International Journal of Image and Graphics

A Review of Performance Evaluation for Biometrics Systems

Jin-Hyuk Hong, Eun-Kyung Yun, and Sung-Bae Cho
Department of Computer Science, Yonsei University
134 Shinchon-dong, Sudaemoon-ku, Seoul 120-749, Korea
hjinh@sclab.yonsei.ac.kr ekfree@sclab.yonsei.ac.kr sbcho@cs.yonsei.ac.kr

Received (Day Month Year)
Revised (Day Month Year)
Accepted (Day Month Year)

Biometrics is a technology to automatically recognize person with his/her natural and distinct characteristics, and recently it attracts attentions as an effective authentication method of information society. With the great interests of biometrics, the need for reliable evaluation for these technologies increases and the research on objective and quantitative performance estimation methodology is actively investigated. In this paper, we give a comprehensive overview of biometric technology and performance evaluation with more than 100 publications, especially focused on fingerprint. After the thorough review, we propose a promising evaluation method based on affecting factors.

Keywords: authentication; biometrics; evaluation; affecting factors; state-of-the-art.

1. Introduction

The information society revolutionizes quickly and the way of transactions becomes very complicated. In this complex society, people need methods to keep their information and to authenticate themselves. Especially since many people use electronic transactions, it is critical to achieve a high accurate automatic personal authentication. As organization needs high degree of security for user access, e-commerce, and other security application, biometrics attracts attention as one of remarkable authentication methods. While biometrics has been used for criminal identification and prison security, it is recently adopted as efficient method for authentication in many applications. Although biometrics is not the most powerful authentication method, it provides high security and possibility to be applied. With the great interest of biometrics, it is necessary to evaluate the biometric systems accurately. For most biometric products, the evaluation was not good enough to estimate the performance. These days many evaluation projects have been conducted, thereby methodology for evaluation is developed. In this paper, we are interested in the performance evaluation of biometric systems. The rest of this paper is organized as follows. In section 2, we present the definition and characteristics of biometric systems and features, its applications, related works, etc. In section 3 the performance evaluation of biometric systems including the existing methodologies are presented. We propose an improved method for effective evaluation, called factor-based evaluation, which is based on all affecting factors of the biometric systems. Then, we analyze the various evaluation projects from all over the world. Finally, in section 4, we present the state-of-art on fingerprint recognition and performance evaluation as a case study.

2. Biometric Systems

2.1. *Definition and Characteristics*

Authenticating an individual is to distinguish an authorized person from imposters to access the system or information, and it is very important in information society [114]. Two major traditional authentication methods have been used: knowledge-based and token-based. Knowledge-based authentication uses "something you know" to verify oneself such as PIN (Personnel Identification Number) and password, and token-based authentication uses "something you have" such as ID card and a key. However, there are many disadvantages and limitations with these traditional methods. PIN may be easily forgotten or guessed by an imposter and the tokens may be lost or stolen. In order to overcome these problems, biometrics has got attention and actively investigated [115,48,11]. Biometrics automatically identifies or verifies an individual based on one's physiological and behavioral characteristics [113,2,63] and usually fingerprint, face, iris, voice, and signature are used as characteristics [121,90]. Contrary to the traditional authentication methods, biometric systems have the best performance in terms of security, management, and user convenience. It is very useful for users because biometric features are difficult to be forged and robbed. In addition, it is free from obligations of possession [15,79]. Biometric authentication can be used in two modes: identification and verification. The former is to identify a person from database of the system without an identity claim, and it is called "one-to-many" search [110]. The latter is to verify someone with identity, and it is called "one-to-one" search. Identification is much more difficult than verification, because identification requires a number of matchings. The computational overhead in identification depends on the number of people in database, and the following formula shows it [25].

$P_N = 1 - (1 - P_i)^N$, where
P_i : probability of false acception verification
P_N : probability of false acception identification with N templates
N: the size of database

Traditional authentication methods are static with fixed information and items, but biometric systems need dynamic process because the characteristics are changeable. It is difficult to control the difference between biometric samples from same person, and the system is subject to have low performance. Therefore, researchers focus on the solution of these limitations to increase the performance.

2.2. *Biometric Feature*

Biometric system uses a part of body as personal characteristics for authentication. There are many characteristics but not all characteristics are useful. To design an effective system, it is very important to decide which characteristics the system uses [107]. General criteria for selection of biometric feature are as follows [116,48].

- Universality: everyone should have this distinguishable trait
- Uniqueness: no two persons should be the same in terms of this trait
- Permanence: it should be invariant with time
- Collectability: it can be measured quantitatively

In addition, the following criteria can be considered.

- Performance: achievable identification accuracy, resource requirements, and robustness
- Acceptability: to what extent people are willing to accept it
- Circumvention: how easy it is to cheat the system

Common biometric features used in biometric systems are fingerprint, face, iris, voice, signature, retina, DNA, hand, etc [33,113,30,75,77,89,90,85]. Table 1 shows the traits of each biometric feature [48]. Ideal biometric feature satisfies the above criteria but such a biometric feature is not known yet. So the research on multimodal biometric is progressed to compensate the weakness of each biometric feature and to generate ideal biometric feature. Table 2 shows the analysis of biometric systems for each biometric feature [117].

Table 1. Comparison of Biometric Features

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Keystrokes	Low	Low	Low	Medium	Low	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Medium	Low	Low	Medium	Low	High	Low
F.Thermograms	High	High	Low	High	Medium	High	High
Odor	High	High	High	Low	Low	Medium	Low
DNA	High	High	High	Low	High	Low	Low
Gait	Medium	Low	Low	High	Low	High	Medium
Ear	Medium	Medium	High	Medium	Medium	High	Medium

Table 2. Comparison of Biometric Systems

	Fingerprint	Face	Hand	Typing dynamics	Signature	Voice	Retina	Iris
Sensor principle	optical capacitive infrared ultrasonic pressure	Camera digital(CCD) video infrared	Camera	Keyboard	Cheap CAD type pen tablets Special pens	Microphone	Infrared laser	Video camera
Data size	Small-Medium (depending on algorithms)	Average (depending on algorithms)	Small	Medium	Small-Medium (depending on algorithms)	Small-Medium (depending on algorithms)	Small	Small
Variability	Variations at sensor-human interface	User's position or light conditions	Incorrect hand positioning	Typing rhythm is keyboard-and emotion-dependent	Natural variability of signatures	Natural variability of voice (ex: sickness)	Fatigue or temperature	High uniqueness
Acceptance	Criminological associations or hygiene considerations	Management system (non-invasive)	Hygiene considerations	Permanent keyboard monitoring enables surveillance	High level of acceptance in the literate environment	Health considerations	Acceptance problems possible as method is perceived as invasive	
Reliability	Extensive experience with optical sensors in field trials and applications	Lighting conditions are crucial	Reliable in numerous field trials, successfully deployed in the 1996 Olympic in Atlanta	Maximum attributes of a personal rhythm only with experienced typists with characteristic typing habits Reliable in the literate environment	Low error rates with precise focusing	Light-dependent		
Life test	Counter deceptions using severed or artificial fingers	Test in the form of 3-dimensional image processing or evaluation of the reflectance characteristics of human skin etc. must be employed to counteract imitations	Test necessary to prevent imitations using artificial hands		Since no two signatures are absolutely identical, signature process requires human action	To prevent deception using voice recordings	To counter fake retinas	To prevent fake irises
Price	Sensor principle-dependent	Midrange	Expensive		Cheap	Cheap	Expensive	Expensive

2.3. *Applications*

As described previously, each biometric feature has individual characteristics, and a biometric system has strength and weakness depending on its application. So the analysis and detailed classification of applications are essential for practical use of system [107,17]. Applications are partitioned according to seven criteria shown in Table 3 [116].

Table 3. Criteria for Classification of Application

User	Environment	System
Cooperative / non-cooperative	Standard / non-standard	Overt / covert
Habituated / non-habituated		Attended / non-attended
Public / private		Open / closed

2.4. *System Architecture*

Biometric system consists of input device, authentication algorithm and database, and its main processes are acquisition, feature extraction, matching and detection, as shown in Fig. 1 [3,116]. Acquisition of biometric samples is a process to collect physiological or behavioral characteristics from user automatically. If the quality of collected sample does not satisfy some criteria, acquisition executes repeatedly until it collects satisfied sample. Input device has certain criteria and procedure to collect samples according to its type. It is very important to collect good quality signals because it affects the whole performance of system.

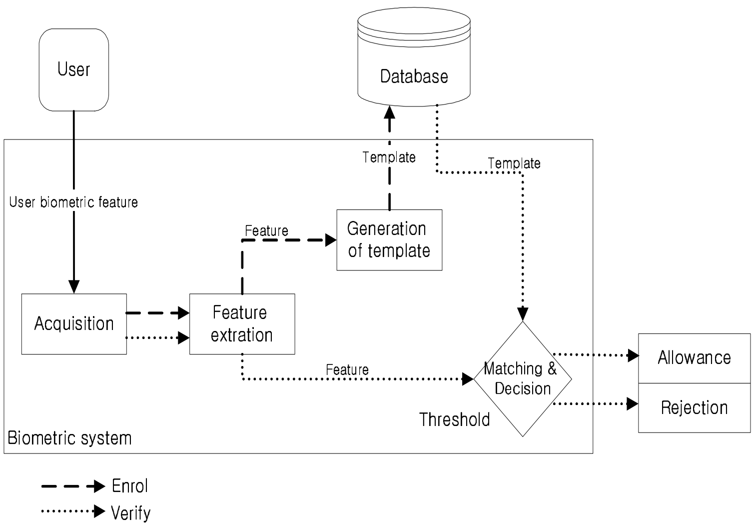


Fig. 1. The structure of biometric system

Since collected samples by sensor have useless information and noises, useful features are needed to be extracted. Too much information deceases the performance of system, so that the proper size and complexity of information must be extracted and they have to be distinct and repeatable. Extraction is determined by the design of system and its biometric feature. Because the uniqueness of features is a factor determining the system's recognition performance, features must meet the criteria of system even though the system needs several trials for collection. Especially at enrollment, the quality of samples must be controlled as high as possible. After feature extraction, the system performs creation of template when it conducts enrollment and it performs matching when the authentication is on. Biometric system is initialized with enrollment of the users' template. Template includes features and user information, which are stored in database. Therefore, templates are created only in enrollment and since this template is always used in authentication, its quality is very important. Template can be stored with many kinds of method, which encourages the research on IC card and smart card as storage of template recently [1]. A large-scale identification system needs a process to reduce processing time, such as dividing database into bins by some criteria, and the occurred error is called binning error rate. In authentication mode, the system executes matching that compares a sample with templates to find a match, and in decision stage, the result of matching determines decision of system. Verification needs just one matching trial, but identification needs several matching trials until the system finds the match. In decision stage, the system uses the result of matching and a threshold determined by operator. Usually the threshold is calculated with test database. All steps of biometric system influence performance and use different algorithms and devices according to the types of biometric feature and application. Therefore, we can get high performance by designing a system based on analyses of each step. The followings are the general considerations in designing a biometric system.

