on paper. Today, compact sensors provide digital images of these patterns. Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse. Since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners. Solid state sensors overcome this and other technical difficulties because the coated silicon chip itself is the sensor. Solid state devices use electrical capacitance to sense the ridges of the fingerprint and create a compact digital image. Today, a fingerprint scanner costs about 20 USD and has become affordable in a large number of applications (laptop computer). In real-time verification systems, images acquired by sensors are used by the feature extraction module to compute the feature values. The feature values typically correspond to the position and orientation of certain critical points known as minutiae points [4]. The matching process involves comparing the two-dimensional minutiae patterns extracted from the user's print with those in the template. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources.

Face. Facial images are the most common biometric characteristic used by humans to make a personal recognition, hence the idea to use this biometric in technology. This is a nonintrusive method and is suitable for covert recognition applications. The applications of facial recognition range from static ("mug shots") to dynamic, uncontrolled face identification in a cluttered background (subway, airport). Face verification involves extracting a feature set from a two-dimensional image of the user's face and matching it with the template stored in a database. The most popular approaches to face recognition are based on either: 1) the location and shape of facial attributes such as eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces [2]. Although performance of commercially available systems is reasonable there is still significant room for improvement since false reject rate (FRR) is about 10% and false accept rate (FAR) is 1% [5]. These systems also have difficulties in recognizing a face from images captured from two different angles and under different ambient illumination conditions. It is questionable if a face itself is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence [6]. Facial recognition system should be able to automatically detect a face in an image, extract its features and then recognize it from a general viewpoint (i.e., from any pose) which is a rather difficult task. Another problem is the fact that the face is a changeable social organ displaying a variety of expressions.

Retina. Retinal recognition creates an "eye signature" from the vascular configuration of the retina which is supposed to be a characteristic of each individual and each eye, respectively. Since it is protected in an eye itself, and since it is not easy to change or replicate the retinal vasculature, this is one of the most secure biometric. Image acquisition requires a person to look through a lens at an alignment target, therefore it implies cooperation of the subject. Also retinal scan can reveal some medical conditions and as such public acceptance is questionable.

Iris. The iris begins to form in the third month of gestation and the structures creating its pattern are largely complete by the eight month. Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette [7]. Iris scanning is less intrusive than retinal because the iris is easily visible from several meters away. Responses of the iris to changes in light can provide an important secondary verification that the iris presented belongs to a live subject. Irises of identical twins are different, which is another advantage. Newer systems have become more user-friendly and cost-effective. A careful balance of light, focus, resolution and contrast is necessary to extract a feature vector from localized image. While the iris seems to be consistent throughout adulthood, it varies somewhat up to adolescence.

Palmprint. Like fingerprints, palms of the human hands contain unique pattern of ridges and valleys. Since palm is larger then a finger, palmprint is expected to be even more reliable than fingerprint. Palmprint scanners need to capture larger area with similar quality as fingerprint scanners, so they are more expensive. A highly accurate biometric system could be combined by using a high-resolution palmprint scanner that would collect all the features of the palm such as hand geometry, ridge and valley features, principal lines, and wrinkles.

Voice. The features of an individual's voice are based on physical characteristics such as vocal tracts, mouth, nasal cavities and lips that are used in creating a sound. These characteristics of human speech are invariant for an individual, but the behavioral part changes over time due to age, medical conditions and emotional state. Voice recognition techniques are generally categorized according to two approaches: 1) Automatic Speaker Verification (ASV) and 2) Automatic Speaker Identification (ASI). Speaker verification uses voice as the authenticating attribute in a two-factor scenario. Speaker identification attempts to use voice to identify who an individual actually is. Voice recognition distinguishes an individual by matching particular voice traits against templates stored in a database. Voice systems must be trained to the individual's voice at enrollment time, and more than one enrollment session is often necessary. Feature extraction typically measures formants or sound characteristics unique to each person's vocal tract. The pattern matching algorithms used in voice recognition are similar to those used in face recognition.

Signature. Signature is a simple, concrete expression of the unique variations in human hand geometry. The way a person signs his or her name is known to be characteristic of that individual. Collecting samples for this biometric includes subject cooperation and requires the writing instrument. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of a subject. In addition to the general shape of the signed name, a signature recognition system can also measure pressure and velocity of the point of the stylus across the sensor pad.

DNA. Deoxyribonucleic acid (DNA) is probably the most reliable biometrics. It is in fact a one-dimensional code unique for each person. Exception are identical twins. This method, however, has some drawbacks: 1) contamination and sensitivity, since it is easy to steal a piece of DNA from an individual and use it for an ulterior purpose, 2) no real-time application is possible because DNA matching requires complex chemical methods involving expert's skills, 3) privacy issues since DNA sample taken from an individual is likely to show susceptability of a person to some diseases. All this limits the use of DNA matching to forensic applications.

