情報保護學會論文誌
第19卷 第1號, 2009. 2

# 다중 다항식을 이용한 지문 퍼지볼트*

문 대 성,†‡ 최 우 용, 문 기 영

한국전자통신연구원

# Fuzzy Fingerprint Vault using Multiple Polynomials*

Daesung Moon,†‡ Woo-Yong Choi, Kiyoung Moon

ETRI

## 요 약

사용자 인증을 위해 저장된 중요한 바이오정보가 타인에게 유출되어 도용된다면 패스워드나 PIN과 달리 변경이 불가능하므로 심각한 문제를 일으킬 수 있다. 따라서 타인에게 유출되더라도 재사용이 불가능하도록 하기 위하여 사용자의 바이오정보에 역변환이 불가능한 함수를 적용하여 저장하고 변환된 상태에서 인증과정을 수행할 수 있는 방법이 필요하다. 최근 바이오정보를 안전하게 보호하기 위해 암호학적 방법으로 연구되어지고 있는 퍼지볼트 이론을 지문정보에 적용하는 연구가 활발히 진행되고 있다. 그러나 대부분의 연구들이 지문 특징점의 개수를 고려하지 않고 고정된 차수의 다항식을 선택하기 때문에 지문영상에서 특징점의 개수가 다항식의 차수보다 적을 경우 동작하지 못하는 문제점이 발생한다. 본 논문에서는 지문 퍼지볼트의 보안성과 인식성능을 향상시키기 위해서 다항식의 차수를 특징점의 개수에 따라 가변적으로 선택하는 방법을 제안한다. 특히, 낮은 차수의 다항식을 사용할 경우 두 개 이상의 서로 다른 다항식을 사용하여 보안성을 향상시킬 수 있다. 실험을 통하여 제안한 방법은 보안성과 인식성능이 향상되는 것을 확인하였다.

## ABSTRACT

Security of biometric data is particularly important as the compromise of the data will be permanent. To protect the biometric data, we need to store it in a non‐invertible transformed version. Thus, even if the transformed version is compromised, its valid biometric data are securely remained. Fuzzy vault mechanism was proposed to provide cryptographic secure protection of critical data(e.g., encryption key) with the fingerprint data in a way that only the authorized user can access the critical data by providing the valid fingerprint. However, all the previous results cannot operate on the fingerprint image with a few minutiae, because they use fixed degree of the polynomial without considering the number of fingerprint minutiae. To solve this problem, we use adaptive degree of polynomial considering the number of minutiae. Also, we apply multiple polynomials to operate the fingerprint with a few minutiae. Based on the experimental results, we confirm that the proposed approach can enhance the security level and verification accuracy.

**Keywords** : Fingerprint Verification, Fuzzy Fingerprint Vault, Multiple Polynomials

## Ⅰ. 서 론

정당한 사용자가 정보시스템에 접근하기 위하여 패스워드 또는 PIN(Personal Identification Number)을 이용한 사용자 인증 방법이 현재까지 널리 쓰이고 있으나, 타인에게 노출되거나 잊어버리는 등의 문제가 있다. 이러한 문제를 해결하기 위하여 개인의 고유한 바이오정보를 이용한 정보보호 및 사용자인증 등의 연구가 활발히 진행되고 있다[1,2,3].

그러나 이러한 바이오정보가 악의적인 목적을 가진 공격자에게 유출된다면 심각한 문제를 야기할 수 있다. 왜냐하면 하나의 얼굴, 열개의 손가락 등 한정된 개수를 가진 바이오정보는 패스워드와 다르게 유출시 마다 변경할 수 없으며, 일반적으로 사용자는 동일한 바이오정보를 다양한 응용에 사용하기 때문에 유출된 바이오정보는 모든 응용에서 재사용될 수 있기 때문이다. 따라서 바이오정보의 불법적인 취득이나 위변조 시도로부터 안전하게 보호하기 위한 문제를 해결해야 한다[2,3].

본 논문에서는 바이오정보 중 지문을 선택하였으며, 지문은 가용성, 정확도, 경제성 면에서 현재까지 가장 현실적인 대안으로 평가받고 있다[1].

Jules[4]가 암호키 보호를 위하여 제안한 퍼지볼트 이론을 지문, 홍채, 서명 등의 바이오정보 보호에 적용하는 연구가 활발히 진행되고 있다. 본 논문에서도 퍼지볼트(Fuzzy Vault) 이론[4]을 지문인증 시스템에 적용한 지문 퍼지볼트 시스템의 효율적으로 구현방안에 대하여 기술한다. 지문 퍼지볼트 시스템은 등록과정에서 다항식을 생성하고 지문영상으로부터 추출된 사용자의 지문 특징정보를 다항식에 사영한다. 또한 사용자의 지문 특징정보를 타인으로부터 은닉하기 위해서 다수의 거짓 특징정보를 추가하여 볼트라는 형태로 저장한다. 인증과정에서 거짓 특징정보를 함께 포함하고 있는 볼트로부터 사용자의 지문 특징정보만을 선택한 후, 등록과정에서 사용된 것과 동일한 다항식을 생성할 경우 본인으로 인증한다. 즉, 지문 퍼지볼트 시스템의 보안성은 볼트로부터 사용자의 지문특징과 거짓특징을 구분하는 어려움에 기반한다. 본인의 경우에는 등록과정에서 제공했던 것과 동일한 지문으로 지문인증을 요구하기 때문에 볼트에서 사용자의 지문 특징정보를 쉽게 분리할 수 있다.