- Usability: easy usage (input devices, the types of templates storage)
- Performance: accuracy, speed, robustness, resources, size, etc
- Circumvention: counterplans against the illegal authentication trials (input devices, features used)
- Cost:
  - Production costs (input devices, whole system, databases)
  - Initialization costs (set up, enrollment, and training administrators)
  - Use costs (training users, processing exceptions, maintenance, and authentication failures)
- Acceptability: relation with privacy (input devices)

2.5. *Related Works*

2.5.1. *Multimodal biometrics*

Biometric system has many limitations of the performance and its application because of biometric feature. A biometric feature is not absolutely superior to the others in terms of universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention. In addition, every biometric feature is dependent on various environments and users. Since many biometric systems in practical do not satisfy with the performance in some applications, multimodal biometric technologies of combining various biometric features get attention from many researchers [97,63,31]. Multimodal biometric technologies are classified into following five categories [31].

- Multiple sensors: various sensors are available to capture the same biometric
- Multiple biometrics: multiple biometrics such as fingerprint and face may be combined [97]
- Multiple units of the same biometric: for example, several signals from two irises, or two hands, or 10 fingerprints may be combined [123]
- Multiple instances/impressions of the same biometrics: multiple signals/samples of the same biometric [60]
- Multiple representation and matching algorithms for the same input biometric signal: combining different approaches to feature extraction and matching of the biometric [50,81]

2.5.2. *Standardization*

With the development of biometric technology, several standardizations have to be involved for the industry maturity: interoperability, interchangeability, standard database, and API (Application Programming Interface). Application standards include BioAPI, HA-API, BAPI, SVAPI, etc that provide the standardization about interfaces and techniques for effective development of APIs [103]. There are standards for data interoperability and security, such as CBEFF (the Common Biometric Exchange File Format) and X9.84 [103] which define the common data elements and provide the policies for protecting data. Also, there are many leading groups for biometrics standardization, such as BioAPI [4], ANSI [102], NIST [105], UK Biometrics Working Group [104], IBI, AfB [101], etc. BioAPI Consortium is developing a widely available and acceptable API, and NIST produced CBEFF for biometric interoperability [4]. UK Biometrics Working Group works mainly on evaluation and announces requirements for functional certification of commercial biometric systems [115,63,98].

3. Performance Evaluation

3.1. *Definition and Characteristics*

Performance evaluation of biometric system estimates how suitable biometric is used in the system, especially about universality, uniqueness, permanence, and security. Universality means the percentage of people who have biometric feature used in the system, and uniqueness means how distinctive biometric feature is to separate people. Permanence is used to estimate the robustness of system against changes in time and space, and security shows the degree of safety against illegal trial for authentication. The result of evaluation leads the developer to develop better technology by analyzing the weakness, and provides users with a guideline for selection of biometric system and its usage [69,96,57,79,92,10,44,48]. The evaluation has two properties: objective and quantitative. First, in order to be objective, test must be fair for all systems. If a test gives advantages to particular system, the result may be useless. Second, used data must not be used again in test. It is because that a developer is able to adjust their system to have good performance on data already known. Third, test has to keep the difficulty in the middle. If a test is easy to perform, most systems have good performance and if test is difficult to perform, most systems work poor. It might lose the discrimination between systems. Forth, test must be repeatable [10]. To make test quantitative, the result is usually represented by recognition rate of the whole system or its part, and sometimes ROC (Receiver Operating Characteristic) curve and DET (Detection Error Trade-off) curve are used for presenting the results [71]. According to the object and goal of evaluation, the performance can be estimated by various measures [109,110]. The application of biometric system has various variables and they change continuously because of many factors, and evaluation must be able to estimate the real performance of system in practice. Since most traditional performance evaluations are conducted with very restricted environment and standard users, the result of the test is much different from the performance of system when it applies to real world. To estimate the real performance of system, we consider various factors which affect the biometric systems.

3.2. *Evaluation Methodology*

The evaluation divides into three stages, planning, performing, and analyzing as shown in Fig. 2. Test protocol is designed at planning stage, and test is performed at performing stage. Results from the test are analyzed and reported at analyzing stage [69].

3.2.1. *Planning evaluation*

An evaluator designs the test protocol, the subject and the type of evaluation [9,45]. The structure and biometric feature used in a system determine the subject of evaluation, and the type is set as one of technical, scenario, and operational types [79]. Technical evaluation is for individual modules of recognition algorithm or input device, and it usually applies for comparison between performances of algorithms. The data used in test are collected by common sensors from real world, but it depends on the environment and population. Therefore, it is difficult to estimate the performance of system in real application. This evaluation progresses in offline and uses static databases, and the test is repeatable and is not as expensive as other type of evaluations. In scenario evaluation, evaluator first sets environment for specific prototype and estimates the performance in it. Test data is collected by the sensor, and it does not need any static database but needs online collection. To

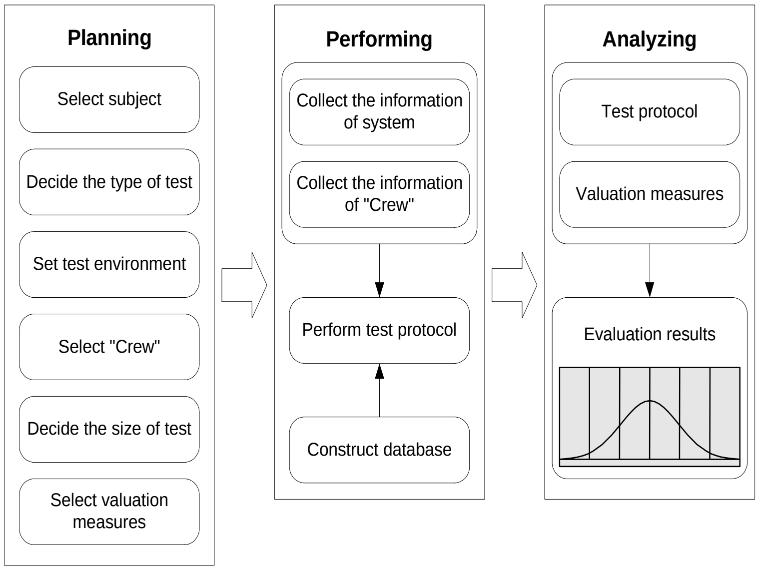


Fig. 2. Procedure of performance evaluation

compare the performance of systems, the environment and population for target systems must be the same and restricted. Different from above types, operational evaluation estimates real performance by conducting in real application. However it is very inefficient, expensive, and difficult to be conducted [12]. Once the subject and type of evaluation are determined, evaluator designs the concrete test protocol based on them. Analysis for system information, settlement of environment, selection of population and determination of size for the test are basic processes of planning. An evaluator designs the schedule of data collection and confirms some notifications during collection with gathering information from system and analyzing it. In particular, for scenario and operational evaluations, information of system is used for proper installation. In settlement of environment, evaluator gets expected the type of results by analyzing affecting factors and controlling the environment for the test [12,76,9,17]. As performance of biometric system is very dependent on environment and population, the control of these factors must be confirmed [45]. Common classification of environment for biometric systems is defined in [116]. After settlement of environment, selection of population is conducted. Population affects the performance of system directly, because biometircs is a human-dependent technology. Accordingly, it is very importance to control the distribution and quality of population through the test. Moreover to get confidence for the result, it needs to decide proper size of population. Usually if the size of test increases confidence increases, but the efficiency of test declines and cost increases [68,16]. After determination of test protocol, evaluator needs to decide some measures for analysis. Measures are usually divided into quantitative and qualitative measures [69]. The former is used to represent numerically recognition and efficiency of system, and the latter is used for evaluation of performance which is not related with recognition directly such as user convenience, security, privacy, and so on [3]. Quantitative measures are usually used in the evaluation of biometric systems, and Table 4 shows the most common measures [111]. FAR and FRR are measures to estimate recognition performance of the whole system, while each means stranger allowance error rate and user rejection error rate. If the system cares user convenience more, FAR increases by decreasing the threshold of matching. On the other hand if high security is required, FRR increases by increasing the threshold in matching. Both are calculated as follows.

$$FAR = (1 - FTA) \times FMR$$
$$FRR = (1 - FTA) \times FNMR + TA$$

FMR and FNMR are used for estimation of recognition performance at matching stage, especially for partial modules of system, such as matching algorithm. ROC (Receiver Operating Characteristic), EER (Equal Error Rate), and DET (Detection Error Trade-off) curve are often used to show the result of FAR / FRR and FMR / FNMR together (Fig. 3 and 4) [71]. FTE is enrollment failure rate which occurs when the system is impossible to recreate user's template during the enrollment, while FTA means acquisition failure rate which occurs when the system does not get a good quality sample during verification. Because in many cases the system does not verify just once from user input and user tries to verify several trials, the number of trials is also considered in evaluation. The efficiency of system is evaluated with processing time to verify by comparison of input sample from templates. First, biometric sample is collected in considerable amount of time. Then, it takes some more time for algorithm. Especially the large scale of biometric system, since it takes too much time to compare with all templates in database, reduces processing time by dividing database into bins and comparing with templates just in a bin. When the system divides database, bin error rate and penetration rate are both considered. Bin error rate is for cases that the system classifies a sample to wrong bin, while penetration rate is rate of searching against total database.