It is obvious that no single biometric is the "ultimate" recognition tool and the choice depends on the application. A brief comparison of the above techniques based on seven factors described in section 2 is provided in Table I [2].

Table I Comparison of various biometric technologies [2]

Biometric characteristic	**Universality**	**Distinctiveness**	**Permanence**	**Collectabillity**	**Performance**	**Acceptability**	**Circumvention**
Facial thermogram	H	H	L	H	M	H	L
Hand vein	M	M	M	M	M	M	L
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Ear	M	M	H	M	M	H	M
Hand geometry	M	M	M	H	M	M	M
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
Retina	H	H	M	L	H	L	L
Iris	H	H	H	M	H	L	L
Palmprint	M	H	H	M	H	M	M
Voice	M	L	L	M	L	H	H
Signature	L	L	L	H	L	H	H
DNA	H	H	H	L	H	L	L

4. BIOMETRIC SYSTEM PERFORMANCE

Due to different positioning on the acquiring sensor, imperfect imaging conditions, environmental changes, deformations, noise and bad user's interaction with the sensor, it is impossible that two samples of the same biometric characteristic, acquired in different sessions, exactly coincide. For this reason a biometric matching systems' response is typically a matching score *s* (normally a single number) that quantifies the similarity between the input and the database template representations. The higher the score, the more certain the system is that the two samples coincide [1]. A similarity score *s* is compared with an acceptance threshold *t* and if *s* is greater than or equal to *t* compared samples belong to a same person. Pairs of biometric samples generating scores lower than *t* belong to a different person. The distribution of scores generated from pairs of samples from different persons is called an *impostor distribution*, and the score distribution generated from pairs of samples of the same person is called a *genuine distribution*, Figure 1 [1].

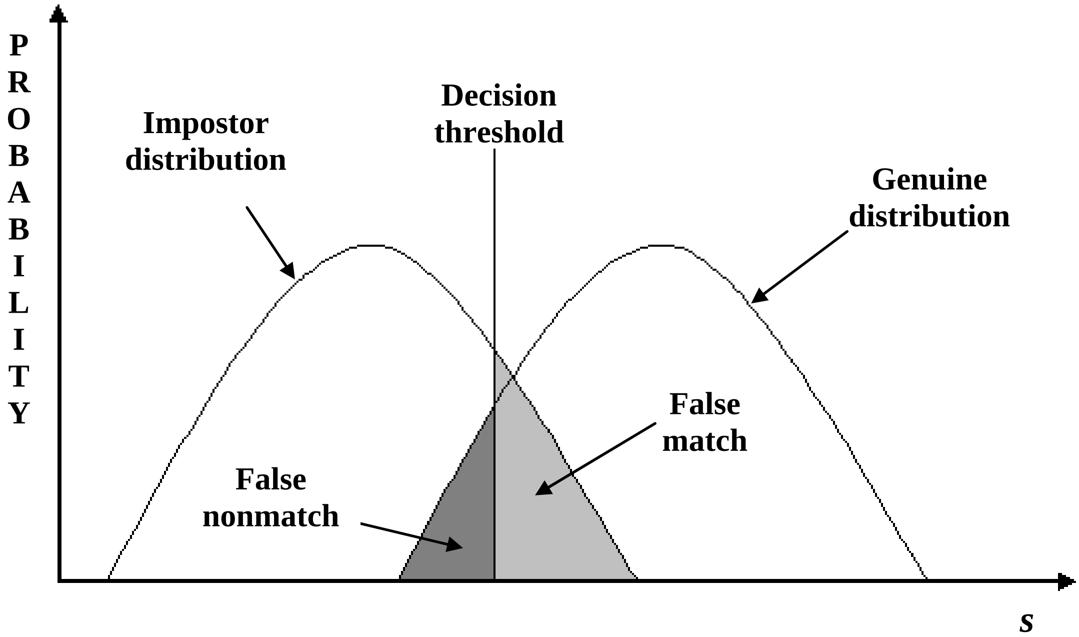

Fig. 1. Biometric system error rates [1]

The main system errors are usually measured in terms of:

- FNMR (*false nonmatch rate*) – mistaking two biometrics measurements from the same person to be from two different persons;
- FMR (*false match rate*) – mistaking biometric measurement from two different persons to be from the same person.

