

지문 퍼지볼트 시스템의 하드웨어 구현*

임성진,[†] 채승훈, 반성범[‡]
조선대학교

Hardware Implementation of the Fuzzy Fingerprint Vault System^{*}

Sung Jin Lim,[†] Seung-Hoon Chae, Sung Bum Pan[‡]
Chosun University

요약

지문정보를 이용한 사용자 인증은 편리함과 동시에 강력한 보안을 제공한다. 그러나 유한개의 손가락 개수로 인해 패스워드처럼 변경을 자유롭게 할 수 없기 때문에 사용자 인증을 위해 저장된 지문정보가 타인에게 도용된다면 심각한 문제를 일으키게 된다. 지문정보를 안전하게 보호하기 위한 지문 퍼지볼트 시스템에 대한 연구가 활발히 진행되고 있다. 또한, 기하학적 해싱 기법을 적용하여 지문 정렬 문제를 해결하려는 연구도 진행되었다. 본 논문에서는 기하학적 해싱 기반 지문 퍼지볼트 시스템의 하드웨어 구조를 제안한다. 제안한 구조는 소프트웨어 모듈과 하드웨어 모듈로 통합 구성된다. 하드웨어 모듈은 등록 해시 테이블과 인증 해시 테이블의 변환 특징점의 정합을 담당한다. 실험결과, 제안한 하드웨어 구조의 수행 시간은 지문 특징점의 수가 36개이고 거짓 특징점의 수가 100개 일 때 0.2초, 400개 일 때, 0.53초이다.

ABSTRACT

The user authentication using fingerprint information not only provides the convenience but also high security. However, the fingerprint information for user authentication can cause serious problems when it has been compromised. It cannot change like passwords, because the user only has ten fingers on two hands. Recently, there is an increasing research of the fuzzy fingerprint vault system to protect fingerprint information. The research on the problem of fingerprint alignment using geometric hashing technique carried out. This paper proposes the hardware architecture fuzzy fingerprint vault system based on geometric hashing. The proposed architecture consists of software and hardware module. The hardware module has charge of matching between enrollment hash table and verification hash table. Based on the experimental results, the execution time of the proposed system with 36 real minutiae is 0.2 second when 100 chaff minutiae, 0.53 second when 400 chaff minutiae.

Keywords: Fingerprint authentication, Fuzzy vault, Geometric hashing, Fuzzy fingerprint vault

1. 서론

현대 사회에서는 인터넷과 같은 통신 매체의 발달로 언제, 어디서든 원하는 정보를 손쉽게 접근하고 열

람할 수 있다. 정보에 대한 접근이 용이해짐에 따라 사용자 인증과 개인의 정보를 보호할 수 있는 강인한 인증 시스템의 필요성이 증가하고 있다. 그러나 현재, 대부분의 응용에서 지원하는 패스워드 또는 PIN (Personal Identification Number) 방식은 패스워드의 길이가 충분히 크지 않으며, 지원되는 패스워드 크기 내에서 사용자들은 랜덤한 패스워드를 사용하는 대신 사용자가 기억하기 쉬운 문자 등으로 여러 응용에 동일한 패스워드를 사용하고 있는 실정이다. 따라서 패스워드는 쉽게 추측 또는 유출될 수 있다.^[1]

접수일(2009년 10월 29일), 수정일(2010년 2월 3일),
게재확정일(2010년 2월 9일)

* 이 논문은 2009년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. (2009-0073999)

[†] 주저자, gigasj83@gmail.com

[‡] 교신저자, sbpan@chosun.ac.kr

패스워드 기반의 사용자 인증 방식이 갖고 있는 이러한 문제점들은 사용자의 바이오정보를 이용함으로써 해결할 수 있다. 하지만, 사용자 인증을 위해 저장된 바이오정보가 타인에게 도용된다면 패스워드나 PIN과는 달리 변경이 불가능하거나 제한적이기 때문에 심각한 문제를 일으키게 된다.