3.2.2. *Performing evaluation and analyzing results*

After the test protocol is determined, database for evaluation has to be constructed. Collection of samples constituting database processes without any error as possible, because the bias and noise of samples affect the performance of system. For an effective performance of test, collected samples must be reported accurately and fully, and the environment of collection must be same through collection [68]. Technical evaluation performs in offline after construction of database while scenario and operational evaluation perform construction of database and evaluation at the same time. Detailed procedures and principles are written in [69]. The performance

Table 4. Quantitative Measures for Performance Evaluation

Measure	Description
FAR (False Accept Rate)	Stranger allowance error in system
FRR (False Reject Rate)	User rejection error in system
FMR (False Match Rate)	Stranger allowance error at matching stage
FNMR (False Non-Match Rate)	User rejection error at matching stage
FTE (Failure To Enroll)	Enrollment failure rate
FTA (Failure To Acquire)	Acquisition failure rate
Processing time	Sample collection time + computation time
Bin error rate	Search error rate by dividing database into bins
Penetration rate	Average search rate in database
Template evaluation	Template size and discrimination

of system is estimated by some measures selected at planning stage. To express the result of test well, ROC/DET curves and the distribution of matching score are often used. Various analyses for the results help users to understand the performance of system more detailed and concrete [12]. In many evaluations, however, the analysis for the result is too poor to understand the real performance. Therefore, the various methodologies for analysis have to be developed.

3.3. *Evaluation for System Modules*

Division into modules of system for evaluation helps evaluator to analyze the result much efficient and detailed [111]. Detailed in previous, a biometric system is composed of various modules and steps as shown in Fig. 5 [16], and each module has different conditions, processes and results. Evaluation at acquisition stage is focused on sensor (input device) and acquired samples. Because of influences such as user's attitude and condition of biometric feature and sensor, samples acquired from sensor are always changed. Biometric system is very sensitive to quality of acquired samples, and even excellent matching algorithms show decrease in performance if a low-quality sample is collected from sensor. The evaluation for sensor based on quality of acquired samples is necessary for this reason [17]. The contents of test are type of sensor, processing time, necessity of additional devices, quality of acquired samples, and Table 5 shows the detailed measures for evaluation.

Previous evaluations for sensor just described hardware characteristics of system, but recently the concern for performance of sensor spreads with quality of samples and environmental conditions, liveness detection, and so on. Especially function of liveness detection promotes the security level of biometric systems, and it is perceived as one of main item for evaluation of sensor [44]. Evaluation for feature extraction stage is focused on the system's power of searching feature pattern from samples. Feature extraction module of system must generate discriminate and reproducible features from sensor even though some noises and losses occur in collection and transmission. To perform well in matching, a level of features is extracted. If the quality of feature is low, the system acquires sample again.

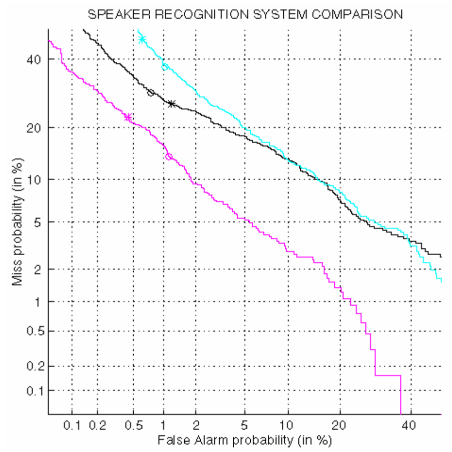


Fig. 3. DET curve

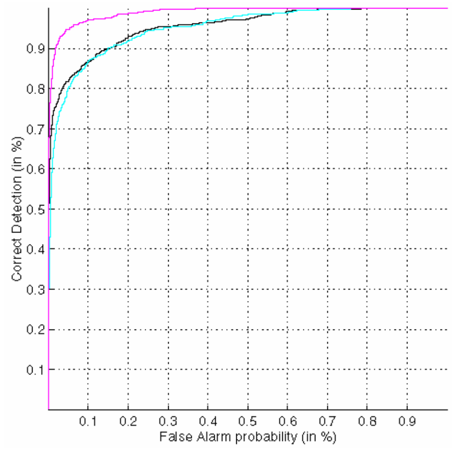


Fig. 4. ROC curve

Therefore, the evaluation of features is necessary for these reasons, and in case of fingerprint recognition, it evaluates feature extraction algorithms and samples based on the number of minutiae extracted from samples. Matching is related with the recognition performance of system directly, so that matching algorithm is evaluated with corresponding failure rate. Moreover discrimination between oneself and others based on matching score may be useful. Table 6 shows measures usually used in feature extraction and matching

In general the evaluation of feature extraction and matching algorithms uses FMR/FNMR, and Distance distribution as measures, adopts ROC and DET curves for representation. When the quality of input sample is not beyond threshold, the

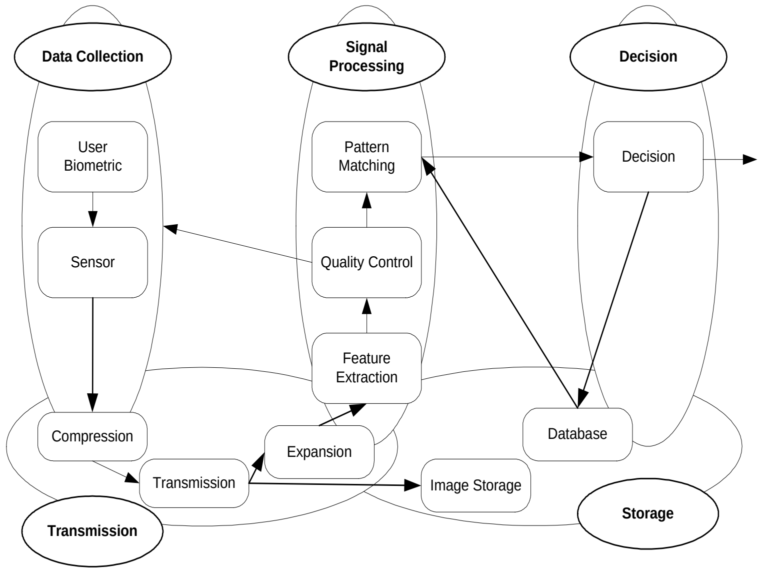


Fig. 5. Basic procedures of biometric system

Table 5. Evaluation Measure for Sensor

Evaluation Measure	Description
Processor	Type of CPU and its processing power (MHz)
Additional hardware	Necessity of an additional device for enhancement of performance
Non-standard hardware	Necessity of a self-developed device for enhancement of performance
Resolution	Resolution (dpi) of input sample
Image quality	Quality of input sample
Biometric data size [44,118]	Size of collected biometric feature
Sensor size	Size of sensor
Module size	Size of module
Environmental condition	Environmental conditions of system [humidity, temperature, light, noise, etc)
Power consumption	Power consumption
API standard compliant	Support of standard API
Device interface	Convenience and use of device interface
Liveness detection	Support of antispoofing function for detection of biometric forgery

rate of failures acquiring the sample is called FTA and the rate of failures enrolling in the system is called FTE. For large scale biometric system, bin error rate and penetration rate are used to estimate the performance of classification algorithms. Classification is one optional part of matching, especially in large scale biometric system. The total performance of whole system can be estimated by error in decision stage. The system decides allowance/rejection by its policy based on matching score. Table 6 shows the evaluation measures in decision stage. Threshold for decision policy is possible to be controlled by manager, and if threshold is adjusted high,

Table 6. Evaluation Measure for Feature Extraction and Matching

Evaluation Measure	Evaluation Content
FMR / FNMR	Imposter accept error / Legitimate user reject error
EER [108]	Error rate when accumulation of FMR and FNMR are equal
ROC	Graph representing FMR, FNMR together
FTE	False Enrollment rate
FTA	False acquisition rate
Distance distribution [111]	Distribution of matching score between users in database
Matching time	Time for matching
Average ROC	Average result of ROC from several test
Upper bound	Best result among some algorithms for specific database
Resource	Minimum required memory, storage
Bin error rate	Search error rate by dividing database into bins
Penetration rate	Average search rate in database
Liveness detection	Support of antispoofing function for detection of biometric forgery

the security of system increases but not in user convenience.

Table 7. Evaluation Measure for Whole System

Evaluation Measure	Evaluation Content
FRR / FAR	Stranger allowance error in system / Legal user rejection error in system
Threshold	Critical point of system's policy

3.4. *Factor-based Evaluation*

Biometric system is based on biometric feature, so that the comprehension of biometric feature's characteristics and good design of system help to improve the performance. Evaluation based on affecting factors makes it possible to understand the characteristics of feature more detailed and to design the system based on it. Biometric feature is generated based on genetic factor and social factor. Genetic information forms it with a person's birth, afterward it is developed to unique biometric feature by social factor such as one's living environment. Since the samples acquired by biometric system are changed because of sensor, environmental condition, user condition, etc, they cannot be considered identical as user's biometric feature. Fig. 6 shows the generation of biometric samples by stages and influences by environmental and user factors. The genetic factors of biometric feature are natural traits based on human's DNA, and among families, relatives, and identical twins it is easy to affect on the performance of recognition because they are very similar in biometric feature against others [99]. To make the system more robust against these factor, the research on analysis of genetic relation for each biometric feature and the evaluation methodology of robustness of system for genetic factors. One of remarkable works of evaluation for genetic factors is Twin Test [54], and it targets identical twins having same gene expression and estimates the performance of system among them. The evaluation on genetic factors can be possible as it targets identical twins and families who have similar genetic effects. Table 8 shows some effects of generic factors, but the research on effects of genetic factors which are invisible and unknown is necessary and the evaluation methodology must be developed.