대부분의 지문 퍼지볼트 관련 기존 연구들[5,6,7]에서 고정된 다항식 차수(degree)를 사용하였다. 그러나 고정된 차수를 사용할 경우 등록과정에서 추출된 사용자 지문특징의 개수가 다항식 차수보다 적을 경우에는 올바르게 동작하지 못하는 심각한 문제점이 있다. 왜냐하면 지문인증 과정의 결과로 나오는 두 지문에서 일치하는 특징의 개수는 등록 지문특징 개수 이하이기 때문이다.

이러한 문제점을 해결하기 위한 직관적인 방법은 등록 시 입력지문에서 추출된 특징정보의 개수보다 낮은 차수의 다항식을 사용하는 것이다. 그러나 이러한 방법은 높은 차수의 다항식을 사용하는 일반적인 방법에 비하여 보안(security)성에 문제를 야기할 수 있다. 즉, 지문 퍼지볼트 시스템의 공격방법 중에 하나인 다항식 전수조사에서 낮은 차수의 다항식이 높은 차수의 다항식에 비하여 취약한 보안성을 가진다.

본 논문에서는 이러한 문제점을 해결하기 위해서 전형적인 퍼지볼트[5,6,7], 특히 기존의 지문 퍼지볼트 시스템[5,6,7]에서처럼 하나의 다항식을 사용하는 대신에 두 개 이상의 서로 다른 다항식을 사용하는 방법을 제안한다. 즉, 낮은 차수의 다항식을 사용하더라도 서로 다른 두 개의 다항식을 사용하기 때문에 직접적인 다항식 공격이 불가능하며, 적은 개수의 지문특징을 가진 사용자의 경우에도 올바르게 동작할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 지문인증 시스템의 일반적인 내용과 퍼지볼트에 대해 설명한다. 3장에서는 본 논문에서 제안한 다중 다항식 기반 지문 퍼지볼트에 대하여 설명 하고, 4장에서는 실험결과에 의한 성능을 평가한다. 마지막으로 5장에서는 결론을 맺는다.

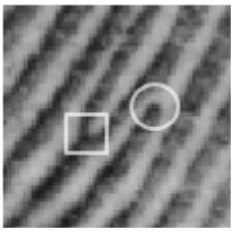
## Ⅱ. 지문인식 시스템

### 2.1 지문인식

본 논문에서는 다양한 바이오정보 중에서 지문 정보를 이용하여 사용자 인증을 한다. 지문이란 인간의 손바닥에 존재하는 땀구멍이 융기한 선으로 형성된 문형을 말

접수일(2008년 8월 29일), 수정일(2008년 10월 21일), 게재확정일(2008년 12월 20일)
* 본 연구는 지식경제부 및 정보통신연구진흥원의 IT신성장 동력핵심기술개발사업[2008-S-020-2, 프라이버시 보호형 바이오인식 시스템 개발]의 일환으로 수행하였음
† 주저자, daesung@etri.re.kr
‡ 교신저자, daesung@etri.re.kr

하는 것으로, 융기되어 나타나는 융선(ridges)과 두 융선 사이의 패인 골(valleys)로 나타내어진다. 지문 인식의 방법으로는 영상을 기반으로 하는 방법과 영상 내에 존재하는 특징점을 이용하는 특징점(minutiae) 기반으로 나눌 수 있다[1]. 이때 특징점을 구성하는 요소로는 기본적으로 특징점의 좌표($x$, $y$), 각도($\theta$) 그리고 종류(끝점, 분기점)가 될 수 있고 임의의 지문영상으로부터 $n$개의 특징점이 추출되었다면 $A=\{(x_i,y_i,\theta_i,t_i)|i=1,\cdots,n\}$로 표현한다.



[그림 1] 지문 특징점; 분기점(Bifurcation): 사각형, 끝점(Ending): 원

지문을 이용한 특징점 기반 사용자 인증 시스템은 사용자 등록(enrollment) 과정과 사용자 인증(verification) 과정으로 수행된다. 주로 오프라인에서 수행되는 사용자 등록 과정은 획득된 지문 영상의 품질을 향상시키기 위한 전처리 단계를 거친 후 특징추출 단계에서 특징점 정보들을 추출하여 서버에 저장하는 과정이며, 사용자 인증 과정은 등록과정과 동일하게 전처리, 특징추출 단계를 거쳐 추출된 특징점 정보와 미리 저장된 특징점 사이에 정합(matching)을 수행함으로써 입력된 지문이 저장된 지문과 동일한 지문인지를 판단하는 과정이다.

서버에 저장된 특징점 정보가 타인에게 유출되었을 경우를 가정해보자. 비록, 유출된 특징점 정보로부터 원 지문영상과 동일한 영상은 복원 할 수 없지만 동일한 특징점이 추출될 수 있는 지문영상은 복원 할 수 있다. 이렇게 생성된 지문영상을 특징점 기반 지문인식 시스템에 입력할 경우 동일한 특징점이 추출되기 때문에 정당한 사용자로 인식하게 된다. 이와 같은 문제점을 해결하기 위해서 최근 지문정보 보호 분야의 연구가 활발히 진행되고 있으며, 특히 퍼지볼트 이론을 이용하여 지문 특징점을 보호하는 연구[5,6,7]가 많이 보고되고 있다.