본 논문에서는 다양한 바이오정보 중 가용성, 정확도, 경제성면에서 현재까지 가장 현실적인 대안으로 평가받고 있는 지문을 선택하였다.^[2] 지문을 이용한 사용자 인증 시스템에서도 문제가 있다. 먼저, 패스워드와 달리 동일인의 동일 손가락으로부터 입력되는 지문정보가 매번 유사하지만 완전히 일치되지 않는다는 단점이 있다. 또한, 사람의 손가락은 한정되어 있기 때문에 유출시 변경이 어려우며, 유출된 바이오정보가 모든 응용에 재사용될 수 있다는 문제가 있다. 따라서 바이오정보를 불법적인 취득이나 위변조로부터 안전하게 보호하기 위한 연구가 필요하다.^[3-5] 최근, Juels와 Sudan이 퍼지볼트 이론을 제안하면서부터 퍼지볼트 이론을 지문 인식에 적용하는 지문 퍼지볼트에 관한 연구를 진행하였다.^[6] 지문 퍼지볼트는 사용자의 비밀키와 지문 정보를 통합하여 정당한 사용자만이 비밀키를 획득할 수 있는 암호학적 방법이다. 사용자의 비밀키를 이용하여 다항식을 생성하고, 거짓 특징점(chaff minutiae)을 랜덤적으로 생성한 후 사용자의 지문 특징점(real minutiae)과 함께 지문 템플릿을 구성함으로써 사용자의 지문 특징점을 보호한다. 지문 퍼지볼트를 이용하여 사용자의 지문정보와 그 사용자의 비밀키를 동시에 보호하려는 연구가 보고되고 있으나, 지문의 기준점 부재에 따른 정렬 과정을 생략하였기 때문에 실용화 할 수 없는 문제점이 있다.^[6-8] 지문 정렬 문제를 해결하기 위하여 지문 퍼지볼트 시스템에 기하학적 해싱 기법을 적용하는 방법이 제안되었다.^[9-11] 기하학적 해싱 기법은 객체인식 알고리즘으로 객체의 정보를 추출하고 기하학적 변형을 수행하여 변형된 객체의 정보를 데이터베이스에 저장, 검색하는 알고리즘이다.^[12]

본 논문에서는 기하학적 해싱 기반 지문 퍼지볼트 시스템의 하드웨어 구조를 제안한다. 제안한 구조는 소프트웨어와 하드웨어 모듈을 통합 구현한다. 소프트웨어 모듈은 지문 특징 정보 추출, 지문 템플릿 생성, 지문 해시 테이블 생성, 그리고, 데이터베이스에 저장하는 모듈로 구성된다. 하드웨어 모듈은 매칭모듈, 인증모듈 및 등록 해시 테이블과 인증 해시 테이블을 저장하는 메모리로 구성된다. 매칭모듈은 등록 해시 테

이블의 변환 특징점과 인증 해시 테이블의 변환 특징점을 비교한다. 인증모듈은 매칭모듈의 결과에 따라 유사도 계산을 담당한다.

본 논문의 구성은 다음과 같다. II장에서는 기하학적 해싱 기반 지문 퍼지볼트에 대해 분석한다. III장에서는 제안한 하드웨어 구조에 대해 설명한다. IV장에서는 실험결과, V장에서는 결론을 내린다.

II. 기하학적 해싱 기반 지문 퍼지볼트

사람의 지문은 융선(ridge)과 골(valley)의 형태를 가지고 있다. 융선이 이루고 있는 형태에 따라 분기점(bifurcation point), 단점(ending point), 중심점(core point), 등과 같은 지문에 나타나는 특징을 특징점(minutiae)이라고 한다. 특징점은 특징점의 좌표(x, y), 각도(θ), 그리고 종류(분기점, 단점)로 표현할 수 있다.

지문인식 시스템은 등록과 인식과정으로 구분된다. 오프라인에서의 지문등록은 전처리, 특징점 추출, 그리고 저장하는 순으로 진행된다. 그리고 온라인에서의 지문인식은 입력된 영상에서 추출된 특징점과 저장된 특징점을 비교하여 본인 여부를 확인한다. 그러나 이러한 지문인식 시스템에서 저장되어 있는 지문정보가 유출되거나 공격당할 경우 심각한 문제가 발생한다. 만일 지문인식 시스템에서 지문정보가 유출되었을 경우 사람마다 단지 10개의 지문만을 사용할 수 있기 때문에 변경 할 수 있는 한계가 있고, 유출된 지문은 재등록 할 수 없다. Clancy와 Uludag은 퍼지볼트를 이용하여 지문인식을 수행할 수 있는 지문 퍼지볼트 이론을 제안하였다. 지문 템플릿이 공격당할 경우 사용자의 지문정보가 도용될 수 있는데 이 문제를 해결하기 위해 지문 퍼지볼트 시스템은 지문 템플릿에 다수의 거짓 특징점을 그림 1과 같이 생성하여 삽입한다.^[7,8] 이렇게 지문 템플릿은 복원되지 않은 상태에서 사용자의 지문인식을 수행할 수 있고, 보호된 지문 템플릿은 도난당하여도 공격자는 거짓 특징점이 추가된 지문 템플릿으로부터 사용자의 지문 특징점을 분리할 수 없게 된다.

