

지문 식별을 위한 동적 임계치 설정방법

Dynamic Thresholding Scheme for Fingerprint Identification

김 경 민*, 이 범, 박 중 조, 정 순 원
(Kyoung-Min Kim¹, Buhm Lee¹, Joong-Jo Park², and Soon-Won Jung³)

¹Chonnam National University

²Gyeongsang National University

³Ria Soft

Abstract: This paper proposes dynamic thresholding scheme for fingerprint identification. As a user authentication method by fingerprint recognition technology, verification method based on 1:1 matching was mainly used in the past, but identification method based on 1:N matching is generally used recently. The control of the value of FAR is very important in the application areas such as access control and time attendance systems. This paper proposes dynamic thresholding scheme which could properly control the value of FAR according to the field of applications and size of the fingerprints database.

Keywords: labeling, feature, defect inspection, neighbor

I. 서론

지문 인식은 생체인식의 여러 분야 가운데서도 가장 오랫동안 성공적인 생체인식의 수단으로 받아들여져 온 분야이다. 지문은 땀샘이 융기하여 일정한 흐름을 형성한 것으로, 태어날 때의 모습 그대로 평생 동안 변하지 않는다는 것이 일찍부터 증명되어 오래 전부터 범죄 수사용으로 이용되어 왔으며, 최근에는 정확한 개인인증을 필요로 하는 다양한 분야에 적용되고 있다[1].

지문인식시스템은 일반적으로 지문 입력 장치와 인식 알고리즘으로 구성되며, 지문인식 알고리즘은 크게 특징점 데이터 추출과정과 매칭과정으로 나누어진다. 통상 많이 사용되는 특징점(minutiae) 기반의 지문인식 알고리즘에 있어서 특징점 데이터 추출과정을 좀 더 상세히 살펴보면, 입력된 지문에 대하여 영상의 전처리, 융선의 방향 검출, 영상의 이진화, 세션화 등의 처리과정을 거치게 되며, 이러한 과정을 통해 지문의 특징점 데이터라 불리는 융선의 끝점, 분기점의 위치와 방향성분을 추출할 수 있다[2,3].

두 지문으로부터 추출된 특징점 데이터의 매칭 여부를 판단하기 위해서는 특징점간의 기하학적 유사성을 분석하여 매칭 점수를 계산하며, 계산된 매칭 점수가 미리 정해진 임계값(threshold value)을 넘는 경우 두 지문이 매칭된 것으로 판단한다. 동일한 지문 매칭 알고리즘에 대하여 임계값을 변화시키면 오인식률(FAR: False Acceptance Ratio) 및 오거부율(FRR: False Rejection Ratio)이 변화되며, 응용분야

에 따라 임계값이 다르게 설정되어 사용된다[4-6]. 통상, 응용분야에 따른 임계값 변경 시에는 사용자의 편의를 위해서 임계값을 직접 사용자가 설정하지는 않고 FAR 및 FRR 값과 연계된 보안 레벨(security level)이라는 개념을 도입하여 사용자로 하여금 이 값을 조정하도록 한다. 표 1은 보안 레벨에 따른 FAR 및 FRR 값의 예를 보여준다. 잘 알려진 바와 같이, 이 FAR 및 FRR 값은 사용되는 지문인식 알고리즘에 따라 크게 변할 뿐 아니라 테스트에 사용되는 지문 DB의 품질에 따라서도 큰 영향을 받는다[7,8,13].

한편, 지문 인식 시스템이 점차 널리 보급됨에 따라 사용자의 요구가 다양해지고 복잡해지고 있는데, 사용자의 중요한 요구 중 하나가 1:N 지문 식별(identification)에 관련된 요구이다. 잘 알려져 있는 바와 같이 지문 인식 시스템은 두 가지 모드로 동작할 수 있는데, 1:1 지문 검증 모드(verification mode)는 인증 받고자 하는 본인의 ID와 지문을 입력하면, 저장되어 있는 지문 특징점 데이터 중 ID에 해당하는 지문 특징점 데이터(template)와 입력된 지문으로부터 추출한 특징점 데이터를 매칭시키는 모드이고, 1:N 지문 식별 모드(identification mode)는 지문만을 입력하여 전체 지문 특징점 데이터 중 일치하는 지문이 있는지를 판별하는 모드이다. 즉, 지문 식별 모드의 경우, 사용자는 본인의 ID입

표 1. 보안레벨에 따른 FAR 및 FRR 값(%).