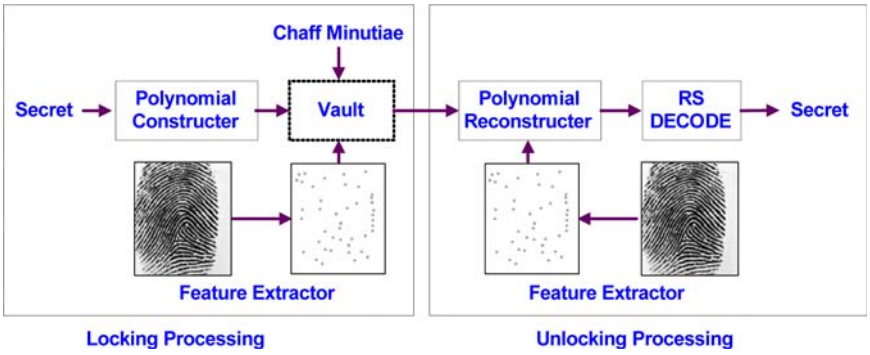
### 2.2 퍼지볼트 이론

본 절에서는 Juels[4]가 제안한 퍼지볼트 이론에 관해 간략히 설명한다. 만약 사용자가 $n$개의 점들로 구성된 집합 $L$로 비밀키 $S$를 숨기는 것을 목표로 한다고 가정해보자. 사용자는 $S$를 이용하여 단일 변수 $x$만 있는 $k$차 다항식 $p(x)$를 생성할 수 있다. 이때, $n > k$ 이다. 다항식을 생성한 후에, 사용자의 집합 $L$의 각 원소 $l_i$를 다항식의 $p(x)$값에 대입한 결과 $p(l_i)$를 계산한다. 이것은 결국 사용자의 집합 $L$의 점들을 다항식 $p(x)$ 상에 있는 점들로 사영하는 것으로 간주할 수 있다. 결과적으로 ($l_i$, $p(l_i)$)로 구성된 집합을 생성한다. 집합 $L$로부터 생성된 값들을 숨기기 위해서 $p(x)$에 존재하지 않는 많은 수의 거짓 점들 $(\alpha_j,\beta_j)$를 생성하여 ($l_i$, $p(l_i)$)에 추가한 집합 $R$을 생성한다(원소 개수가 $r$개인 집합 $R$을 볼트라고 부른다). 이때 $\beta_j \neq p(\beta_j)$ 이다. 비밀키 $S$를 복원하기 위해서는 $k$+1 개의 $p(x)$위에 존재하는 점들이 필요하다.

다른 사용자가 자신의 집합 $U$로 $S$를 복원하기를 원한다고 가정해보자. 만약 집합 $U$와 집합 $L$의 원소들이 상당부분 겹친다면 집합 $U$로부터 볼트 $R$에 있는 점들 중 $p(x)$상에 존재하는 많은 점들을 선택할 수 있다. 그리고 선택된 점들로부터 다항식 $p(x)$를 생성하고 다항식으로부터 $S$를 복원할 수 있다. 이때 집합 $L$과 집합 $U$는 정확하게 동일하지 않기 때문에 거짓 점들도 일부 볼트 R로부터 선택될 수 있는데 이는 랜덤노이즈로 간주하여 오류정정을 거치게 되면 정확한 $S$를 복원 할 수 있다. 만약 집합 $U$와 집합 $L$이 겹치는 부분이 적다면 볼트 $R$에서 거짓 점들이 추출될 확률이 높기 때문에 정확한 다항식 $p(x)$의 복원이 어렵다. 퍼지볼트 이론에서 비밀키 $S$를 숨기기 위해 사용되는 집합 $L$을 라킹셋(Locking Set), 복원하기 위해 사용되는 집합 $U$를 언라킹셋(Unlocking Set)이라고 정의한다.

### 2.3 지문 퍼지볼트

지문, 홍채, 얼굴 등 다양한 바이오인식 시스템들 중에서 지문인식 시스템이 퍼지볼트 이론과 통합하기에 가장 적당하다. 왜냐하면, 지문인식 시스템의 특징점은 지문영상 평면에서 점으로 존재하기 때문에 등록과정의 특징점을 Locking Set으로 인증과정의 특징점을 Unlocking Set 으로 대입하여 적용할 수 있다. [그림 2]




[그림 2] 지문 퍼지볼트 시나리오

에 나타난 바와 같이 지문 퍼지볼트는 Locking 과정과 Unlocking 과정으로 구성되며, 각 단계에 대한 자세한 설명은 다음과 같다.

### 2.3.1 Locking 과정

지문 퍼지볼트의 Locking 과정은 다음과 같다.

① 등록지문으로부터 n 개의 특징점을 추출한다. 이렇게 사용자의 등록지문으로부터 추출된 특징점을 진짜 특징점(real minutiae)이라 정의한다.

$$L=\{(x_i,y_i,\theta_i,t_i)|i=1,\cdots,n\} \quad (1)$$

② 비밀정보 $S$로부터 $k$차 다항식을 생성하고, 비밀정보 $S$를 해쉬함수 $h$에 대입하여 해쉬값 $h(S)$를 생성한다.

$$p(x)=a_0+a_1x+\cdots+a_kx^k \quad (2)$$

$$S=(a_0\|a_1\|\cdots\|a_k) \quad (3)$$

$$a_i\in \mathrm{GF}(p^2) \quad (4)$$

$$\kappa=h(S) \quad (5)$$

③ 집합 $L$의 원소들을 $\mathrm{GF}(p^2)$ 의 원소로 변환하여 이 값을 $p(x)$ 상에 수식 7과 같이 사영(projection)하여 집합 $R_L$ 을 생성한다. 예를 들어 $\mathrm{GF}(p^2)$ 의 원소를 $AX+B$ $(A,B\in \mathrm{GF}(p))$로 표시한다면 특징점의 $x$, $y$ 좌표를 각각 $A,B$로 바꾸는 방법을 생각해볼 수 있다.

$$R_L=\{(r_i,v_i)|i=1,\cdots,n\},\ r_i=(x_i,y_i,\theta_i,t_i) \quad (6)$$

$$v_i=p(X_i),\ X_i=x_iX+y_i\in \mathrm{GF}(p^2),\ i=1,\cdots,n \quad (7)$$

모든 다항식 연산은 $\mathrm{GF}(p^2)$ 상에서 수행된다.