지문 퍼지볼트는 지문 정렬의 문제가 있다. 지문 정렬은 지문 특징점들이 서로 이루는 구조적 정보를 이용해서 수행된다. 하지만 지문 퍼지볼트는 지문정보에 수백 개의 거짓 정보가 추가된다. 지문 템플릿으로부터 지문 특징점과 추가된 거짓 특징점을 구분하는 것이 어렵다. 따라서 정확한 구조적 정보를 이용할 수

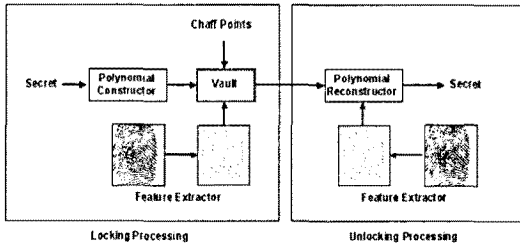


그림 1. 지문 퍼지볼트 블록도

없이 정렬과정을 수행하는 데 어려움이 있다. 기존 연구들은 지문인식의 중간단계인 정렬 과정이 수행되었다고 가정하거나, 수동으로 정렬하였기 때문에 현실적이지 못하며 자동화된 시스템을 구현할 수 없다는 문제점이 있다. [7,8] 이러한 문제점을 해결하기 위해 Chung 등은 기하학적 해싱 기법을 적용하여 자동으로 정렬을 수행하였다. [9-11] 기하학적 해싱 기법은 지문 템플릿을 구성하는 사용자의 특징점과 거짓 특징점 모두를 기준점으로 선택하여 자동 정렬하는 방법이다.

기하학적 해싱 기반 지문 퍼지볼트의 등록과정은 그림 2의 (a)와 같다. 지문의 특징점을 추출하고 거짓 특징점을 추가하여 특징점의 기하학적인 특성을 고려한 등록 테이블을 생성한다. 거짓 특징점과 사용자의 지문 특징점이 포함된 등록 템플릿(라킹셋)을 $L = \{m_i | 1 \leq i \leq r\}$ 으로 표현할 수 있다. L에서 사용자의 지문 특징점과 거짓 특징점들의 집합은 각각 $G = \{m_i | 1 \leq i \leq n\}$, $C = \{m_i | n+1 \leq i \leq r\}$ 으로 표현한다. 등록 템플릿은 기하학적 해싱 기법을 통해 등록 해시 테이블을 생성한다. 사용자의 지문 특징점 G와 거짓 특징점 C의 모든 특징점에 대하여 기준점을 선택하고 선택된 기준점을 제외한 나머지 특징점들의 회