Table 1. FAR, FRR Value for a Security Level (%).

보안레벨	0	1	2	3	4
FAR(%)	1.0006	0.5010	0.2515	0.1000	0.0316
FRR(%)	0.1190	0.1480	0.2220	0.3410	0.5490
보안레벨	5	6	7	8	9
FAR(%)	0.010	0.0031	0.001	0.0003	0.0001
FRR(%)	0.786	1.0530	1.335	1.8390	2.5800

* 책임저자(Corresponding Author)

논문접수: 2012. 2. 8., 수정: 2012. 7. 1., 채택확정: 2012. 7. 31.

김경민, 이범: 전남대학교 전기전자통신컴퓨터공학부

(kkm@jnu.ac.kr/buhmlee@jnu.ac.kr)

박중조: 경상대학교 제어계측공학과(jjpark@nongae.gsnu.ac.kr)

정순원: (주) Ria Soft(jsw123@naver.com)

※ 본 논문은 2010년 전남대학교 연구원 지원에 의한 것임.

력 없이 지문만 입력하면 되므로 편리성 측면에서 우수한 방법이라고 할 수 있다.

지문 인식 시스템을 검증 모드로 운영하는데 있어서, 표 1을 기준으로 보안레벨을 '3'으로 설정했다고 가정하면, FAR = '0.1%', FRR = '0.341%'의 인식성능을 보일 것이다. 그러나, 동일한 지문 인식 시스템을 식별 모드로 운영할 경우 보안레벨을 동일하게 '3'으로 설정하면 FRR 값은 동일하게 유지되나 FAR 값은 변한다. 왜냐하면 지문 식별을 위해서는 지문 검증에 비해 다수의 매칭이 필요하고, 확률적으로 볼 때 매칭 횟수가 많아지면 많아질수록 FAR 값이 커지기 때문이다. 따라서 지문 식별 모드로 지문 인식 시스템을 운영하는 경우, 지문 검증모드에서의 보안레벨과는 별도로 지문 식별 모드에서의 보안레벨을 설정하여 사용한다. 예를 들면 표 1을 기준으로 하여, 지문 검증 모드에서의 보안레벨은 '3'으로 사용하고, 지문 식별 모드에서의 보안레벨은 '7'로 설정하는 식으로 운영을 하는 것이다.

그러나 지문 식별 모드에서의 보안레벨을 이렇게 고정 값으로 운영하는 경우, 운영상의 편리함은 있으나 지문 인식 시스템의 성능, 특히 FAR 값을 안정적으로 보장해주지 못하는 단점이 있다. 이러한 문제를 해결하기 위해서는, 지문 데이터베이스의 크기, 응용분야 등을 고려하여 보안레벨을 가변적으로 적용하는 동적 임계치 설정 기법(dynamic thresholding scheme)이 필요하다. 그동안 지문 인식 분야에 있어 동적 임계치 설정 기법은 학술적이나 수학적 해석을 통한 정량적인 방법보다는 휴리스틱(Huristic)한 임계치 설정 방법을 통해, 실제 지문 인식 기기를 사용하는 환경하에서 사용자의 편의성을 증대시키거나 상황에 따라 보안성을 증대시키는 방법이 제시되었다.

먼저 Sullivan [9]은 표 1과 같은 데이터가 주어진 지문 인식 시스템에서, 기준 FAR, FRR을 설정한 후, 실제 사용자가 인증에 성공할 때마다 인증성공 매칭점수 및, 타 템플릿과의 매칭점수(impostor matching scores)를 구하여 표 1을 업데이트시킴으로서 임계치를 동적으로 설정한 효과를 내는 방법을 제시하고 있다. Lo [10]는 기준 FAR, FRR을 설정해 놓지 않고, 사용자의 지문을 등록하는 시점에 타 템플릿과의 매칭점수를 구한 후, 가장 큰 매칭점수를 기초로 하여 해당 사용자에 대한 매칭 임계치를 설정함으로써 고정된 임계치가 아니라 개인별로 다른 임계치를 사용하게 하는 방법을 제시하고 있다. 이러한 방법들은 모두 동적 임계치를 사용함으로써 사용자의 편의성이나 보안성을 증대시키는 방법으로 사용될 수 있으나, 등록된 지문 데이터베이스가 커지면 커질수록 적용에 어려움이 있으며, 통상 대용량의 데이터베이스를 기준으로 측정된 표 1과 같은 알고리즘 성능지표를 정량적으로 구할 수 없는 문제가 있다. 또한 본 논문에서 제시하는 인식(identification)모드에 있어서 매칭 임계치를 동적으로 설정하는 기법이 아니라 개별 인증(verification)모드에만 적용 가능한 기법들을 제시하고 있다.