④ $L$을 숨기기 위한 거짓 특징점(chaff minutiae)을 생성한다.

$$C=\{(c_i,v_i)|i=n+1,\cdots,r\},\ c_i=(x_i,y_i,\theta_i,t_i) \quad (8)$$

$$v_i=p(X_i)+\alpha_i,\ \ X_i=x_iX+y_i\in \mathrm{GF}(p^2),\ i=n+1,\cdots,r \quad (7)$$

여기서, $\alpha_i$는 0이 아닌 임의의 수이다.

⑤ $R_L$과 $C$를 원소의 순서가 무작위가 되도록 통합하여 집합 $R$을 구성한다.

$$R=\{(r_i,v_i)|i=1,\cdots,r\},\ r_i=(x_i,y_i,\theta_i,t_i) \quad (10)$$

⑥ 집합 $R$과 비밀정보 $S$의 해쉬값 및 다항식의 차수 $k$로 구성된 볼트를 저장된다.

$$V=\{(r_i,v_i),\kappa,k|i=1,\cdots,r\} \quad (11)$$

### 2.3.2 Unlocking 과정

지문 퍼지볼트의 Unlocking 과정은 입력 지문의 특징점으로부터 다항식을 복원하는 과정이다. 지문 퍼지볼트의 Unlocking 과정은 다음과 같다.

① 입력지문으로부터 $m$개의 특징점을 추출한다.

$$U=\{(x_i',y_i',\theta_i',t_i')\,|\,i=1,\cdots,m\} \quad (12)$$

② 집합 $U$와 Locking 과정에서 저장된 집합 $V$의 $r_i$를 입력으로 지문정합을 수행하여 $t$ 개의 서로 일치하는 특징점들을 구하고, 이들 일치하는 특징점정보와 해당 $v_i$ 값으로 구성된 집합 $M$을 생성한다.

$$M=\{(m_i,v_i)\,|\,i=1,\cdots,t\},\ m_i=(x_i,y_i,\theta_i,t_i) \quad (13)$$

이때, $M\subseteq R, t\le r$ 이다.

③ 다항식의 차수 $k$와 집합 $M$을 $\mathrm{RS}_{\mathrm{DECODE}}$ 의 입력으로 하여 $k$차 다항식 $p'(x)$을 복원하고 비밀정보의 해쉬값 κ'를 구한다.

$$p'(x)=\mathrm{RS}_{\mathrm{DECODE}}(k,M) \quad (14)$$

$$p'(x)=a_0'+a_1'x+\cdots+a_k'x^k \quad (15)$$

$$\kappa'=h(a_0'\|a_1'\|\cdots\|a_k') \quad (16)$$

④ κ'와 κ가 일치하면 본인으로 수락하고, 그렇지 않으면 거절한다.

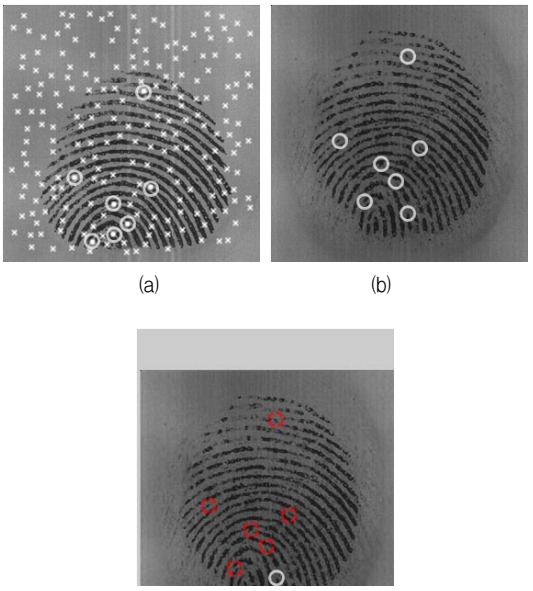
$$\mathrm{Decision}=\begin{cases}\mathrm{Accept}, & \kappa'=\kappa\\ \mathrm{Reject}, & \mathrm{otherwise}\end{cases} \quad (17)$$

지문 퍼지볼트에서 일치하는 특징점의 개수가 $k$+1개 이상 존재할 경우 $k$차 다항식을 복원할 수 있다. 그러나 동일인의 지문을 이용하여 지문인증을 시도할 경우에도 일치하는 특징점의 집합인 $M$에 거짓 특징점이 포함될 수 있으며, 이러한 거짓 특징점은 RS(Reed Solomon) DECODE를 이용하여 제거하고 Locking 과정에서 사용한 것과 동일한 다항식을 복원할 수 있다. 다만, RS DECODE를 이용하여 다항식을 복원할 경우 RS DECODE의 특성상 $k$차 다항식을 복원하기 위해서는 $(k+t)/2$개 이상의 진짜 특징점이 필요로 한다[5].