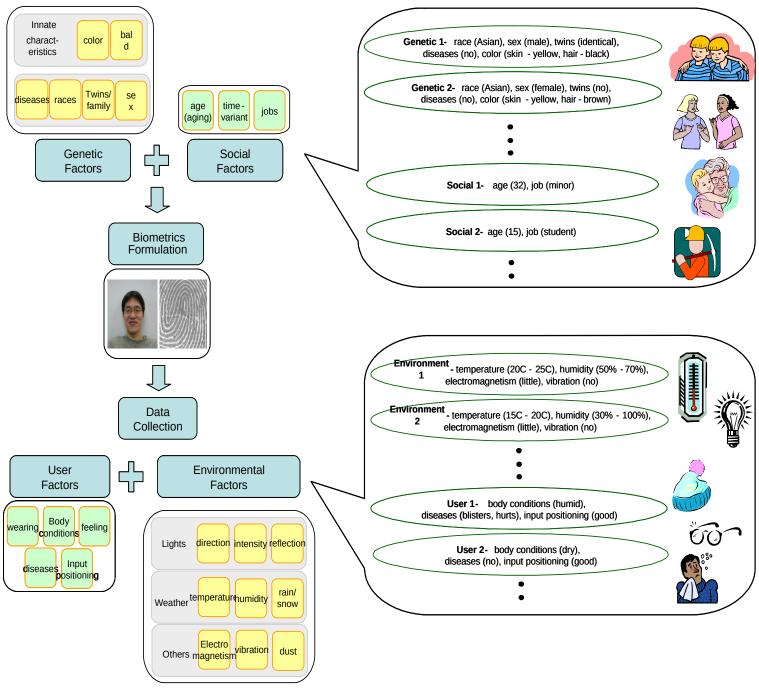


Fig. 6. Generation of biometric samples

Table 8. Effect of Genetic Factors for each Biometric Feature

	Fingerprint	Face	Iris	Retina	Hand	Voice
Physical feature	Class of fingerprint	Baldhead, beard, hair color, skin color	Eye color	Eye color	unknown	unknown
Disease	unknown	unknown	Eye disease	Eye disease	unknown	unknown
Etc	Race, age, sex, identical twins, family, etc					

After birth, biometric feature is continually affected by social factors. Most representative social factors are one's growth environments, job, age, and so on. In case of fingerprint, fingers of someone who has job using hands much might be damaged and cause difficulty in recognizing fingerprint. Besides in case of using system in long period, if only the system considers changes of biometric feature through the time, it performs well enough. Therefore it is very difficult to analyze and understand the effect of social factor such as time, when the system just uses data collected in short period. It is known that people have different fingerprints and irises because of social effects even though they are identical in inheritance. Especially changes of biometric feature though time are researched as template aging. However, concrete methodology of evaluation is not yet developed and conducted in practice. Biometric feature which is generated from genetic and social factors changes in sample collecting process of biometric system because of effects such as noise, transformation, etc [3,69,76,21]. Environmental and user factors affect during the collection of biometric samples. Environmental factors are surroundings of application of biometric system, and they affect sensor directly [33,9]. The variation of temperature and moisture of environment changes humidity of hands, and it influences the acquisition of fingerprint images, while light and color affect in optical sensor. Even though environmental factors are controlled by restricting conditions of environment, but it is very difficult and restricts the scope of application of the system [14]. So it is necessary to develop various evaluations based on environmental factors to estimate the real performance of biometric system [76,44,17,13]. Environmental factors for each biometric feature are described in Table 9, and Fig. 7 shows the effect of environmental factors of fingerprint [119].

Table 9. Environmental Factors for Biometric Samples

Environmental condition		Fingerprint Optical	Fingerprint Contact	Face	Iris	Retina	Hand	Voice
Light	Intensity	O		O	O	O	O	
	Color	O		O	O	O		
	Direction	O		O	O	O		
Air condition	Temperature	O	O				O	O
	Humidity	O	O				O	O
	Dirty	O	O	O	O	O	O	
Etc	Electric	O	O	O	O	O	O	O
	Noise	O						O
	Tremor	O	O	O	O	O	O	O
	Object			O				

Collected samples are changed not only by environmental factors but also by user's state. Basic biometric feature of user does not change, but in collection the user's conditions are not always same and they break out some difference between biometric feature and sample of user. These biases are minimized by control of collection procedure with many restrictions, while the user convenience is reduced. Table 10 shows the user factors affecting the performance of biometric system [69,17].

Fig. 7. Fingerprint Images Affected by Various Environmental Factors (a) normal (b) dried (c) moist (d) low quality

Table 10. User Factors for Biometric Sample

	Fingerprint	Face	Iris	Retina	Hand	Voice
Accessory	Ring	Glasses, ear ring, necklace, scarf, sunglasses, mask, hat	Glasses, sunglasses	Glasses, sunglasses	Ring, watch, bangle, gloves	Mask
Physical trait	Humidity, cosmetics	Hair style, color	N/A	N/A	Humidity, cosmetics	N/A
Mode	N/A	Expression	N/A	N/A	N/A	Interval, volume, speed
Disease	Blister	N/A	Eye disease	Eye disease	N/A	Cold
Input condition	Position against sensor (Location, angle, pressure)	Pose, distance, height, angle, movement	N/A	N/A	Hand shape, position, direction	Position against sensor (Distance)

Biometric sample used in biometric system is affected by many kinds of factors, so the evaluation must consider those factors to be more effective and analytic and the results from this are recognition performances of biometric system in real applications. Fig. 8 shows a variety of results based on this evaluation methodology. Analyzing the result, the performance of system is comparatively good in collection but not for genetic and social factors. Evaluator can find that the counter measures for imposture of twins and families are needed for the biometric system.

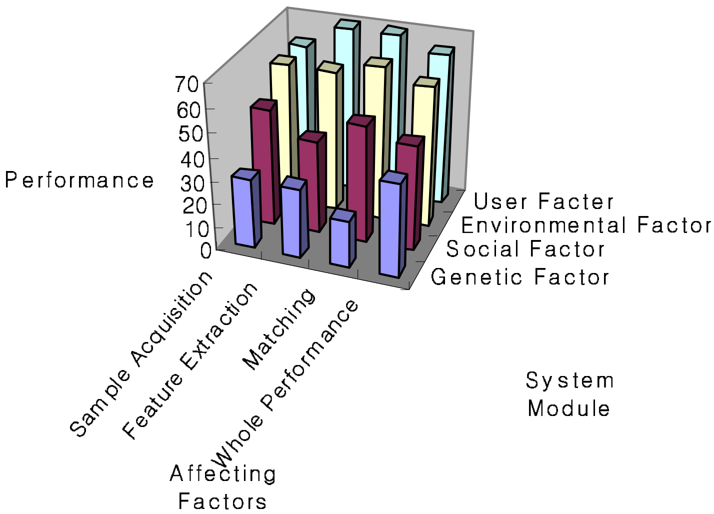


Fig. 8. Diversified analysis of evaluation

3.5. *Related Works on Evaluation*

Biometric evaluation projects are performed by many research groups on a large scale, and Table 11 shows projects to date. Shown in type and measure, most projects are conducted as technical type and target for recognition algorithms. FRVT2000, FVC2000, BioIS, and Biometric product test get a favorable reception for their procedures and results. FRVT2000 (Facial Recognition Vendor Test 2000) is a project by United State, and it's for evaluation of commercial face recognition systems. It purposes to understand the trends of face recognition technologies and to certify the growth of technologies since FERET [80]. It adopts most procedures of FERET and uses ROC, CMC chart for representation of results. Total test is divided into technical and scenario evaluation, and it executes concrete and detailed tests by analyzing environmental factors and changing parameters more various than other projects. FVC (Fingerprint Verification Competition) is supervised by Bologna university in Italy and Michigan university in United State, and it evaluates the performance of fingerprint recognition algorithms. Four kinds of database are used in the project, while three databases are collected by different sensors and one database are constructed by fingerprint generating algorithm [112,20]. The result is represented by ROC curve, average FTE, enrollment time, matching time, and etc. It just considers recognition algorithms but not any external effects. Moreover, even it constructs databases from different sensors but it doesn't evaluate sensors. BioIS is a project to evaluate biometric system by Fraunhofer university in Germany in 1999. It defines test protocol for evaluation and divides evaluation into general assessment, reliability of acquisition, security/dupability by its purpose. To estimate the performance, it uses operational time, number of user's trials, EER, FAR and FRR as quantitative measures and reports some comments in detail for each system as qualitative results. Biometric product testing is conducted by NPL in 2000, and evaluates 7 biometric systems. It divides users by age and sex, sets various experimental environments to estimate the robustness of systems for them. FTE, FTA, FMR/FNMR, FAR/FRR, and FR for each trial are used to estimate the recognition performance, and processing time, efficiency of matching algorithm, performance for a specific population are used to analyze the results.

Until now most performance evaluation projects are conducted as technical evaluation, and they construct database without any specific purpose. So they cannot estimate the performance of system in real application which has many changeable variables. FRVT2000 adopts various factors and collects data to conquest the limit, so the result is more confident than other projects although the performances of systems are very poor.

4. Fingerprint Recognition and Evaluation

4.1. *Fingerprint Recognition Systems*

Fingerprint recognition is the technology that distinguishes between the user and the others using the unique information in fingerprint. Fingerprint recognition system consists of input devices, recognition algorithms, and databases like general biometrics systems. Fig. 9 shows whole processes. There are lots of publications in each module [53,77,87].