이에 본 논문에서는 지문 식별 시스템에 있어서, 매칭 임계치를 상황에 따라 가변적으로 적용하되 알고리즘 성능지표를 정량적으로 예측할 수 있고, 지문 인식 시스템의 보안성을 안정적으로 보장할 수 있는 기법을 제안하고자 한다.

II. 지문 식별 시스템

본 장에서는 지문 식별 시스템이 적용되는 다양한 상황에 대해 살펴보도록 한다.

1. 근태관리(time and attendance)/출입통제(access control)

지문 식별에 있어서 가장 기본적인 방법인 순차 검색(sequential search)은 입력된 지문으로부터 특징점 데이터(minutiae data)를 추출한 후, 데이터베이스에 저장되어 있는 템플릿들과 순차적으로 비교하는 것이다. 그림 1은 순차 검색에 대한 개념도를 보여준다. 근태관리의 목적으로 지문 식별시스템을 운영하는 경우처럼, 매칭될 지문이 데이터베이스에 저장되어 있다고 가정하고 지문을 입력할 때, 데이터베이스의 크기를 n , 오거부율을 FRR 이라 가정하면, 순차 검색에 있어서 평균 매칭횟수는 식 (1)과 같이 구할 수 있다. 만일, $FRR \ll 1$ 인 경우에 식 (1)은 식 (2)로 근사 가능하다.

$$M_{avg} = (1 - FRR) * \frac{(n+1)}{2} + FRR * n \quad (1)$$

$$M_{avg} = \frac{1}{2} * (n+1) \quad (2)$$

예를 들어 그림 1에서 DB의 크기가 '100'이고 오 거부율이 ' $FRR \ll 1$ '이라 가정하면, 최소의 매칭 횟수는 '1'이고 최대 매칭 횟수는 '100'이며, 평균 매칭 횟수는 식 (2)에 따라 '50.5'회가 된다.

한편, 출입통제의 경우에도 등록된 사용자가 인증을 시도하는 경우에는 근태관리의 경우와 마찬가지로 식 (1), 식 (2)에 의해 평균 매칭횟수를 구할 수 있으나, 출입통제의 경우에는 그 특성상 등록되지 않은 사용자가 등록되지 않은 지문으로 인증을 시도할 경우를 반드시 고려해야 하며, 이럴 경우 매칭횟수는 데이터베이스의 크기와 동일한 n 이 된다.

2. 데이터베이스 분류(classification)에 따른 지문 식별

순차검색 방법으로 지문 식별을 수행할 경우, 데이터베이스의 크기가 커지면 커질수록 평균 검색 시간이 길어진다. 이러한 문제를 해결하기 위하여 데이터베이스 전체가 아닌 일부에 대해서만 매칭을 수행하는 기법이 사용되며, 전체 데이터베이스 중 매칭의 대상이 되는 일부 데이터베이스를 선정하는데 분류(classification) 기법이 사용된다. 분류는 크게 텍스트추출(textual) 기반의 분류 및 콘텍스트추출

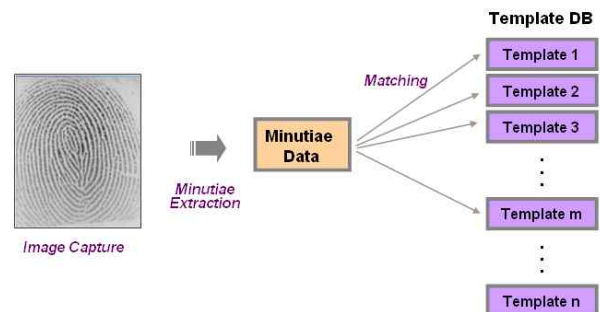


그림 1. 순차 검색 개념도.