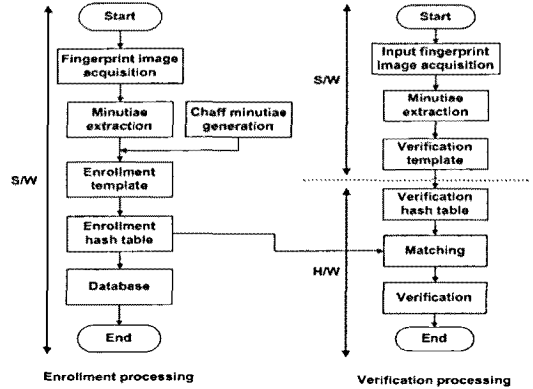


그림 3. 지문 퍼지볼트 시스템의 소프트웨어와 하드웨어 통합 구현

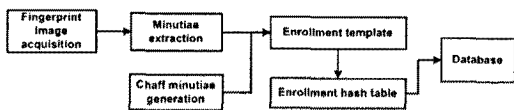
전 및 이동 변환을 거쳐 해시 테이블이 생성된다. 해시 테이블은 기하학적 변환으로 생성된 변환 특징점으로 구성된다. 인식 과정은 그림 2의 (b)와 같이 특징점 정보 추출 단계, 테이블 생성 단계, 정합 단계, 그리고 인증 단계(후보자 목록 생성 단계)를 순차적으로 수행한다. 특징점 정보 추출 단계, 테이블 생성 단계는 등록 과정과 동일한 순서 및 방법으로 수행한다. 정합 단계는 변환 특징점 집합을 기본 단위로 하여 위치와 각도가 일치하는 특징점 쌍을 구하는 단계이다. 인식 테이블의 변환 특징점들 집합과 지문 데이터베이스에 저장된 등록 테이블의 변환 특징점들 집합 사이에 일치하는 변환 특징점들의 쌍의 수를 구함으로써 측정이 가능하다. 이렇게 만들어진 특징점 셋은 언라킹셋 U가 된다. [9]

인증 단계는 인식 테이블의 모든 변환 특징점들 집합에 대하여 지문 데이터베이스에 저장된 등록 테이블의 모든 변환 특징점들 집합과 비교하여 유사도를 측정하고, 높은 유사도 순으로 후보자 목록을 구한다.

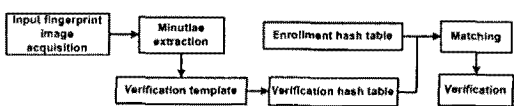
III. 지문 퍼지볼트의 하드웨어 구조

본 장에서는 퍼지볼트의 이론과 기하학적 해싱 기법을 이용하여 지문 템플릿을 보호하는 기하학적 해싱 기반 지문 퍼지볼트 시스템의 하드웨어 구조를 제안한다.

지문 퍼지볼트의 하드웨어 시스템 구현을 위해 그림 3과 같이 소프트웨어와 하드웨어 모듈을 통합하여 구현한다. 지문 퍼지볼트 시스템의 등록 과정은 지문 특징점 추출, 거짓 특징점 생성, 지문 템플릿 생성, 지문 해시 테이블 생성, 그리고 지문 데이터베이스 저장 단계로 이루어진다. 인식 과정은 입력 지문의 특징점



(a) 등록 과정



(b) 인식 과정

그림 2. 지문 퍼지볼트 시스템

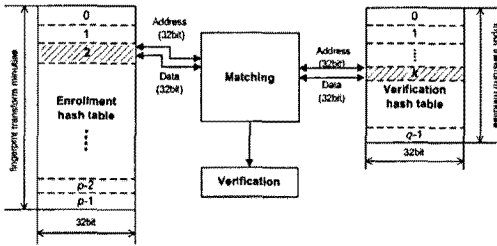


그림 4. 제안한 하드웨어 모듈의 구조도

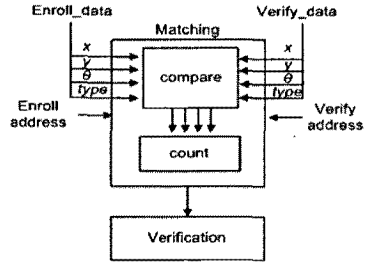


그림 5. 매칭모듈과 인증모듈의 구조도

추출, 지문 해시 테이블 생성, 정합, 그리고 인증 단계 (후보자 목록 생성단계)로 이루어진다.

인식 과정의 정합 단계와 인증 단계는 하드웨어로 구현한다. 정합 단계와 인증 단계는 등록 과정에서 거트 특징점의 수가 증가될수록 연산량이 많아지며, 다른 단계에 비해 동일한 과정을 반복 수행하므로 이를 하드웨어로 구현하는 것이 바람직하다. 반면에, 등록 과정과 인식 과정의 입력 지문 해시 테이블 생성단계 등은 소프트웨어로 구현한다.