공격자가 지문 퍼지볼트 시스템을 공격하기 위한 방법은 다음과 같은 3가지의 경우가 가능하다.

첫째, 지문특징점을 안전하게 보호하기 위해서 거짓 특징점을 추가한 볼트정보를 저장하게 된다. 본인이 인증요청을 하였을 경우에 등록과정에서와 동일한 지문을 사용하기 때문에 볼트에서 진짜 특징점을 분리하여 다항식 복원을 할 수 있다. 그러나 악의적인 공격자는 진짜특징점 정보를 알 수 없기 때문에 전수조사 공격(brute-force)을 시도 할 것이다. 이럴 경우 지문 퍼지볼트의 공격 복잡도(complexity)는 수식 18과 같다. 수식 18은 볼트에서 정확하게 $k$+1개의 진짜 특징점을 선택할 수 있는 확률이며, 거짓특징점을 많이 추가할수록 그리고 진짜 특징점 개수에 가까운 다항식 차수를 사용할수록 복잡도는 향상된다.

$$Complexity={}_rC_{k+1}/{}_nC_{k+1} \quad (18)$$



(a) (b)

(c)

[그림 3] 적은 개수의 특징점의 지문 퍼지볼트 적용 예.
(a) 등록지문(O : 진짜특징점, X : 가짜특징점),
(b) 인증지문, (c) 인증지문(b)의 정렬 후 지문 퍼지볼트 인증 결과

둘째, Locking 과정의 수식 2에서 사용된 다항식($p(x)$)을 직접 공격하는 것이다. 전수조사에 의해서 다항식을 복원할 경우 공격 복잡도는 수식 19와 같다. 수식 19에서 $k$는 다항식의 차수이며, $l$은 계수(coefficient)

의 비트수이다. 즉, 일반적으로 계수의 비트수는 지문영상의 크기에 의해서 결정되므로 다항식의 차수가 높을수록 지문 퍼지볼트 시스템의 보안성은 향상된다.

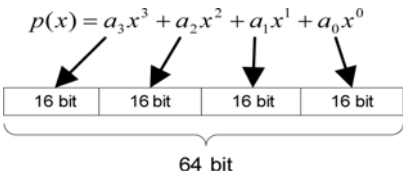
$$2^{((k+1)*l)} \quad (19)$$

마지막으로, 비밀정보 *S*로부터 다항식이 생성되기 때문에 비밀정보 S를 직접 공격하는 것이 가능하다. 그러나 비밀정보 S는 시스템에서 요구하는 보안수준에 맞게 선택할 수가 있고, 수식 5에서와 같이 해쉬함수의 결과로 저장되기 때문에 안전하다고 할 수 있다.

지문특징점으로부터 정확한 다항식을 복원하기 위해서는 등록 시 입력지문의 특징점 개수보다 낮은 차수의 다항식을 사용해야 한다. 즉, $n > k$ 조건을 만족해야 한다. 왜냐하면 지문인증 과정의 결과로 나오는 두 지문에서 일치하는 특징점의 개수는 등록 지문특징점 개수 이하이기 때문이다. [그림 3]에서와 같이 등록지문의 추출된 특징점 개수가 7개인 경우에 사용할 수 있는 다항식은 6차 이하의 다항식이 가능하다. 그러나 대부분의 지문 퍼지볼트관련 기존 연구들[5,6,7]에서 고정된 다항식 차수를 사용하였다. 예를 들어 Clancy[5]는 14차 다항식을 사용했는데, 이는 지문인증의 결과인 일치하는 특징점들의 집합에서 거짓 특징점이 없을 때 15개 이상의 진짜 특징점이 있어야 한다는 의미이다. 또한, Uludag[6]은 8차 다항식을 사용했다. 이처럼 고정된 차수를 사용하는 지문 퍼지볼트 시스템을 구현함에 있어서 특징점의 개수가 적은 지문을 소유한 사용자는 사용할 수 없기 때문에 비현실적이다. [그림 3]은 FVC 2002 지문 데이터베이스를 이용한 지문 퍼지볼트의 인증 예이다. [그림 3(a)]에서 처럼 인증지문으로부터 7개의 특징점(원으로 표현됨)이 추출되었으며, 200개의 가짜 특징점(X로 표현됨)이 추가되었다. [그림 3(b)]는 인증지문으로 7개의 특징점이 추출되었다. [그림 3(c)]는 진짜(real)와 가짜(chaff) 특징점을 포함하는 [그림 3(a)]의 특징점 집합과 [그림 3(b)]의 특징점을 입력으로 지문매칭(matching)과정을 수행한 결과이다. [그림 3]에서와 같이 올바르게 정렬(alignment)된 후 6개의 일치하는 특징점 쌍(점선 원으로 표현됨)을 찾았으며 모두 진짜(real)특징점임을 실험에서 확인하였다. 하지만, 기존 연구들에서처럼 제안한 고정된 다항식 차수를 사용한다면, [그림 3]에서와 같이 사용자의 지문영상으로부터 지문인증이 성공적으로 수행하더라도 일치하는 특징점 쌍의 개수가 적어서 타인으로 오동작을 하게 된다는 것이다.