Firstly, the system needs to obtain the digitalized fingerprint images using the fingerprint capture devices [82]. The traditional method is an ink-based sensor, which uses the ink to get the fingerprint onto a piece of paper. Otherwise modern live scan devices contain the optical fingerprint capture device with a light source and lens, and non-optical with an array of sensing elements. With optical sensors, the finger is placed on a plate and illuminated by a LED light source. Through a prism and a system of lenses, the image is projected on a camera. Non-optical sensors have temperature sensor using the array of temperature measurement pixels, electronic field sensor, and ultrasonic sensor [35,82]. Fingerprint recognition system must obtain the good quality images in order to work better [24]. However, the fingerprint depends on a variety of work and environmental factors such as age, gender, race etc. In particular, fingerprint image is in low quality if one is a manual worker or is at an advanced age. In addition, the fingerprint depends on weather, a hurt, and skin conditions. Besides the information of fingerprint can be modified because 3-dimensional information of fingerprint convert 2-dimensional information on sensors. Recent researches focuses on the smaller and cheaper sensors that control these variable factors. Especially the technology with capturing the 3-dimensional fingerprint information is remarkable in the futures [100]. After the capture of finger-

Table 11. Evaluation Projects of Biometric System

	Object	Target	Manager	Type	Measure
FERET [76,80,86] (1993 1998)	Development of automatic face recognition technology and performance evaluation	Face recognition algorithms (total 6 participating college/company)	DoD Counterdrug Technology Development Program Office of	Technical	Cumulative score
FRVT2000 [8,9] (2000)	Understanding of the trends of face recognition technology since FERET	Face recognition algorithms (total 5 participating company)	United State DoD Counterdrug Technology Development Program Office of United State, National Institute of Justice, DARPA	Technical, scenario	ROC, CMC
FVC2000 [66] (2000)	Understanding of the level of present technology and presenting future direction	Fingerprint recognition algorithms (total 11 participating college/company)	Bologna Univ. in Italy, Michigan state Univ. , NBTC in United State	Technical	FMR, FNMR, ROC, etc
FVC2002 [67,] (2002)	Understanding of the level of present technology	Fingerprint recognition algorithms (total 33 algorithms from 29 teams)	Bologna Univ. in Italy, Michigan state Univ. , NBTC in United State	Technical	FMR, FNMR, ROC, FMR100, FMR1000, etc
BioIS [5,124] (1999)	Definition of standard for reliable evaluation	Fingerprint, face, palm, iris, signature, voice recognition system (total 12 systems of 8 company)	Fraunhofer institute of Graphical Data Processing , Federal Criminal Investigation Office(BKA), German Information Security Agency(BSI) in German	Technical, scenario	FRR, FAR, etc
Biometric Product Testing [68] (2000)	Suggesting methodology for performance, activity	Fingerprint, face, palm, iris, vessel, voice recognition system (total 7 systems of 7 company)	National Physical Laboratory, CESG(Communications Electronics Securit Group) in England	Technical	FTA, FTE, FRR, FAR, etc
BioTrusT [7] (1999)	Supplying applications and evaluation criterion in electronic commerce	Face, fingerprint, void, iris, multimodal biometric system (total 8 systems)	TeleTrusT WG6	4 stage evaluations	-
BioTest [6] (1999)	Developing standard methodology for comparison and evaluation of biometric system	-	EU	-	-

print image from the sensors, the feature extraction is going on [87]. Fingerprint has ridges and valleys that contain unique information in every person. These features are global and local information. The whole directions of ridgelines in fingerprint images are used as global features. Local features using the local structures of ridgelines are called as minutiae. In general, the ending points and bifurcation points

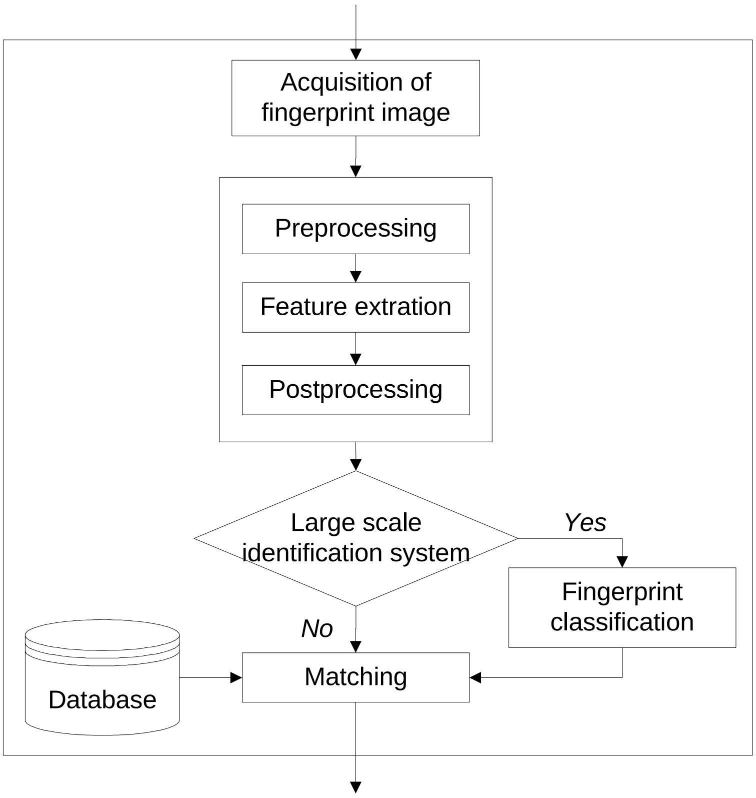


Fig. 9. The Structure of fingerprint recognition system

are used as the most popular minutiae. For better performance, the singular points such as cores and deltas are also used. Fig. 10 shows the structure of fingerprint including the features. Table 12 and 13 show the fingerprint features used in existing fingerprint models and researches.

General fingerprint recognition systems work based on minutiae and this paper focuses on the minutiae extraction. Firstly, preprocessing, minutiae extraction, and post processing procedures apply to the fingerprint images. The performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. If the acquired images have many noises, the minutiae extraction cannot be applicable directly. [26]. Therefore in order to ensure that the performance of the minutiae extraction algorithm will be robust with respect to the quality of input fingerprint images, an enhancement algorithm which can improve the clarity of the ridge structures is necessary [37,42,94]. In addition, a post processing algorithm is necessary because there are many pseudo minutiae in very poor fingerprint images, which are needed to delete. The final minutiae extracted through these procedures are used in fingerprint matching. The popular fingerprint matching algorithms use

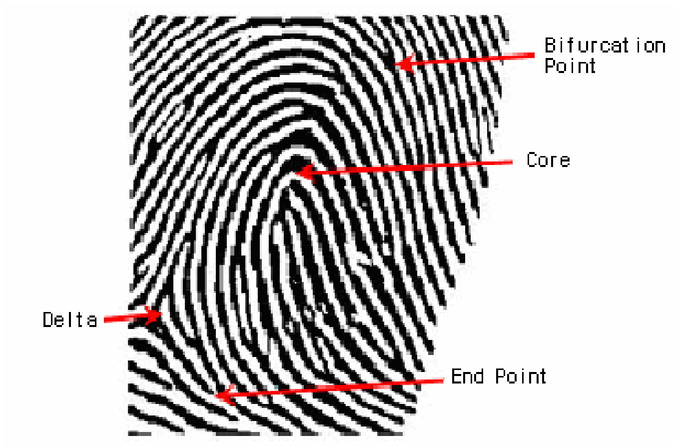


Fig. 10. The structure of fingerprint

Table 12. Evaluation Projects of Biometric System

Author	Year	Fingerprint feature
Cummins and Midlo	1843	Minutiae locations and types, core-to-delta ridge count
Galton	1892	Ridges, minutiae types
Henry	1900	Minutiae locations, types, core-to-delta ridge count
Balthazard	1911	Minutiae locations, two types, and two direction
Bose	1917	Minutiae locations and three types
Wentworth and Wilder	1918	Minutiae locations
Pearson	1930	Ridges, minutiae types
Roxburgh	1933	Minutiae locations, two minutiae types, two orientations, fingerprint and core types, number of possible positioning, area, fingerprint quality
Amy	1948	Minutiae locations, number, types, and orientation
Trauring	1963	Minutiae locations, two types, and two orientations
Kingston	1964	Minutiae locations, number, and types
Gupta	1968	Minutiae locations and types, types, ridge count
Osterburg et al.	1980	Minutiae locations and types
Stoney et al.	1986	Minutiae location, distribution, orientation, and types, variation among prints from the same source, ridge counts, and number of alignments

minutiae-based and frequency-based methods. Minutiae-based matching uses the minutiae and frequency-based matching uses the information from the whole ridge-lines flows filtered [51]. At the matching stage, the template from the claimant fingerprint is compared against that of the enrollee fingerprint. One result of the matching is a match score that is subject to a use-chosen threshold value. The threshold is determined according to the level of user convenience and the system security. In the large-scale fingerprint recognition system, in order to decrease the

Table 13. Fingerprint Features used in Recent Work

Author	Year	Fingerprint feature
Driscoll et al.[27]	1991	Grayscale intensity
Marsh et al.[70]	1991	Grayscale intensity
Coetzee and Botha	1993	Minutiae and frequency-domain features
Maio et al.[65]	1995	Minutiae, core, delta
Ratha et al.	1996	Minutiae
Sibbald[95]	1997	Grayscale intensity
Jain et al.[47]	1997b	Thin ridges, minutiae
O'Gorman	1999	Minutiae
Jain et al.[51]	2000a	FingerCode, Orientation, Grayscale intensity
Jiang et al.[55]	2000	Minutiae
Kovacs-Vajna[61]	2000	Minutiae and its 16 x 16 grayscale neighborhood
Jain et al.52	2001a	Texture features

time-consuming the fingerprint classification executes first instead of comparison against all fingerprints.

4.2. *Related Works*

Table 14 shows the recent related works in fingerprint identification.