제안하는 하드웨어 모듈은 그림 4와 같이 등록 해시 테이블과 인증 해시 테이블을 각각 저장하는 메모리, 매칭모듈과 인증모듈로 구성된다. 각각의 해시 테이블은 변환 특징점으로 이루어져 있다. 등록 지문 변환 특징점은 등록 과정에서 사용자의 지문 특징점과 이를 보호하기 위해 삽입된 거트 특징점이 기하학적 변환을 통해 생성된 특징점이다. 인증 지문 변환 특징점은 인증을 위한 지문의 특징점이 기하학적 변환을 통해 생성된 특징점이다. 변환 특징점은 x축과 y축 각각 11비트, 각도 9비트, 그리고 종류 1비트 총 32비트로 이루어진다. 등록 지문 변환 특징점을 $E = \{tr_i | 0 \leq i < p\}$ 로 표현할 수 있다. 여기서 p는 등록 지문 변환 특징점의 총 수이며, $r \times (r-1)$ 로 표현할 수 있다. 여기서 r은 등록 지문 템플릿의 수이다. 기하학적 변환은 지문 템플릿의 모든 특징점을 기준점으로 선정하여 수행하기 때문에 생성되는 변환 특징점의 수는 $r \times (r-1)$ 이다. 인증 지문 변환 특징점을 $V = \{tr_j | 0 \leq j < q\}$ 로 표현할 수 있다. 여기서 q는 인증 지문 변환 특징점의 총 수이며, $s \times (s-1)$ 로 표현할 수 있다. s는 인증 지문 템플릿의 수이다. 해시 테이블을 저장하는 메모리의 크기는 각각의 등록 지문 변환 특징점 수 p, 인증 지문 변환 특징점 수 q이다. 매칭모듈에 인증 해시 테이블의 k번째 변환 특징점이 입력된다고 가정하면, 등록 해시 테이블의 0번째부터 마지막 p-1번째 변환 특징점까지 순서대로 입력된다. 두 변환 특징점의 비교 후 일치여부를 판단한다. 이후 매

칭모듈에 인증 해시 테이블의 k+1번째 변환 특징점이 입력되고 동일한 방법으로 인증 해시 테이블의 q-1번째 변환 특징점까지 비교한다.

매칭모듈과 인증모듈의 구조는 그림 5와 같다. 매칭모듈은 compare모듈과 count모듈로 구성된다. Compare모듈은 등록 지문 변환 특징점과 인증 지문 변환 특징점을 비교하는 모듈이고, count모듈은 일치된 변환 특징점의 수를 계산하는 모듈이다. 인증모듈은 계산된 유사도를 높은 유사도 순으로 정렬하는 모듈이다.

제안하는 하드웨어 구조의 정합 방법의 흐름도는 그림 6과 같다. 예를 들어, 등록 해시 테이블 E의 변환 특징점의 수가 p개, 인증 해시 테이블 V의 변환 특징점이 q개라고 가정한다. 인증 해시 테이블의 0번째부터 q-1번째까지의 변환 특징점이 매칭모듈에 입력되고, 등록 해시 테이블의 0번째부터 마지막 p-1번째까지 변환 특징점이 매칭모듈에 순서대로 입력된다. 먼저, 매칭모듈의 compare모듈에 0번째 인증 지문 변환 특징점과 0번째 등록 지문 변환 특징점이 비교된다. 두 변환 특징점의 좌표(x, y), 각도(θ), 종류(type)를 비교하여 일치여부를 count모듈로 전송한다. count모듈은 일치된 변환 특징점의 수를 구한다. 이후, 1번째 등록 지문 변환 특징점이 compare모듈에 입력되어 0번째 인증 지문 변환 특징점과 비교된다. 동일한 방법으로 등록 해시 테이블의 모든 변환 특징점들의 비교가 완료되면, 인증 해시 테이블의 1번째 변환 특징점이 매칭모듈에 입력된다. 이를 반복적으로 수행하여 인증 해시 테이블의 q-1번째 변환 특징점까지 비교한다.

인증모듈은 계산된 유사도의 정렬을 수행한다. 구해진 일치된 변환 특징점의 수를 이용하여 유사도를 측정하고 높은 유사도 순으로 후보자 목록을 생성한다.