이러한 문제점을 해결하기 위한 직관적인 방법은 등록 시 입력지문에서 추출된 특징점의 개수보다 낮은 차수의 다항식을 사용하는 것이다. 그러나 이러한 방법은 지문 퍼지볼트 시스템의 공격방법 중에서 다항식 전수조사를 가정했을 때, 높은 차수의 다항식을 사용하는 일반적인 방법에 비해 상대적으로 취약하게 된다.

등록지문의 특징점 개수가 적은 경우에 지문 퍼지볼트 시스템이 동작하게 하기 위해서 낮은 차수의 다항식을 사용한다고 가정해보자. [그림 4]와 같이 16bit의 계수를 가지는 3차 다항식을 사용한다면 공격자는 4개의 계수에 대해서 전수조사를 하여 해쉬함수의 입력으로 사용할 것이다. 즉, 최악의 경우 $2^{64}$ 번의 해쉬함수를 수행한다면 지문 퍼지볼트 시스템을 공격하여 정당한 사용자를 사칭할 수 있다.

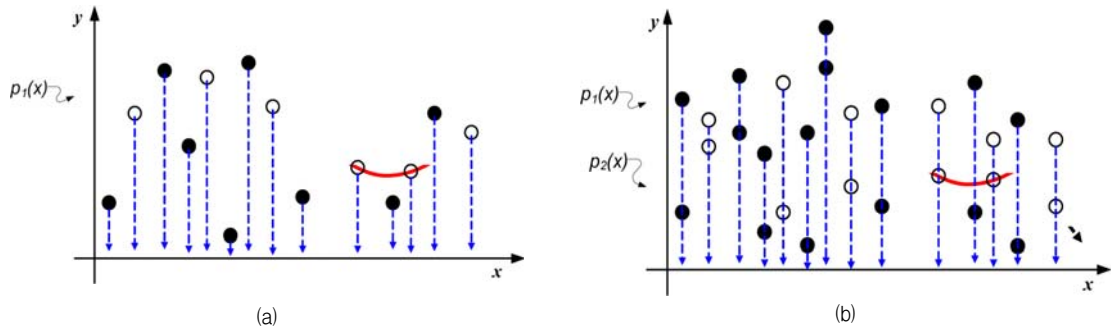



[그림 4] 낮은 차수 다항식의 예

물론, 특징점의 개수가 아주 많은 경우에도 안정적인 복잡도(complexity)를 보장하기 위해서 상대적으로 높은 차수의 다항식을 사용해야한다. 즉, 특징점의 개수에 따라서 적응적으로 다항식의 차수를 결정해야 된다는 의미이다. 본 논문에서는 특징점의 개수가 적은 지문영상을 지문 퍼지볼트에 적용시키기 위한 방법에 중점을 둔다.

## Ⅲ. 다중 다항식을 이용한 지문 퍼지볼트

본 논문에서는 이러한 문제점을 해결하기 위해서 [그림 5(a)]와 같이 전형적인 퍼지볼트[5,6,7,8], 특히 기존의 지문 퍼지볼트 시스템[5,6,7]에서처럼 하나의 다항식을 사용하는 대신에 [그림 5(b)]처럼 2개 이상의 서로 다른 다항식을 사용하는 방법을 제안한다. 즉, [그림 5(b)]와 같이 하나의 특징점은 서로 다른 다항식 $p_1(x)$와 $p_2(x)$에 사영한 두 개의 $y$값을 가진다. 거짓 특징점 또

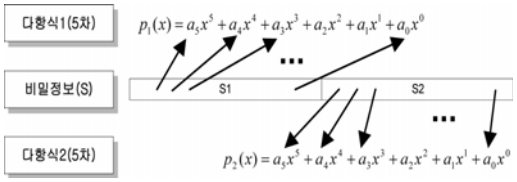



[그림 5] 다중 다항식을 사용한 예(흰색 원 : 진짜 특징점, 검은색 원 : 거짓 특징점). (a) 기존 방법, (b) 제안한 방법

한 두 개의 임의의 $y$값을 가지도록 생성한다. 따라서 2.3.1절의 Locking ⑥번 과정의 결과는 수식 20과 같이 변경된다.

또한, Unlocking ②과정의 수식 13은 수식 24와 같이 재 정의된다. Unlocking ③과정에서는 다항식의 차수 $k$와 수식 24에서 재 정의된 집합 $M$을 $RS_{DECODE}$ 의 입력으로 하여 두 개의 $k$차 다항식 $p'_1(x)$와 $p'_2(x)$를 복원한다. 여러 가지 방법에 의해 비밀정보($S$)로부터 두 개 이상의 다항식을 생성할 수 있으며, 두 개의 다항식을 생성하는 예를 [그림 6]에서 보여준다.

[그림 6]처럼 비밀정보(S)를 두 개의 비밀정보($S1$,$S2$)로 분리하여 각각을 다항식의 계수로 대입하여 다항식을 생성할 수 있다. $S$는 다항식의 차수 및 개수에 따라서 동일한 크기로 분리된다. 이 때, $S1$과 $S2$는 일반적으로 동일하지 않다고 가정한다. Locking ②번 과정에서 해쉬함수의 입력으로 $S1$과 $S2$를 각각 입력하여 두 개의 해쉬값을 저장하는 것이 아니라, $S$를 해쉬함수의 입력으로 취하여 하나의 해쉬값을 저장하게 된다. 이는, 해쉬함수의 입력으로 $S1$과 $S2$를 각각 입력하였을 경우에 공격자가 hash($S1$)을 전수조사 공격을 하여 $S1$에 의해 생성된 다항식을 복원한다면 $V$로부터 진짜 특징점을 분리할 수 있고, 진짜 특징점으로부터 $S2$에 의해 생성된 다항식의 공격도 가능하기 때문이다.