4.3. *The state of the art of Fingerprint Recognition*

Fingerprint is one of biometrics that are easily corrupted and damaged. Therefore, in the performance evaluation the quality measurement of samples including image quality check and feature quality check are used. Common used databases in the system evaluation are provided from NIST [32]. Fingerprints have higher uniqueness but depend on genetic factors, social factors, and various factors in collection. Therefore, thorough evaluation and analysis are essential. One of the related works about genetic factors is Jain's twin test. In addition, fingerprints are very sensitive to the impression conditions, humidity, and temperature. Performance evaluation based on these factors is needed [82]. Table 15 shows the performance measures used in the fingerprint recognition researches.

Besides the evaluations with imitated fingerprints are going on for liveness detection of biometrics. It uses dummy fingers and measures mainly the liveness detection performance of input devices [28].

4.4. *Discussion*

As shown in Table 15, most tests of fingerprint recognition systems focus on just algorithm performances such as FRR, FAR etc. However, these simple numerical values are of little importance for the practical uses in real worlds. That is, the

Table 14. State of the art in Fingerprint Recognition

	Author	Year	Methods used	Features used
Preprocessing	Sherlock et al.[93]	1994	Directional Fourier filtering	Minutiae
	Hong et al[38].	1998	Gabor filters	Local orientation and frequency
	Greenberg et al.[34]	2000	Weiner filtering, Gabor filtering	Minutiae
	Jiang[56]	2001	Low pass filter	-
	Hsieh et al.[41]	2003	Wavelet transform	Global texture, local orientation
Feature Extraction	Hung et al.[43]	1996	-	Cores and deltas
	O'Gorman[77]	1999	-	Minutiae
	Jain[49]	1999b	Gabor filter	FingerCode
	Lee et al.[62]	2001	Gabor-basis function	Core, orientation, ridge frequency
Postprocessing	Xiao et al.[120]	1991	Statistical	Minutiae
	Luo et al.[64]	2000	Knowledge-based Minutiae	
	Farina et al.[29]	1999	Elimination algorithms	Minutiae
Classification	Moayer et al.[73], Rao et al.[84]	1975, 1980	Syntactic methods (terminal symbols, production rules)	Directional image
	Candela et al.[18]	1995	Probabilistic neural networks	Minutiae
	Karu et al.[58]	1996	Rule-based	Singular points (cores and deltas)
	Chong[23]	1997	Geometry (B-spline curves)	Global geometric shapes (ridgelines)
	Senior[91]	1997	2-dimensional hidden Markov models	Row features and whole-print row models
	Cappelli et al.[19]	1999	Cost function	Orientation field
	Nagaty[74]	2001	Neural network	Structural and statistical information
	Yao et al.[122]	2003	Recursive neural networks, support vector machines	Flat features (FingerCode), structural features (orientation)
Matching	Hrechak[40]	1990	Structure-based	Minutiae
	Ranade[83]	1993	Point pattern matching (Relaxation approach)	Minutiae
	Chang et al.[22]	1997	Point pattern matching (2-D cluster)	Minutiae
	Sibbald[95]	1997	Correlation-based	Global patterns of ridges
	Jain[49]	1999b	Gabor filter	FingerCode
	Miklos et al.[75]	2000	Point pattern matching(Triangular matching)	Minutiae
	Jiang et al.[55]	2000	Local and global structure matching	Minutiae, Global patterns of ridges
	Jain et al.[52]	2001a	Minutiae-based	Minutiae, texture features
	Horton[39]	2002	Gabor filters	FingerCode
	Ross et al.[88]	2002	Correlation-based	Global patterns of ridges

evaluation tests from various angles are necessary. Biometric has various influence factors as described in section 2 because they are parts of human body. Fingerprints also have many chances that the system acquires different samples against the same person with respect to genetic factors, social factors, environmental conditions and

Table 15. Performance Measures used for Fingerprint Recognition

Author	Year	Performance measures
Khanna et al.[59]	1994	Reliability, selectivity, false hits, consolidation efficiency, search time, encoding time, position summary
Jain et al.[46]	1996	Recognition rates, rejection rates, CPU time
Hong et al. [38]	1998	ROC, FAR, FRR
Wahab et al.[106]	1998	Enrolment time, verification time, FRR, FAR
Jain et al.[49]	1999b	ROC, FAR, FRR
Horton et al.[39]	2002	FAR, FRR, ROC
Jain et al.[54]	2002	ROC, FAR, FRR, EER
He et al.[36]	2003	EER, ZeroFMR, ZeroFNMR, ROC

user conditions. Therefore, it is desirable that the tests process the classes with combining each element of factors via an analysis of each factor. It makes a practical use in real worlds possible.

5. Conclusions

With the increase of need and interest on biometrics, the research is actively conducted in the academic and industry, especially for main biometric features such as fingerprint, face, iris, voice, signature, and so on [121]. Because each biometric feature has merits and demerits, it is hard to say that which biometric feature is superior to the others. Each biometric feature has to be applied for proper applications and environments. Conventional research was focused on biometric systems with individual feature, but recently the research on multi-feature based recognition system spreads to overcome the limit of individual biometric feature. With these progresses, the detailed analyses for biometric features are required and the systemic summaries and evaluations of biometric system make the biometrics more powerful. In addition, proper combinations between modules and features lead to enhanced recognition performance. The main purpose of evaluation is to discriminate the possibility of the system in practice and to understand the weakness and restricted condition for improvement and application of system. Recently evaluations are conducted by several leading groups, but they cannot satisfy users because the evaluations are dependent on FAR/FRR, FMR/FNMR and there are not any detailed analyses of the systems and results. So various measures for analysis have to be developed and many kinds of factors which affect the system must be included in the evaluation. As future works, we analyze each biometric feature with factor-based evaluations, and develop technologies for the weakness of biometric features and systems, especially focused on the following three topics.

o Explicit and implicit characteristics of biometric features
o Analysis of biometric technologies for each biometric feature
o Effective combination methods, i.e., sensor integration and data fusion technologies

Acknowledgements

This work was supported by the Korea Science and Engineering Foundation (KOSEF) through the Biometrics Engineering Research Center (BERC) at Yonsei University.

References

1. J. Adams, "Survey: Biometircs and Smart Cards," *BBT*, pp.8-11, August 2000.
2. Association for Biometrics and Int. Computer Security Association, 1999 Glossary of Biometric Terms, 1999.
3. Common Criteria Biometric Evaluation Methodology Working Group, "Biometric Evaluation Methodology Supplement(BEM)," *Common Criteria Projec, ver 1.0*, August 2002.
4. http://www.bioapi.org/
5. "Comparative Study of Biometric Identification Systems," *BIOIS Study, Public Final Report, Technical Study*, May 2000.
6. http://www.npl.co.uk/npl/sections/this/biotest
7. http://www.biotrust.de/
8. D. M. Blackburn, J. M. Bone, and P. J. Phillips, "FRVT 2000 Evaluation Report Appendices," *Facial Recognition Vendor Test 2000 Documents*, February 2001.
9. D. M. Blackburn, J. M. Bone, and P. J. Phillips, "Facial Recognition Vendor Test 2000 Evaluation Report," *Facial Recognition Vendor Test 2000 Documents*, February 2001.
10. D. M. Blackburn, "Evaluating Technology Properly - Three Easy Steps to Success," Facial Recognition Vendor Test 2000 Documents, Article originally published in Corrections Today, July 2001.
11. R. Bolle, J. Connell, S. Pankanti, N. Ratha, A. Senior, "IBM Research Report : Biometrics 101," *IBM Research Division*, 2002.
12. J. Bone, J. Wayman, and D. Blackburn, "Evaluating Facial Recognition Technology for Drug Control Applications," *ONDCP Int. Technology Symposium*, 2001.
13. J. M. Bone, C. L. Crumbacker (and D.M. Blackburn), "Facial Recognition - Assessing its Viability in the Corrections Environment," *Facial Recognition Vendor Test 2000 Documents, Article originally published in Corrections Today*, vol. 63, July 2001.
14. F. Bouchier, J. S. Ahrens, and G. Wells, "Laboratory Evaluation of the IriScan Prototype Biometric Identifier," *SAND96-103*, 1996.
15. E. Bowman, "Everything You Need to Know About Biometrics," *Identix Corporation*, 2000.
16. Biometrics Working Group(UK), "Best Practices in Testing and Reporting Performance of Biometric Devices," *ver. 1.0*, Jauary 2000.
17. "Biometrics for Identification and Authentication - Advice on Product Selection," *Biometrics Working Group(UK) Issue 1.0*, November 2001.
18. G. T. Candela, P. J. Grother, C. I. Watson, R. A. Wilkinson and C. L. Wilson, "PCASYS-A Pattern-Level Classification Automation System for Fingerprints," *Technical Report NISTIR 5647*, 1995.
19. R. Cappelli, A. Lumini, D. Maio and D. Maltoni, "Fingerprint Classification by Directional Image Partitioning," *IEEE Transations on Pattern Analysis and Machine Intelligence*, vol. 21, no. 5, May 1999.
20. R. Cappelli, A. Erol, D. Maio and D. Maltoni, "Synthetic Fingerprint-image Generation," *Proc. 15th Int. Conference on Pattern Recognition(ICPR2000)*, September

2000.