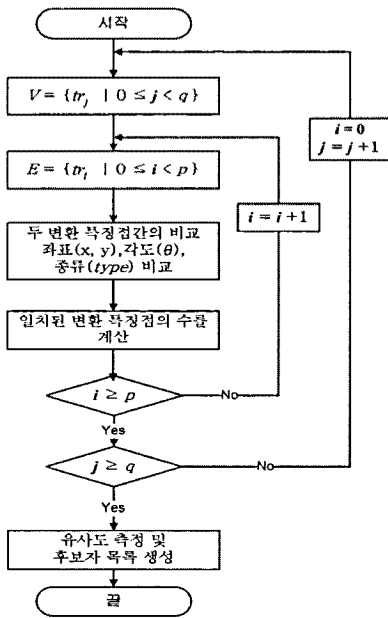


그림 6. 제안하는 하드웨어 모듈의 흐름도

IV. 실험 결과

본 논문에서 제안한 기하학적 해싱 기반 지문 퍼지볼트 시스템의 하드웨어 구조 실험에 사용된 지문 특징점의 수는 최대 90개이고, 최소 16개이며 평균 36개이다. 거짓 특징점의 수는 100개, 200개, 400개를 추가하여 실험하였다. 실험에 사용한 지문 데이터베이스는 광학 센서를 사용하여 100개의 손가락으로부터 한 개의 손가락당 4개의 지문으로 구성된 400개의 지문 이미지이다.¹⁹ 소프트웨어 모듈은 Visual C++ 6.0에서 C언어를 사용하여 구현하였다. 하드웨어 모듈 구현은 Spartan 3E starter board 개발 보드를 사용하였다. 개발 보드에는 Xilinx XC3S500E FPGA가 내장되어 있다. 하드웨어 모듈은 Xilinx ISE 9.2에서 VHDL언어를 사용하여 설계하였다. 하드웨어 시뮬레이션은 Moledmsim XE 6.0에서 실험하였다.

그림 7은 지문 퍼지볼트 시스템에서 제안한 하드웨어 구조의 정합 모듈 시뮬레이션 결과이다. 지문 특징점 36개, 거짓 특징점 200개를 추가하여 실험하였다. 인증 지문 특징점은 34개였다. 제안한 하드웨어 구조의 정합은 입력 지문 해시 변환 특징점과 등록 지문 해시 변환 특징점을 비교한다. 두 변환 특징점간의 일치여부를 판단하며, 그 수를 측정하여 유사도를 구한다.

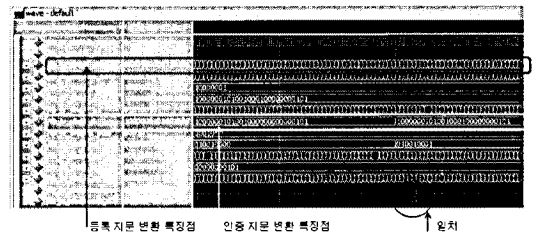


그림 7. 하드웨어 매칭모듈의 시뮬레이션 결과

표 1은 제안한 지문 퍼지볼트의 하드웨어 구조를 개발 보드에 구현했을 때 사용된 주요 자원을 나타내고 있다.

지문 퍼지볼트 시스템의 하드웨어 모듈의 수행시간을 거짓 특징점의 수를 100개, 200개, 400개에 따라 측정하였다. 거짓 특징점의 수, 수행시간과 보안성은 상관관계가 있다. 거짓 특징점이 많을수록 수행시간이 길어지지만, 보안성은 강화된다. 표 2는 소프트웨어와 제안한 하드웨어 구조의 수행시간을 비교하고 있다. 지문 특징점 수 36개이고, 거짓 특징점의 수가 100개 일 때, 소프트웨어는 0.6초, 제안한 방법은 0.2초 거짓특징점이 400개일 때, 소프트웨어는 2.2초 제안한 방법은 0.53초였다. 표 2와 같이 제안한 하드웨어 구조는 보안성을 향상시키기 위해 거짓 특징점 수를 증가시켜도 실시간 처리가 가능하다.

V. 결론

지문정보를 이용한 사용자 인증 시스템은 편리함과 동시에 강력한 보안을 제공하나 지문정보가 도용당하거나 유출되었을 때 심각한 문제를 발생시키게 된다.