Fig. 1. Sequential search scheme.

(contextual) 기반의 분류 방법이 사용된다.

텍스트추얼 기반의 분류는 지문 템플릿에 대한 ID와 같은 텍스트 부가정보를 이용하여 분류를 수행하는 것이다. 예를 들면, 사용자가 지문 식별 시스템을 사용하는 데 있어서, 사용자 ID의 첫자리 숫자를 입력한 후, 지문을 입력하는 경우를 가정해보자. 만일 ID가 네자리이고 [0000 ~ 9999] 사이의 범위에 골고루 퍼져있다면, ID의 첫자리 숫자를 입력한 후, 지문을 입력하면 지문 인식에 사용되는 데이터베이스의 크기는 약 1/10로 줄어드는 것을 쉽게 알 수 있다. 쉽게 예상할 수 있듯이, ID 두자리를 입력하면 검색에 사용되는 데이터베이스의 크기는 약 1/100로 줄어든다. 만일 사용자가 원하는 ID로 데이터베이스가 구성될 경우, ID가 [0000 ~ 9999] 구간내에서 골고루 분포하지 않을 수 있는데, 이를 경우를 방지하기 위하여 지문 등록시 ID와 별도로 그룹 ID를 부여하고, 지문 식별시 이 그룹 ID를 사용하게 함으로서 텍스트추얼 기반의 분류 효과를 극대화시키도록 하기도 한다.

컨텍스트추얼(contextual) 기반의 분류 방법은 지문 등록시 지문 원영상 이나 특징 데이터에 함의된(implicit) 정보를 이용하여 분류를 하는 것이다[11,12]. 지문의 원영상 으로부터 추출할 수 있는 대표적인 컨텍스트추얼 정보는 용선의 흐름 으로부터 추출한 것으로서 이 정보를 특징점 정보와 함께 템플릿에 저장한다. 지문인식을 위해 미지의 지문이 입력되면 입력된 지문으로부터 컨텍스트추얼 정보를 추출한 후, 등록된 지문 중 동일하거나 유사한 컨텍스트추얼 정보를 가지는 템플릿들만을 분류하여 매칭을 수행한다. 이럴 경우 매칭 대상이 되는 템플릿 개수 n' 은 전체 데이터베이스 크기 n 에 비해 작다. 다만, n'/n 이 작아지면 작아질수록 매칭시간이 줄어들 수 있는 반면 비닝 에러(binning error)로 불리는 분류 에러가 커진다.

매칭 대상이 되는 템플릿의 갯수를 n' , 오거부율을 FRR 이라 가정하면, 평균 매칭횟수는 식 (1)과 유사한 식 (3)으로 구할 수 있다. 만일, $FRR \ll 1$ 인 경우에 식 (3)은 식 (4)로 근사 가능하다.

$$M_{avg} = (1 - FRR) * \frac{(n' + 1)}{2} + FRR * n' \quad (3)$$

$$M_{avg} = \frac{1}{2} * (n' + 1) \quad (4)$$

이 경우에도 등록되지 않은 사용자가 등록되지 않은 지문으로 인증을 시도할 경우를 고려하면, 매칭횟수는 매칭 대상이 되는 템플릿의 갯수와 동일한 n' 이 된다.

III. 지문 식별을 위한 동적 임계치 설정방법

앞장에서 살펴본 바와 같이 동일한 데이터베이스라 하더라도 응용분야 및 분류 기법에 따라 지문인식에 있어서의 매칭횟수는 큰 차이를 보이며, 이 매칭횟수에 따라 시스템의 오인식률 값이 크게 좌우된다. 통계학적으로 볼 때, 지문 검증에 있어서의 오인식률을 FAR 이라 하고, 매칭되지 않는 지문에 대해 N 번 연속 매칭하여 오인식할 확률을 FAR_N 이라 하면 FAR 과 FAR_N 의 관계는 식 (5)로 나타낼 수 있다. 또한, 특정 조건이 만족되면 식 (5)는 식 (6)과 같

이 근사적으로 나타낼 수 있다.