21. "Common Evaluation Methodology (CEM)," *, ver 1.0*, 2000.
22. S. Chang, F. Cheng, W. Hsu, G. Wu, "Fast Algorithm for Point Pattern Matching: Invariant to Translations, Rotations and Scale Changes," *Pattern Recognition*, vol. 30, no. 2, pp. 311-316, 1997.
23. M. Chong, "Geometric Framework for Fingerprint Image Classification," *Pattern Recognition*, vol. 30, no. 9, pp. 1475-1488, 1997.
24. L. Coetzee and E. C. Botha, 'Fingerprint Recognition in Low Quality Images'," *Pattern Recognition*, vol. 26, no. 10, pp. 1441-1460, 1993.
25. C. Do and M. Hurusawa, "Application of Biometric Fingerprint in m-Commerce," *Consumer Data Link(CDL*, January 2001.
26. P. E. Danielsson and Q. Z. Ye, "Rotation-Invarient Operators Applied to Engancement of Fingerprints," *Proc. Ninth ICPR*, pp. 329-333, 1988.
27. E. C. Driscoll, C. O. Martin, K. Ruby, J. J. Russel and J. G. Watson, "Method and Apparatus for Verifying Identity Using Image Correlation," *US Patent No. 5067162*, 1991.
28. T. Endo, H. Matsumoto, T. Matsumoto, "Comparison between Dry Live Fingers and Artificial Fingers in Fingerprint Authentication," *Technical Report of IEICE, ISEC2001-14*, pp. 17-24, 2000.
29. A. Farina, Z. M. Kovacs-Vajna, and A. Leone, "Fingerprint Minutiae Extraction from Skeletonized Binary Images," *Pattern Recognition*, vol. 32, no. 5, pp. 877-889, 1999.
30. L. Flom and A. Safir, "Iris Recognition System," *US patent 4,631,349, Patent and Trademark Office, Washington, D. C.*, 1987.
31. R. Frischholz, U. Dieckmann, "BioID: A Multimodal Biometric Identification System," *IEEE Computer*, vol. 33, no. 2, 2000.
32. M. D. Garris, R. M. McCabe, "Fingerprint Minutiae from Latent and Matching Tenprint Images," *NIST Special Database 27.*
33. Gartner Dataquest, *Pointing the Finger at Biometric Technology*, June 2001.
34. S. Greenberg, M. Aladjem, D. Kogan, I. Dimitrov, "Fingerprint Image Enhancement Using Filtering Techniques," *Proc. 15th Int. Conference on Pattern Recognition*, vol. 3, pp. 322-325, 2000.
35. M. Hartman, "Compact Fingerprint Scanner Techniques," *Proc. Biometric Consortium Eighth Meeting*, June 1996.
36. Y. He, J. Tian, X. Luo and T. Zhang, "Image Enhancement and Minutiae Matching in Fingerprint Verification," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1349-1360, 2003.
37. L. Hong, A. K. Jain, S. Pankanti, and R. Boole, "Fingerprint Enhancement," *Proc. First IEEE WACV*, pp. 202-207, 1996.
38. L. Hong, Y. Wan and A. Jain, "Fingerprint image enhancement: algorithm, and performance evaluation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, pp. 777-789, 1998.
39. M. Horton, P. Meenen, R. Adhami, and Paul Cox, "The Costs and Benefits of Using Complex 2-D Gabor Filters in a Filter-Based Fingerprint-Matching System," *IEEE 34th Southeastern Symposium on System Theory (SSST)*, pp. 171-175, March 2002.
40. A. K. Hrechak and J. A. McHugh, "Automated Fingerprint Recognition Using Structural Matching," *Pattern Recognition*, vol. 23, pp. 893-904, 1990.
41. C.-T. Hsieh, E. Lai, and Y.-C. Wang, "An Effective Algorithm for Fingerprint Image Enhancement Based on Wavelet Transform," *Pattern Recognition*, vol. 36, no. 2, pp. 303-312, February 2003.

42. D. C. Huang, "Enhancement and Feature Purification of FingerprintImages," *Pattern Recognition*, vol. 26, no. 11, pp. 1661-1671, 1993.
43. D. Hung, C. Huang, and H. Cheng, "Detecting fingerprint singular points by a hierarchical model," *Proc. of the 7th Int. Conference on Signal Processing Applications & Technology (ICSPAT '96)*, pp. 1153-1157, October 1996.
44. "Biometric FAQ," *Int. Biometric Group, ver. 1.0*, 2001.
45. "Comparative Biometric Testing - Official Test Plan 2.0," *Int. Biometric Group, ver 2.0*, 2002.
46. A. K. Jain and L. Hong, "On-Line Fingerprint Verification," *Proc. of ICPR'96*, pp. 596-600, 1996.
47. A. Jain, L. Hong, and R. Bolle, "On-Line Fingerprint Verification," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, pp. 302-314, 1997.
48. A. Jain, R. Bolle and S. Pankanti, *Biometrics - Persnal Identification in Networked Society*, Kluwer Academic Publisher, 1999.
49. A. K. Jain, S. Prabhakar, L. Hong and S. Pankanti, "Fingercode: a Filterbank for Fingerprint Representation and Matching," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 2, pp. 187-193, 1999.
50. A. K. Jain, S. Prabhakar, and S. Chen, "Combining Multiple Matchers for a High Security Fingerprint Verification System," *Pattern Recognition Letters*, vol. 20, pp. 1371-1379, 1999.
51. 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, 2000.
52. A. Jain and S. Prabhakar, "Fingerprint Matching Using Minutiae and Texture Features," *The Int. Conference on Image Processing (ICIP)*, pp. 282-285, October 2001.
53. A. K. Jain, S. Pankanti, S. Prabhakar, and A. Ross, "Recent Advances in Fingerprint Verification," *Invited Paper for 3rd Int. Conference on Audio- and Video-Based Person Authentication*, pp. 182-191, June 2001.
54. A. K. Jain, S. Prabhakar, and S. Pankanti, "On The Similarity of Identical Twin Fingerprints," *Pattern Recognition*, vol. 35, no. 11, pp. 2653-2663, 2002.
55. X. Jiang, W. Yau, "Fingerprint minutiae matching based on the local and global structures," *Proc. of 15th Int. Conference of Pattern Recognition*, pp.1042-1045, 2000.
56. X. Jiang, "A study of fingerprint image filtering," *Proc. Int. Conference on Image Processing*, vol. 3, pp. 238-241, 2001.
57. E. Jones, "The Importance of Benchmarking," *Connecticut Department of Social Services - DSS's Biometric ID Project*, 2000.
58. K. Karu, and A. Jain, "Fingerprint classification," *Pattern Recognition*, vol. 29, no. 3, pp. 389-404, March 1996.
59. R. Khanna, S. Weicheng, "Automated fingerprint identification system (AFIS) benchmarking using the National Institute of Standards and Technology (NIST) Special Database 4," *Proc.. Institute of Electrical and Electronics Engineers 28th Annual 1994 Int. Carnahan Conference on Security Technology*, pp. 188-194, October 1994.
60. J. Kittler, J. Matas, K. Johnson, and M. U. Romas Sanchez, "Combining Evidence in Personal Identity Verification Systems," *Pattern Recognition Letters*, vol. 18, pp. 845-852, 1997.
61. Z. M. Kovacs-Vajna, "A Fingerprint Verification System based on Triangular Matching and Dynamic Time Warping," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 22, no. 11, 2000.
62. C.-J. Lee and S.-D. Wang, "Fingerprint feature reduction by principal gabor basis

function," *Pattern Recognition*, vol. 34, no. 11, pp. 2245-2248, November 2001.

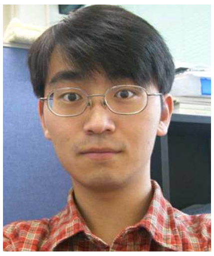
63. S. Liu and M. Silverman, "A Practical Guide to Biometric Security Technology," *IEEE Computer Society IT Pro*, Jan-Feb, 2001.
64. X. P. Luo and J. Tian, "Knowledge-based fingerprint image enhancement," *Proc. Int. Conference on Pattern Recognition*, vol. 3, pp. 783-786, 2000.
65. D. Maio, D. Maltoni, and S. Rizzi, "An Efficient Approach to On-Line Fingerprint Verification," *Proc. Int. Symposium on Artificial Intelligence*, pp. 132-138, 1995.
66. D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2000: Fingerprint Verification Competition," *roc. of Int. Conference on Pattern Recognition*, September 2000.
67. D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Second Fingerprint Verification Competition," *Proc. of Int. Conference on Pattern Recognition*, August 2002. , "," , March 19, 2001.
68. T. Mansfield, G. Kelly, D. Chandler, and J. Kane, "Biometric product testing final report," *Centre for Mathematics and Scientific Computing National Physical Laboratory Queen's Road, CESG/BWG Biometric Test Programme CESG contract X92A/4009309*, March 2001.
69. A. Mansfield and J. L. Wayman, "Best Practices in Testing and Reporting Performance of Biometric Devices," *ver 2.0*, August 2002.
70. R. A. Marsh and G. S. Petty, "Optical Fingerprint Correlator," *US Patent 5050220*, 1991.
71. A. Martin, G. Doddington, T. Kamm, M. Ordowski, M.Przybocki, "The DET curve in Assessment of Detection Task Performance," *Proc. Of Eurospeech'97*, vol. 4, pp. 1895-1898, 1997.
72. Z. Miklos, Z. Kovacs-Vajna, "A fingerprint verification system based on triangular matching and dynamic time warping," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 11, 2000.
73. B. Moayer and K. S. Fu, "A syntactic approach to fingerprint pattern recognition," *Pattern Recognition*, vol. 7, pp.1-23, 1975.
74. K. A. Nagaty, "Fingerprint classification using artificial neural networks: a combined structural and statistical approach," *Neural Networks*, vol. 14, no. 9, pp. 295-309, November 2001.
75. M. Negin, et al, "An Iris Biometric System for Public and Personal Use," *Computer and Information Science(CIS) Penn Engineering, IEEE Computer*, vol.33, no.2, pp.70-75, February 2000.
76. NTL Group, "Technical Evaluation Criteria for the Assessment and Classification of Biometric Systems," *http://homepage.ntlworld.com/avanti/bsi1.pdf*, August 2000.
77. L. O'Gorman, "Fingerprint Verification," *in Biometrics: Personal Identification in a Networked Society, Kluwer Academic Publishers*, pp. 43-64, 1999.
78. P. J. Phillips, H. Wechsler, J. Huang, and P. Rauss, "The FERET Databases and Evaluation Procedure for Face-Recognition Algorithms," *Image and Vision Computing Journal*, vol. 16, no. 5, pp. 295-306, 1998.
79. P. J. Philips, A. Martin, C. L. Wilson, and M. Przybocki, "An Introduction to Evaluating Biometric Systems," *National Institude of Standards and Technology(NIST)*, pp. 56-63, February, 2000. , "," , vol. 22, no. 10, pp. 1090-1104, October, 2000.
80. P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET evaluation methodology for face-recognition algorithms," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, pp. 1090-1104, October 2000.
81. S. Prabhakar and A. K. Jain, "Decision-Level Fusion in Fingerprint Verification," *Pattern Recognition*, vol. 35, no. 4, pp. 861-874, 2002.