[그림 6] 비밀정보로부터 두 개의 다항식을 생성하는 예

$$V=\{(r_i,v_{1i},v_{2i}),\kappa,k|i=1,\cdots,r\} \quad (20)$$

$$v_{1i}=\begin{cases}p_1(X_i) & ,X_i\ is\ real\ minutiae\\ p_1(X_i)+\alpha_i & ,X_i\ is\ chaff\ minutiae\end{cases} \quad (21)$$

$$v_{2i}=\begin{cases}p_2(X_i) & ,X_i\ is\ real\ minutiae\\ p_2(X_i)+\alpha_i & ,X_i\ is\ chaff\ minutiae\end{cases} \quad (22)$$

$$X_i=x_iX+y_i\in GF(p^2),\ i=1,\cdots,r \quad (23)$$

$$M=\{(m_i,v_{1i},v_{2i})|i=1,\cdots,t\},\ m_i=\{x_i,y_i,\theta_i,t_i\} \quad (24)$$

본 논문에서 제안한 방법은 서로 다른 두 개 이상의 다항식을 사용하여 다항식에 대한 전수조사 공격의 비도가 높아지기 때문에 전체적인 지문 퍼지볼트 시스템의 안전성을 보장할 수 있다. 수식 18에 의한 지문 퍼지볼트 시스템의 복잡도는 지문특징점의 개수가 적은 경우에도 지문특징점의 개수에 근접한 다항식 차수를 선택하고, 가짜 특징점을 많이 추가하여 향상시킬 수 있기 때문이다. 즉, 6개의 지문특징점이 추출되었다고 가정했을 때, 지문인식이 가능하도록 5차 다항식을 사용할 수 있다. 이 경우에는 $2^{96}$번의 전수조사가 수행되어야 한다. 그러나 [그림 6]과 같이 서로 다른 두 개의 5차 다항식을 사용한다고 가정했을 때 공격자가 직접적으로 다항식에 대한 공격을 한다면 두 개 다항식의 계수들에서 어떠한 상관관계도 찾을 수 없기 때문에 $2^{192}$(=$2^{96*2}$)번의 해쉬함수 연산을 해야 된다.

## Ⅳ. 실험결과

본 논문에서 제안한 다중 다항식 방법의 성능을 측정하기 위하여 FVC2002 DB1 Set A[9]를 사용하였다. FVC 2002 실험환경과 동일하게 본인정합은 8장의 이미지 각각에 대해서 나머지 이미지와 정합을 수행하였으며, 한번 등록된 것은 이후의 정합에는 사용하지 않았

다. 타인정합은 각 손가락의 첫 번째 이미지만 사용하였는데, 본인정합과 마찬가지로 100장의 이미지 각각에 대해서 나머지 이미지와 정합을 수행하였으며, 한번 등록된 것은 이후의 정합에는 사용하지 않았다. 따라서 본인정합은 총 2,800회, 타인정합은 총 4,950회를 수행하였다. 모든 실험은 2.66GHz CPU에 3GB RAM이 탑재된 PC에서 수행하였다. 지문 퍼지볼트 시스템의 보안성 및 인식 성능을 향상시키기 위해서는 등록 시 지문영상으로부터 추출된 특징점의 개수를 기초로 하여 거짓 특징점의 개수, 다항식의 차수 등을 적절하게 결정하여야 한다. 본 논문에서 제안한 방법의 인식성능 향상 정도를 실험하기 위해서 적은 특징점 개수를 가지는 지문영상에 대해 다중 다항식 기법을 적용하였다. [표 1]에서와 같이 특징점의 개수가 4~5개의 지문영상에 대해서는 3차 다항식 4개를 사용하였으며 특징점의 개수가 6~10개의 지문에 대해서는 4차 다항식 3개, 마지막으로 11~15개의 지문에 대해서는 5차 다항식 2개를 사용하였다. 3차 다항식 하나를 사용하였을 경우 직접적인 다항식 공격의 비도는 $2^{64}$이지만, 3차 다항식 네 개를 사용하면 $2^{256}$로 비도가 증가한다. 실험에서 15개의 특징점을 가지는 경우에도 다중 다항식 기법을 적용하였다. 이는 센서로부터 획득되는 지문영상이 매번 상이하기 때문에 비교되는 두 지문에서 공통으로 존재하는 영역이 적어지고, 결과적으로 등록 지문영상에서의 특징점의 개수보다 훨씬 적은 특징점이 매칭되기 때문이다. 따라서 실험적으로 15개 이하의 특징점을 가지는 지문영상에 대해 본 논문에서 제안한 방법을 적용하였으며, 15개 이상의 특징점을 가지는 지문영상에 대해서는 고정된 다항식 차수를 사용하는 기존의 방법과 동일하게 실험하였다.

[표 2]는 제안한 방법의 인식성능 실험 결과를 보여준다. [표 2]에서 15개 이하의 특징점을 가지는 지문에 대해서는 [표 1]에서 결정된 다항식 차수를 사용하였으며, 15개 이상의 특징점을 가지는 지문에 대해서는 표 2에서와 같이 다항식 차수를 7에서 12까지 고정시키고 실험하였다. 표 2에서 보는바와 같이 본 논문에서 제안한 방법이 FAR(False Accept Rate)에는 변화가 없으면서 GAR(Genuine Accept Rate)은 향상되는 것을 알 수 있다. 특히, 중요한 것은 고정된 10차 다항식을 사용했다고 가정했을 때, 사용자의 지문영상으로부터 11개 이상의 특징점이 추출될 경우에만 지문 퍼지볼트 시스템이 정상적으로 동작하고 10개 이하의 특징점이 추출된다면 모든 특징점이 일치하는 특징점의 쌍일지라도 타인으로 오동작을 하게 된다는 것이다. 실험에서 10차 다항식의 경우에 10개 이하의 특징점을 가지는 실험이 35회 있었다.