$$FAR_N = 1 - (1 - FAR)^N \quad (5)$$

$$FAR_N \approx N * FAR \quad (\text{if, } FAR \ll \frac{1}{N} \ll 1) \quad (6)$$

먼저 식 (1) 혹은 식 (2)의 경우를 살펴보면, M_{avg} 의 의미는 매칭에 성공하기까지의 평균 매칭 횟수를 의미하므로 매칭되지 않는 지문에 대해 $(M_{avg} - 1)$ 회만큼 연속 매칭했다는 의미가 되며, 이를 식 (5) 혹은 식 (6)에 대입하면 식 (7), 식 (8), 식 (9)를 얻을 수 있다.

$$FAR_{M_{avg}-1} = 1 - (1 - FAR)^{(M_{avg}-1)} \quad (7)$$

$$FAR_{M_{avg}-1} \approx (M_{avg} - 1) * FAR \quad (8)$$

$$FAR_{M_{avg}-1} \approx M_{avg} * FAR \quad (\text{if, } M_{avg} \gg 1) \quad (9)$$

출입통제의 경우처럼 등록되지 않은 지문으로 인증을 시도할 경우를 고려하면 매칭횟수는 데이터베이스의 크기와 동일한 n 이 되는데, 이 경우에는 매칭되지 않는 지문에 대해 n 번 연속 매칭하는 것이므로 이를 식 (5) 혹은 식 (6)에 대입하면 식 (10), 식 (11)을 얻을 수 있다.

$$FAR_n = 1 - (1 - FAR)^n \quad (10)$$

$$FAR_n \approx n * FAR \quad (11)$$

식 (9), 식 (11)에 의하면 지문 검증에 있어서의 오인식률을 FAR 이라 할 때, 지문 식별에 있어서는 오인식률 값이 매칭횟수에 거의 정비례하여 커지는 것을 알 수 있다. 또한, 등록된 지문으로 지문인식을 시도하는 경우에 비해 등록되지 않은 지문으로 인증을 시도할 경우, 오인식률 값이 대략 두 배 정도인 것을 알 수 있다.

살펴본 바와 같이, 지문 식별을 수행할 시에는 지문 검증 목적으로 설정된 임계치에 의한 오인식률의 값이 크게 변하므로, 지문 식별시에도 오인식률의 유지를 위해서는 지문 식별의 대상이 되는 데이터베이스의 크기를 고려하여 매칭 임계치를 적절히 재설정해 주어야 한다. 그림 2는 지문 식별 수행시 매칭횟수에 따라 오인식률이 변할 때 임계

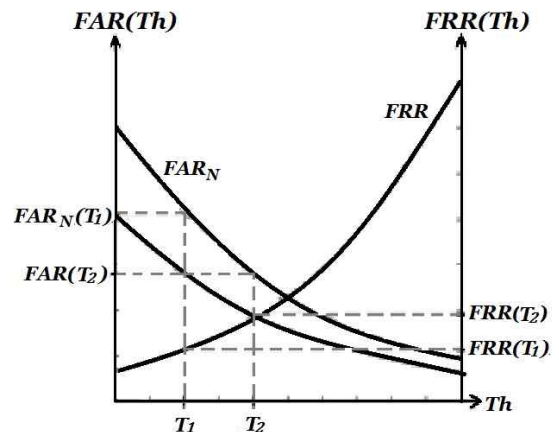


그림 2. 동적 임계치 설정 방법.
Fig. 2. Dynamic Thresholding Scheme.

치를 어떻게 적절히 설정할 수 있는가를 예를 들어 설명해 준다. 가로축은 임계치를 나타내며, 세로축은 오인식률과 오거부율을 각각 로그 스케일로 나타내었다.