82. T. van der Putte and J. Keuning, "Biometrical Fingerprint Recognition Don't Get Your Fingers Burned," *Esire, an Origin Extended Enterprise*, 2000.
83. A. Ranade and A. Rosenfeld, "Point pattern matching by relaxation," *Pattern Recognition*, vol. 12, no. 2, pp. 269-275, 1993.
84. K. Rao amd K. Balck, "Type classification of fingerprints: a syntactic approach," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 2, no. 3, pp. 223-231, 1980.
85. D. Zhang, W.-K. Kong, J. You, and M. Wong, "Online Palmprint Identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 9, pp. 1041-1050, 2003.
86. S. A. Rizvi, P. J. Philips and Hyeonjoon Moon, "The FERET Verification Testing Protocol for Face Recognition Algorithms," *Image and Vision Computing Journal, Technical report NISTIR 6281*, October, 1998.
87. A. Roddy and J. Stosz, "Fingerprint features – statistical analysis and system performance estimates," *Proceedings of IEEE*, vol. 85, no. 9, pp. 1390-1421, 1997.
88. A. Ross, J. Reisman and A. K. Jain, "Fingerprint Matching Using Feature Space Correlation," *Proc. of Post-ECCV Workshop on Biometric Authentication*, June 2002.
89. A. Samal and P. Iyengar, "Automatic recognition and analysis of human faces and facial expressions: A survey," *Pattern Recognition*, vol. 8, no. 25, pp. 65-77, 1992.
90. R. Sanchez-Reillo, C. Sanchez-Avila and A. Gonzalez-Marcos, "Biometric Identification through Hand Geometry Measurements," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, October 2000.
91. A. Senior, "A hidden markov model fingerprint classifier," *Proc. 31st Asilomar Conference on Signals, Systems, and Computers*, pp. 305-310, 1997.
92. W. Shen, M. Surette, and R. Khanna, "Evaluation of automated biometrics-based identification and verification systems," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1464-1478, 1997.
93. B. G. Sherlock, D. M. Monro and K. Millard, "Fingerprint enhancement by directional Fourier filtering," *IEEE Proc. On Vision, Image and Signal Processing*, vol. 141, no. 2, pp. 87-94, April 1994.
94. A. Sherstinsky and R.W. Picard, "Restoration and Enhancement of Fingerprint Images Using M-Lattice: A Novel Non-Linear DynamicalSystem," *Proc. 12th ICPR-B*, pp. 195-200, 1994.
95. A. Sibbald, "Method and Apparatus for Fingerprint Characterization and Recognition Using Auto-Correlation Pattern," *US Patent 5633947*, 1997.
96. V. Skerpac, "Got Biometrics?," *Information Security Bulletin*, April, 2000.
97. B. Souheil, Y. Abdeljaoued, E. Mayoraz, "Fusion of face and speech data for person identity verification," *IEEE Transactions on Neural Networks*, vol. 10, no. 5, pp. 1065-1074, 1999.
98. J. Stapleton, "Biometrics," *PKI Forum*, May 2001.
99. R. G. Steen, D̂NA and Destiny: Nature and Nurture in Human Behavior, New York: Plenum Press, 1996.
100. Y. Sun, M.A. Abidi, "Surface Matching by 3D Point's Fingerprint," *Proc. of the IEEE Int. Conference on Computer Vision*, vol. 2, pp.263-269, 2001.
101. http://www.afb.org.uk
102. http://www.ansi.org
103. http://www.biometrics.org/html/standards.html
104. http://www.cesg.gov.uk/technology/biometrics
105. http://www.nist.gov
106. A. Wahab, S. H. Chin and E. C. Tan, "Novel approach to automated fingerprint

recognition," *IEEE Proceedings -Vis. Image Signal Process*, vol. 145, no. 3, pp. 160-166, June 1998.

107. J. Wayman, L. Alyea, "Picking the Best Biometric for Your Application," *in National Biometric Test Center Collected Works, vol. 1*, pp. 269-275, 2000.
108. J. L. Wayman, "Error Rate Equations for the General Biometric System," *IEEE Robotics and Automation*, vol. 6, no. 1, pp. 35-48, March 1999.
109. J. L. Wayman, "Technical Testing and Evaluation of Biometric Devices," *Biometrics - Personal Identification in Networked Society, Kluwer Academic Publisher*, 1999.
110. J. Wayman, "The Functions of Biometric Identification Devices," *San Jose, CA:National Biometric Test Center, vol. 2000*, 2000.
111. J. Wayman, "Technical Testing and Evaluation of Biometric Identification Devices," *in National Biometric Test Center Collected Works, vol. 1*, pp. 65-87, 2000.
112. J. L. Wayman, "The Philippine AFIS Benchmark Test," *National Biometric Test Center Collected Works, 1997-2000*, September 2000.
113. J. L. Wayman, "National Biometric Test Center Collection Works 1997-2000," *Research at San Jose State University, ver 1.3*, August 2000.
114. J. Wayman, L. Alyea, "A Definition of "Biometrics," *in National Biometric Test Center Collected Works, vol. 1*, pp.21-23, 2000.
115. J. L. Wayman, "Biometrics: The State of the Technology," *Biometric Technic Center, San Jose university, Biometric Technology, CardTech/SecurTech 2001*, pp. 1-14, May 2001.
116. J. L. Wayman, "Fundamentals of biometric authentication technologies," *Int. Journal of Image and Graphics*, vol. 1, no. 1, pp. 93-113, 2001.
117. B. Wirtz, "Biometric Systems 101 and Beyond," *Infineon Technologies AG, Technofile*, pp, 12-21.
118. J. Woodward, K. Webb, E. Newton, M. Bradley, D. Rubenson, "Army Biometric Applications: Identifying and Addressing Sociocultural Concerns," *RAND*, 2001.
119. X. Xia, and L. O'Gorman, "Innovations in Fingerprint Capture Devices," *Pattern Recognition*, vol. 36, no.2, pp. 361-369, 2003.
120. Q. Xiao and H. Raafat, "Fingerprint image postprocessing: a combined statistical and structural approach," *Pattern Recognition*, vol. 24, no. 10, pp. 985-992, 1991.
121. M. Yang, D. Kriegman, N. Ahuja, "Detecting faces in images: a survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 1, pp. 34-58, 2002.
122. Y. Yao, G. L. Marcialis, M. Pontil, P. Frasconi, and F. Roli, "Combining flat and structured representations for fingerprint classification with recursive neural networks and support vector machines," *Pattern Recognition*, vol. 36, no. 2, pp. 397-406, February 2003.
123. E. N. Zois and V. Anastassopoulos, "Fusion of Correlated Decisions for Writer Verification," *Pattern Recognition*, vol. 34, no. 1, pp. 47-61, 2001.
124. A. Zwiesele, A. Munde, C. Busch, H. Daum, "BioIS Study-Comparative Study of Biometric Identification Systems," *34th Annual 2000 Int. Carnahan Conference on Security Technology: 34rd Annual IEEE Conference*, pp. 60-63, 2000.

Photo and Bibliography



Jin-Hyuk Hong received the B.S. and M.S. degree in computer science from Yonsei University, Seoul, Korea, in 2002 and 2004, respectively. Since 2004, he has been a Ph.D. student in the Department of Computer Science, Yonsei University. His research interests include evolutionary computation, conversational intelligent agent, and game strategy generation.

Eun-Kyung Yunreceived the B.S. and M.S. degree in computer science from Yonsei University, Seoul, Korea, in 2002 and 2004, respectively. Since 2004, she has worked on Samsung Electronics, Korea. Her research interests include biometrics, pattern classification, and robot control.

Sung Bae Cho received the B.S. degree in computer science from Yonsei University, Seoul, Korea, in 1988 and the M.S. and Ph.D. degrees in computer science from KAIST (Korea Advanced Institute of Science and Technology), Taejeon, Korea, in 1990 and 1993, respectively. He worked as a Member of the Research Staff at the Center for Artificial Intelligence Research at KAIST from 1991 to 1993. He was an Invited Researcher of Human Information Processing Research Laboratories at ATR (Advanced Telecommunications Research) Institute, Kyoto, Japan from 1993 to 1995, and a Visiting Scholar at University of New South Wales, Canberra, Australia in 1998.

Since 1995, he has been an Associate Professor in the Department of Computer Science, Yonsei University. His research interests include neural networks, pattern recognition, intelligent man-machine interfaces, evolutionary computation, and artificial life. Dr. Cho was awarded outstanding paper prizes from the IEEE Korea Section in 1989 and 1992, and another one from the Korea Information Science Society in 1990. He was also the recipient of the Richard E. Merwin prize from the IEEE Computer Society in 1993. He was listed in Who's Who in Pattern Recognition from the International Association for Pattern Recognition in 1994, and received the best paper awards at International Conference on Soft Computing in 1996 and 1998. Also, he received the best paper award at World Automation Congress in 1998, and listed in Marquis Who's Who in Science and Engineering in 2000 and in Marquis Who's Who in the World in 2001. He is a Member of the Korea Information Science Society, INNS, the IEEE Computer Society, and the IEEE Systems, Man, and Cybernetics Society.