FNMR and FMR are basically functions of the system threshold *t*: if the system's designers decrease *t* to make the system more tolerant to input variations and noise, FMR increases. On the other hand, if they raise *t* to make the system more secure, FNMR increases accordingly [1]. FMR and FNMR are brought together in a receiver operating characteristic (ROC) curve that plots the FMR against FNMR (or 1-FNMR) at different thresholds, Figure 2 [1].

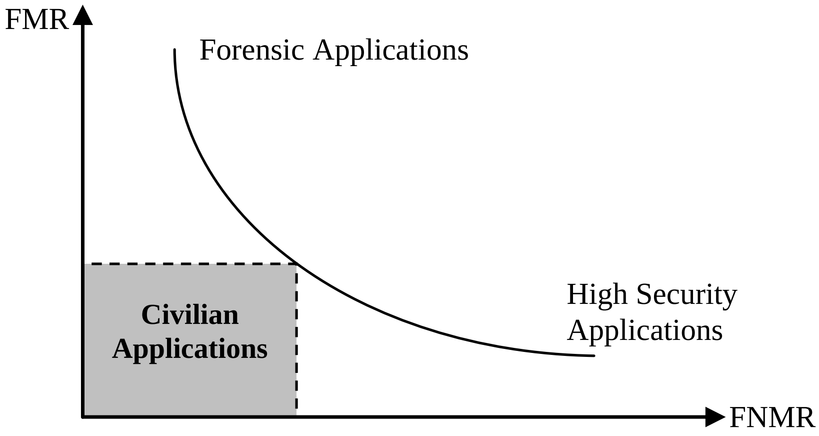

Fig. 2. Receiver operating characteristic (ROC) [1]

There are two other recognition error rates that can be also used and they are: *failure to capture* (FTC) and *failure to enroll* (FTE). FTC denotes the percentage of times the biometric device fails to automatically capture a sample when presented with a biometric characteristic. This usually happens when system deals with a signal of insufficient quality. The FTE rate denotes the percentage of times users cannot enroll in the recognition system.

5. UNIMODAL BIOMETRIC SYSTEMS

There is a variety of problems with biometric systems installed in real world applications which prove that biometrics is not fully solved problem. As shown in Table II [8] there is still plenty of scope for improvement.

Table II State-of-the-Art Error Rates associated with fingerprints, face, and voice biometric systems [8]

Biometric characteristic	**Test**	**Test Parameter**	**FNMR**	**FMR**
Fingerprint	FVC2002 [3]	Users mostly in the age group 20-39	0.2 %	0.2 %
Face	FRVT2002 [5]	Enrollment and test images were collected in indoor environment and could be on different days	10 %	1 %
Voice	NIST2000	Text dependent	10-20 %	2-5 %

Limitations of biometric systems using any single biometric characteristic [2]:

1) *Noise in sensed data*: Example is a fingerprint with a scare. Noisy data can also result from accumulation of dirt on a sensor or from ambient conditions.
2) *Intra-class variations*: Biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment. This variation is typically caused by a user who is incorrectly interacting with the sensor.

3) *Distinctiveness*: While a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these traits. This limitation restricts the discriminability provided by the biometric trait.
4) *Non-universality*: While every user is expected to possess the biometric trait being acquired, in reality it is possible that a group of users do not posses that particular biometric characteristic.
5) *Spoof attacks*: An individual may attempt to forge the biometric trait. This is particularly easy when signature and voice are used as an identifier.

6. MULTIMODAL BIOMETRIC SYSTEMS

Limitations of unimodal biometric systems can be overcome by using *multimodal biometric systems* [9]. A multimodal biometric system uses multiple applications to capture different types of biometrics. This allows the integration of two or more types of biometric recognition and verification systems in order to meet stringent performance requirements. Such systems are expected to be more reliable due to the presence of multiple, independent pieces of evidence [10]. These systems are also able to meet the strict performance requirements imposed by various applications [11].

A multimodal system could be, for instance, a combination of fingerprint verification, face recognition, voice verification and smart-card or any other combination of biometrics. This enhanced structure takes advantage of the proficiency of each individual biometric and can be used to overcome some of the limitations of a single biometric. For instance, it is estimated that 5% of the population does not have legible fingerprints, a voice could be altered by a cold and face recognition systems are susceptible to changes in ambient light and the pose of the subject's head. A multimodal system, which combines the conclusions made by a number of unrelated biometrics indicators, can overcome many of these restrictions.