지문 검증에 있어서 매칭 임계치가 T_1 인 경우를 가정해 보자. 이 경우 그림에서 보는 바와 같이 오인식률 값은 $FAR(T_1)$ 이고 오거부율 값은 $FRR(T_1)$ 이다. 만일 동일한 매칭 알고리즘을 이용하여 지문 식별시스템에 사용할 때, 매칭되지 않는 지문에 대해 N 번 연속 매칭하여 오인식률 확률을 FAR_N 이라 하면, 매칭 임계치 T_1 에 대하여 $FAR(T_1)$ 은 그림에서 보는 바와 같이 커진다. 지문 식별시스템에서도 지문 검증 시스템에서의 오인식률인 $FAR(T_1)$ 값을 유지하기 위해서는 새로운 매칭 임계치 T_2 를 선정하여 적용하면 된다. 매칭 임계치가 커지므로 오거부율 값은 $FRR(T_1)$ 에서 $FRR(T_2)$ 로 커진다. 식 (6)을 기준으로 T_2 선정 방법을 식으로 표현하면 다음과 같다.

$$FAR_N(T_2) = FAR(T_1) \tag{12}$$

$$T_2 = FAR^{-1}\left\{\frac{1}{N} * FAR(T_1)\right\} \tag{13}$$

IV. 실험 및 결과

그림 3은 실제 지문 데이터베이스에 대하여 실험을 통해 동적으로 임계치를 설정하는 예를 보여준다. 가로축은 임계치를 나타내며, 세로축은 각각 오인식률과 오거부율의 [%] 값을 로그 스케일로 표시하고 있다. 동일한 지문 데이터베이스에 대하여 특징점 추출 알고리즘 및 매칭 알고리즘에 따라 그래프의 형태는 차이를 보일 수 있으나 동적으로 임계치를 설정하는 방법은 동일하게 적용할 수 있다.

먼저, 지문 검증에 있어서의 임계값을 T_1 이라 하면, 그에 따른 오인식률은 $FAR(T_1)$ 이 된다. 만일 데이터베이스의 크기가 커져서 식 (9)나 식 (11)의 평균매칭횟수 혹은 데이터베이스 사이즈가 '10'이 될 경우를 고려해보면 $FAR(T_1)$ 값은 $FAR_{10}(T_1)$ 으로 커진다. 데이터베이스가 커짐에도 불구하고 오인식률 값을 유지하기 위해서는 임계값을 크게 하여야 하며, 식 (13)에 따라 오인식률 값을 유지하는 임계값으로 T_2 를 선정할 수 있다. 임계값을 T_1 에서 T_2 로 변경함에 따라 오거부율은 $FRR(T_1)$ 에서

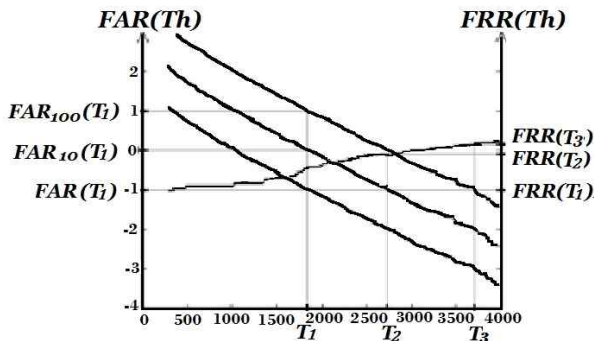


그림 3. 동적 임계치 설정의 예.
Fig. 3. Example of Dynamic Thresholding Scheme.

표 2. 임계값에 따른 오인식률 및 오거부율 (%).
Table 2. FAR and FRR for the Dynamic Thresholding.

	FAR	FAR_{10}	FAR_{100}	FRR
T_1 (1860)	0.1	1	10	0.365
T_2 (2740)	-	0.1	1	0.809
T_3 (3700)	-	-	0.1	1.520

$FRR(T_2)$ 로 커진다. 평균매칭횟수 혹은 데이터베이스의 크기가 '100'이 될 경우에도 동일한 과정을 거쳐 T_3 및 오인식률 값을 구할 수 있다. 표 2는 데이터베이스의 크기가 변함에 따라 오인식률 값을 유지하기 위해 임계값이 어떻게 변하고, 또한 오거부율 값이 어떻게 변하는 지 구체적으로 보여준다.

V. 결론

본 논문에서는 지문 인식에 있어서, 매칭 임계치를 동적으로 설정하는 방법을 제안하였다. 출입통제나 근태관리 목적의 응용 분야에 식별방법이 사용되는 경우 오인식률 값의 제어는 매우 중요하므로, 본 논문에서는 적절한 오인식률 값의 제어를 위하여 응용분야 및 생체정보 데이터베이스의 크기에 따라 매칭 임계값을 동적으로 변경시켜 지문 인식 시스템의 보안성을 확보할 수 있는 방법을 제안하였다. 이 방법을 적용하면 시스템에 목적에 맞게 설정된 오인식률 값이 데이터베이스의 크기와 무관하게 항상 일정하게 유지되는 장점이 있다. 제안한 방법을 실제 데이터베이스에 적용하여 데이터베이스의 크기에 맞추어 임계치를 동적으로 설정할 수 있음을 보였다.