[표 1] 다중 다항식 기법을 위한 parameter setting

| 특징점 개수 | 4~5 | 6~10 | 11~15 |
|---|---|---|---|
| 다항식 차수 | 3 | 4 | 5 |
| 다항식 개수 | 4 | 3 | 2 |

[표 2] 실험결과

| Parameter | | FVC2002 DB1 Set A | | | |
|---|---|---|---|---|---|
| | | 고정다항식방법 | | 제안 방법 | |
| 평균 특징점 개수 | | 27.95 | | 27.95 | |
| Chaff | 다항식 차수 | FAR (%) | GAR (%) | FAR (%) | GAR (%) |
| 200 | 7 | 0.18 | 90.79 | 0.18 | 91.68 |
| 200 | 8 | 0.12 | 86.93 | 0.12 | 88.21 |
| 200 | 9 | 0.08 | 82.86 | 0.08 | 84.54 |
| 200 | 10 | 0.02 | 78.36 | 0.02 | 80.50 |
| 200 | 11 | 0.02 | 72.46 | 0.02 | 74.68 |
| 200 | 12 | 0.00 | 70.25 | 0.00 | 72.57 |

## Ⅴ. 결 론

많은 장점을 가지고 있는 바이오정보, 특히 지문정보가 악의적인 사용자에게 유출되었을 때 심각한 문제가 제기 될 수 있다. 최근 지문정보를 안전하게 보호하기 위해서 암호학적 방법인 퍼지볼트 이론을 지문인식 시스템에 적용하는 지문 퍼지볼트에 관한 연구가 활발히 진행되고 있다. 본 논문에서는 지문 퍼지볼트 시스템을 실제적으로 구현할 때 적은 개수의 특징점을 가지는 지문영상은 동작하지 못하는 문제점을 해결하기 위한 방법을 제안한다. 본 논문에서는 낮은 차수의 다항식에 대해 두 개 이상의 서로 다른 다항식을 사용하여 기존 지문 퍼지볼트 방법에 추가적인 변형 없이 동작할 수 있는 시스템을 구현하였다.

FVC2002 DB1 Set A의 지문 이미지를 사용하여 실험한 결과 높은 보안성을 유지하면서 GAR이 향상되는 것을 보였다.

## 참고문헌


[1] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, pp. 1-52, 2003.

[2] A.K. Jain, R. Bole, and S. Panakanti, Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, pp. 1-41, 1999.

[3] R. Bolle, J. Connell, and N. Ratha, “Biometric Perils and Patches,” Pattern Recognition, vol. 35, no. 12, pp. 2727-2738, Dec. 2002.

[4] A. Juels and M. Sudan, “A Fuzzy Vault Scheme,” Proceedings of IEEE International Symposium on Information Theory, pp. 408-409, June 2002.

[5] T. Clancy, N. Kiyavash, and D.J. Lin, “Secure Smartcard-based Fingerprint Authentication,” Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications, pp. 45-52, Nov. 2003.

[6] U. Uludag, S. Pankanti, and A.K. Jain, “Fuzzy Vault for Fingerprints,” Proceedings of Audio- and Video-based Biometric Person Authentication, LNCS 3456, pp. 310-319, 2005.

[7] Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, and D. Ahn, “Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault,” Proceedings of Conference on Information Security and Cryptology, LNCS 3822, pp. 358-369, 2005.

[8] 이성주, 문대성, 김학재, 정용화, 이옥연, “3차원 기하학적 해싱을 이용한 퍼지볼트에서의 지문 정합,” 정보보호학회논문지, 18(1), pp. 11-21, 2008년 2월.

[9] http://bias.csr.unibo.it/fvc2002/databases.asp.


## <著 者 紹 介>


문 대 성 (Dae-Sung Moon) 정회원
1999년 2월: 인제대학교 전산학과 졸업
2001년 2월: 부산대학교 컴퓨터공학과 석사
2007년 2월: 고려대학교 전산학과 박사
2000년 12월~현재: 한국전자통신연구원 바이오인식기술연구팀 선임연구원
<관심분야> 바이오인식, 영상처리, 바이오정보보호

최 우 용 (Woo Yong Choi) 정회원
1998년 2월: 부산대학교 통계학과 학사
2000년 2월: 부산대학교 전자공학과 석사
2000년 2월~2001년 1월: L&H Korea 연구원
2001년 2월~현재: 한국전자통신연구원 선임연구원
<관심분야> 바이오인식, 정보보호, 영상처리

문 기 영 (Ki Young Moon) 종신회원
1986년 2월: 경북대학교 전자공학과 학사
1989년 2월: 경북대학교 전산학 석사
2006년 2월: 충남대학교 전산학 박사
1992년~1994년: (주)대우정보시스템 기술연구소 전임연구원
1994년 3월~현재: 한국전자통신연구원 바이오인식기술연구팀 팀장
<관심분야> 바이오인식, 정보보호, 웹서비스보안