표 1. Xilinx Spartan 3E FPGA에서 정합 모듈 구현시 사용된 주요자원

	제안한 하드웨어 구조
Frequency	50MHz
Number of Slices	962 out of 4,656(20%)
Number of Slices Flip Flops	61 out of 9,312(1%)
Total Number of 4 input LUTs	1,828 out of 9,312(1%)

표 2. 하드웨어 모듈 수행시간(sec)

	거짓 특징점 수		
	100	200	400
소프트웨어	0.6	1.13	2.2
제안한 하드웨어 구조	0.2	0.24	0.53

최근 지문 템플릿을 보호하기 위해 퍼지볼트 이론을 적용한 지문 퍼지볼트 연구가 진행되고 있다. 본 논문에서는 기하학적 해싱 기반 지문 퍼지볼트 시스템의 하드웨어 구조를 제안하였다. 제안한 하드웨어 구조의 정합모듈은 입력 지문 해시 테이블의 하나의 변환 특징점마다 등록 지문 해시 테이블의 모든 변환 특징점을 정합하여 구현하였다. 제안한 하드웨어 구조의 수행시간은 지문 특징점이 36개일 때 거짓 특징점이 100개일 때 0.2초, 거짓 특징점이 400개일 때 0.53초였다. 실험결과, 실험결과, 제안한 지문 퍼지볼트 시스템의 하드웨어 구조를 이용하여 실시간 지문 인증을 할 수 있음을 확인하였다. 향후에는 지문 퍼지볼트의 다항식을 적용하여 복원하는 방법과 이를 하드웨어로 구현하는 방법에 대해 연구할 계획이다.

참 고 문 헌

- [1] W. Stallings, *Cryptography and Network Security*, Prentice-Hall Inc., Dec. 2003.
- [2] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2003.
- [3] R. Bolle, J. Connell, and N. Ratha, "Biometric perils and patches," *Pattern Recognition*, vol. 35, no. 12, pp. 2727-2738, Dec. 2002.
- [4] B. Schneier, "The uses and abuses of Biometrics," *Communications of the ACM*, vol. 42, no. 8, p. 136, Aug. 1999.
- [5] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric recognition: security and privacy concerns," *IEEE Security and Privacy Magazine*, pp. 33-42, Mar./Apr. 2003.
- [6] A. Juels and M. Sudan, "A fuzzy vault scheme," *Proc. of IEEE Int. Symp. on Information Theory*, p. 408, June 2002.
- [7] T. Clancy, N. Kiyavash, and D. Lin, "Secure smartcard-based fingerprint authentication," *Proc. of ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop*, pp. 45-52, Nov. 2003.
- [8] U. Uludag, S. Pankanti, and A. Jain, "Fuzzy vault for fingerprints," *LNCS 3546*, pp. 310-319, 2005.
- [9] Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, and D. Ahn, "Automatic alignment of fingerprint features for fuzzy fingerprint vault," *LNCS 3822*, pp. 358 - 369, 2005.
- [10] 이성주, 문대성, 김학재, 정용화, 이옥연, "3차원 기하학적 해싱을 이용한 퍼지볼트에서의 지문 정합," *정보보호학회논문지*, 18(1), pp. 11-21, 2008년 2월.
- [11] 김기철, 김민, 정용화, 반성범, "실시간 지문 식별을 위한 하드웨어 구현," *정보보호학회논문지*, 14(6), pp. 79-89, 2004년 12월.
- [12] H. Wolfson and I. Rigoutsos, "Geometric hashing: an overview," *IEEE Computational Science and Engineering*, vol. 4, no. 4, pp. 10 - 21, Oct./Nov. 1997.

〈著者紹介〉



임 성 진 (Sung Jin Lim) 정회원
 2008년 2월: 조선대학교 제어계측공학과 졸업
 2008년 3월~현재: 조선대학교 정보통신공학과 석사과정
 <관심분야> 영상처리, VLSI, 바이오인식



채 승 훈 (Seung-Hoon Chae) 정회원
 2007년 2월: 조선대학교 전기공학과 졸업
 2009년 2월: 조선대학교 정보통신공학과 석사
 2009년 3월~현재: 조선대학교 정보통신공학과 박사과정
 <관심분야> 바이오인식, 영상처리, 정보보호



반 성 범 (Sung Bum Pan) 종신회원
 1999년 2월: 서강대학교 전자공학과 박사
 1999년 2월~2005년 2월: 한국전자통신연구원 정보보호연구단 생체인식기술연구팀 팀장
 2005년 3월~현재: 조선대학교 제어계측로봇공학과 조교수
 <관심분야> 바이오인식, 영상처리, VLSI 신호처리