향후 연구과제로는 데이터베이스 분류에 따른 지문 식별 기법에 있어서, 지문 특징점 데이터정보와 밀접하게 연관된 컨텍스트추출 정보를 사용할 경우에 적용할 수 있는 동적 임계치 설정 방법을 개발하는 것이다.

참고문헌

- [1] A. K. Jain, R. Bolle, and S. Pankaniti(Eds), *Biometrics: Personal Identification in Networked Society*, Kluwer Academic, NewYork, 1999.
- [2] N. K. Ratha, S. Y. Chen, and A. K. Jain, "Adaptive flow orientation-based feature extraction in fingerprint images," *Pattern Recognition*, vol. 28, no. 11, pp. 1657-1672, 1995.
- [3] C. Arcelli and G. S. D. Baja, "A width independent fast thinning algorithm," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 4, no. 7, pp. 463-474, 1984.
- [4] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2003.
- [5] A. Ranade and A. Rosenfeld, "Point pattern matching by relaxation," *Pattern Recognition*, vol. 12, no. 2, pp. 269-275, 1993.
- [6] J. H. Wegstein, "An automated fingerprint identification

system,” U.S. Government Publication, Washington, DC: U.S. Dept. of Commerce, National Bureau of Standards, 1982.

- [7] J. H. Moon and H. I. Kim, “Scoring method of fingerprint image quality using classified block-level characteristics,” *Journal of the Korea Institute of Information Security and Cryptology (in Korean)*, vol. 17, no. 2, pp. 29-40, 2007.
- [8] Y. N. Shin, W. J. Sung, and S. W. Jung, “Quality assessment of fingerprint images and correlation with recognition performance,” *Journal of the Korea Institute of Information Security and Cryptology (in Korean)*, vol. 18, no. 3, pp. 61-68, 2008.
- [9] B. M. Sullivan and S. P. Hsu, “Biometric score normalizer,” U.S. Patent Office, U.S. Patent Issued, US 6,591,224, 2003.
- [10] P. Z. Lo, “Dynamic thresholding for a fingerprint matching system,” U.S. Patent Office, U.S. Patent Issued, US 7,257,241, 2007.
- [11] G. T. Candela, P. J. Grother, C. I. Watson, R. Wilkinson, and C. L. Wilson, “PCASYS - A pattern-level classification automation system for fingerprints,” Tech. Report : NIST TR 5647, Aug. 1995.
- [12] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, “Fingerprint classification by directional image partitioning,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 21, no. 5, pp. 402-421, 1999.
- [13] K. M. Kim, J. J. Park, B. Lee, Y. J. Go, and S. W. Jung, “Efficient 1:N fingerprint matching algorithm using matching score distribution,” *Journal of Institute of Control, Robotics and Systems (in Korean)*, vol. 18, no. 3, pp. 208-217, 2012.



김 경 민

1988년 고려대 전기공학과 졸업. 1991년, 1996년 동 대학원 석사 박사. 2003년, 2010년 캐나다 CENPARMI 방문교수. 현재 전남대 전기전자통신컴퓨터공학부 교수. 관심분야는 컴퓨터비전, 생체인식.



이 범

1981년 고려대 전기공학과 졸업. 1989년, 1995년 동 대학원 석사, 박사. 현재 전남대 공학대 전기전자통신컴퓨터공학부 교수.



박 중 조

1981년 고려대 전기공학과 졸업. 1983년, 1995년 동 대학원 석사 박사. 2006년 캐나다 CENPARMI 방문교수. 현재 경상대 제어계측공학과 교수. 관심분야는 컴퓨터비전, 생체인식.



정 순 원

1990년 고려대 전기공학과 졸업, 1992년, 1997년 동 대학원 석사, 박사. 1999년~2009년 (주)니트젠 기술연구소 연구소장. 2010년~현재 Ria Soft 대표이사 관심분야는 생체인식.