Levels of consolidation

Information presented by multiple traits may be consolidated at various levels. At the *feature extraction level*, the data obtained from each sensor is used to compute a feature vector. Since data from various traits are independent of each other they can be concatenated to a new vector with higher dimensionality that represents a person's identity in a new hyperspace. This new vector is then used in the matching and decision-making modules of the biometric system. At the *matching score level*, each individual system provides a matching score and those scores are combined to affirm the authenticity of the claimed identity. At the *decision level*, each individual system provides multiple biometric data and the resulting vectors are individually classified into two classes – accept or reject. Final decisions are consolidated by employing techniques such as majority voting.

Integration at the feature extraction level is expected to perform better than fusion at two other levels. However, this is not always the best solution. The feature shapes of multiple biometrics may not be compatible and even if they are compatible there is still a problem of combining the feature set. Concatenation could result in a feature vector with a very large dimensionality. Fusion at the decision level is considered to be rigid due to the availability of limited information.

Fusion at the matching score level seems to be the logical choice as it is relatively easy to access and combine scores presented by the different modalities [12]. It is generally believed that a combination scheme applied as early as possible in the recognition system is more effective.

Multimodal biometric systems can be designed to operate in five integration scenarios: 1) *multiple sensors*, 2) *multiple biometrics*, 3) *multiple units of the same biometric*, 4) *multiple snapshots of the same biometric*, 5) *multiple representations and matching algorithms for the same biometric* [2].

7. CONCLUSION

Biometrics refers to an automatic recognition of a person based on her behavioral and/or physiological characteristics. Many business applications (e.g. banking) will in future rely on biometrics since using biometrics is the only way to guarantee the presence of the owner when a transaction is made. For instance, fingerprint-based systems have been proven to be very effective in protecting information and resources in a large area of applications. Although companies are using biometrics for authentication in a variety of situations, the industry is still evolving and emerging. At present, the amount of applications employing biometric systems is quite limited, mainly because of the crucial cost-benefit question: supposing biometrics *do* bring an increase in security, will it be *worth* the financial cost?

The future probably belongs to multimodal biometric systems as they alleviate a few of the problems observed in unimodal biometric systems. Multimodal biometric systems can integrate information at various levels, the most popular one being fusion at the matching score level. Besides improving matching performance, they also address the problem of non-universality and spoofing.

Finally, the use of biometrics raises several privacy questions. A sound trade-off between security and privacy may be necessary; but we can only enforce collective accountability and acceptability standards through common legislation [1]. For example, if and when face-recognition technology improves to the point where surveillance cameras can routinely recognize individuals, privacy, as it has existed in the public sphere, will be wiped out. Even today, in some major cities, you are recorded approximately 60 times during the day by various surveillance cameras.

In spite of all this it is certain that biometric-based recognition will have a great influence on the way we conduct our daily business in near future.

REFERENCES

[1] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy*, March/April 2003, pp. 33-42

[2] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp 4-19, January 2004

[3] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain, "FVC2002: Fingerprint verification competition" in *Proc. Int. Conf. Pattern Recognition (ICPR)*, Quebec City, QC, Canada, August 2002, pp. 744-747

[4] A. Ross, A. K. Jain, "Information fusion in biometrics", *Pattern Recognition Letters 24* (2003) 2115-2125, available at http://www.computerscienceweb.com/

[5] P. J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, J. M. Bone, "FRVT2002: Overview and Summary," available at: http://www.frvt.org/FRVT2002/documents.htm

[6] M. Golfarelli, D. Maio, D. Maltoni, "On the error-reject tradeoff in biometric verification systems," *IEEE Trans. Pattern Anal. Machine Intell.*, Vol. 19, pp. 786-796, July 1997

[7] J. Daugman, "How Iris Recognition Works", *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp. 21-30, January 2004

[8] L. O'Gorman, "Seven issues with human authentication technologies," *in Proc. Workshop Automatic Identification Advanced Technologies (AutoID)*, Tarrytown, NY, Mar. 2002, pp. 185-186

[9] L. Hong, A. K. Jain, S. Pankanti, "Can multibiometrics improve performance?," in *Proc. AutoID'99, Summit*, NJ, October 1999, pp. 59-64

[10] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, R. P. W. Duin, "Is independence good for combining classifiers?," in *Proc. Int. Conf. Pattern Recognition (ICPR)*, Vol. 2, Barcelona, Spain, 2001, pp. 168-171

[11] L. Hong, A. K. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Trans. Pattern Analysis Machine Intell.*, Vol. 20, pp. 1295-1307, December 1998

[12] A. K. Jain, A. Ross, "Multibiometric Systems", *Appeared in Communication of the ACM, Special Issue on Multimodal Interfaces*, Vol. 47, No.1, pp. 34-40, January 2004