情報保護學會論文誌
第 21 卷 第 2 號, 2011. 4

# 상관관계 공격에 강인한 지문퍼지볼트 시스템*

문 대 성[1†], 채 승 훈[2], 정 용 화[3‡], 김 성 영[4], 김 정 녀[1]
[1]한국전자통신연구원, [2]조선대학교, [3]고려대학교, [4]금오공과대학교

# Robust Fuzzy Fingerprint Vault System against Correlation Attack*

Daesung Moon[1†], Seung-Hoon Chae[2], Yongwha Chung[3‡],
Sung-Young Kim[4], and Jeong-Nyeo Kim[1]
[1]ETRI, [2]Chosun University, [3]Korea University, [4]Kumoh National Inst. of Tech.

## 요 약

바이오인식 기술을 이용한 사용자 인증은 편리함과 동시에 강력한 보안성을 제공하는 등 많은 장점을 가지고 있다. 그러나 사용자 인증을 위해 저장된 중요한 바이오정보가 타인에게 유출되어 도용된다면 패스워드나 PIN과 달리 변경이 불가능하므로 심각한 문제를 일으킬 수 있다. 지문 템플릿 정보를 안전하게 보호하기 위해 암호학적 방법으로 연구되어지고 있는 퍼지볼트 이론(Fuzzy Vault Scheme)을 적용한 지문퍼지볼트 시스템이 가장 널리 알려진 방법이다. 그러나 지문퍼지볼트 시스템은 두 개 이상의 지문볼트를 이용하여 진짜특징점을 구분하는 상관관계 공격(Correlation Attack)에 취약한 결정적인 문제점이 있다. 본 논문에서는 거짓특징점을 임의로 추가하지 않고 특징점의 좌표, 방향 등 진짜특징점의 정보를 이용하여 추가함으로써 상관관계 공격에 강인한 지문퍼지볼트 시스템을 제안한다. 또한, 인접위치에 두 개 이상의 거짓특징점을 추가하는 중첩을 허용함으로써 보안성을 향상시킬 수 있다. 실험을 통하여 제안한 방법은 높은 인식성능을 유지하면서 상관관계 공격에 강인함을 보였다.

## ABSTRACT

Biometric-based authentication can provide strong security guarantee about the identity of users. However, security of biometric data is particularly important as the compromise of the data will be permanent. The fuzzy fingerprint vault system is one of the most popular solutions for protecting the fingerprint template stored in the database. Recently, however, this system is very susceptible to a correlation attack that finds the real minutiae using multiple fingerprint vaults enrolled for different applications. To solve this problem, we propose a robust fuzzy fingerprint vault system against the correlation attack. In this paper, we add chaff minutiae based on the relative information of minutiae such as direction, coordinate instead of adding randomly. Also, our proposed approach allow to add multiple chaff minutiae within tolerance box for enhanced security level. Experimental results show that the proposed approach can protect the correlation attack and achieve enhanced verification accuracy.

**Keywords**: Fingerprint Verification, Fuzzy Fingerprint Vault, Correlation Attack

접수일(2010년 6월 14일), 게재확정일(2010년 10월 23일)
* 본 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2010-0027794)
† 주저자, daesung@korea.ac.kr
‡ 교신저자, ychungy@korea.ac.kr

## I. 서 론

최근 개인의 고유한 바이오정보를 이용한 정보보호 및 사용자인증 등의 연구가 활발히 진행되고 있다[1-3]. 그러나 한정된 개수(하나의 얼굴, 열 개의 손가락 등)를 가진 바이오정보는 패스워드와 다르게 유출 시 마다 자유롭게 변경할 수 없으며, 일반적으로 사용자는 동일한 바이오정보를 다양한 응용에 사용하기 때문에 유출된 바이오정보는 모든 응용에서 재사용될 수 있기 때문에 악의적인 목적을 가진 공격자에게 유출된다면 심각한 문제를 야기할 수 있다. 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[5-7]. 본 논문에서도 퍼지볼트(Fuzzy Vault) 이론[4]을 지문인증 시스템에 적용한 지문퍼지볼트 시스템의 효율적으로 구현방안에 대하여 기술한다. 지문퍼지볼트 시스템은 등록과정에서 다항식을 생성하고 지문영상으로부터 추출된 사용자의 지문 특징정보를 다항식에 사영한다. 또한 사용자의 지문 특징정보를 타인으로부터 은닉하기 위해서 다수의 거짓 특징정보를 추가하여 지문볼트라는 형태로 저장한다. 인증과정에서 거짓 특징정보를 함께 포함하고 있는 지문볼트로부터 사용자의 지문 특징정보만을 선택한 후, 등록과정에서 사용된 것과 동일한 다항식을 생성할 경우 본인으로 인증한다. 즉, 지문퍼지볼트 시스템의 보안성은 지문볼트로부터 사용자의 지문특징과 거짓특징을 구분하는 어려움에 기반을 둔다. 본인의 경우에는 등록과정에서 제공했던 것과 동일한 지문으로 지문인증을 요구하기 때문에 지문볼트에서 사용자의 지문 특징정보를 쉽게 분리할 수 있다.

그러나 최근 동일한 지문으로부터 생성되는 두 개의 지문볼트를 취득함으로써 진짜특징점과 거짓특징점을 쉽게 구별할 수 있다는 상관관계 공격(Correlation Attack)을 언급하고 다양한 실험결과가 발표되었다[8-10]. 즉, 두 개의 동일 지문으로부터 추출되는 진짜특징점들은 특징점 간의 위치와 각도에 대한 상대적인 정보가 유지되는 반면, 거짓특징점은 랜덤함수에 의해 임의로 생성된다. 따라서 두 지문볼트를 정렬하여 매칭되는 특징점들을 찾으면 진짜특징점 다수와 거짓특징점 소수가 선택되어 공격자가 지문퍼지볼트 시스템을 쉽게 공격할 수 있다.

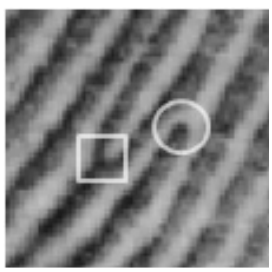
본 논문에서는 상관관계 공격에 대응하기 위해서 거짓특징점을 임의로 생성하는 대신 진짜특징점의 상대적인 정보(좌표, 방향 등)를 이용하여 생성한다. 즉, 진짜와 거짓특징점이 기하학적인 관계를 가지게 함으로써 상관관계 공격에서 다수의 진짜특징점만이 매칭되는 것을 해결할 수 있다. 실험을 통해 제안한 방법은 인식율의 저하 없이 상관관계 공격에 강인함을 보였다.

본 논문의 구성은 다음과 같다. 2장에서는 지문인증 시스템의 일반적인 내용과 퍼지볼트에 대해 설명한다. 3장에서는 본 논문에서 제안한 상관관계 공격에 강인한 지문퍼지볼트에 대하여 설명 하고, 4장에서는 실험결과에 의한 성능을 평가한다. 마지막으로 5장에서는 결론을 맺는다.

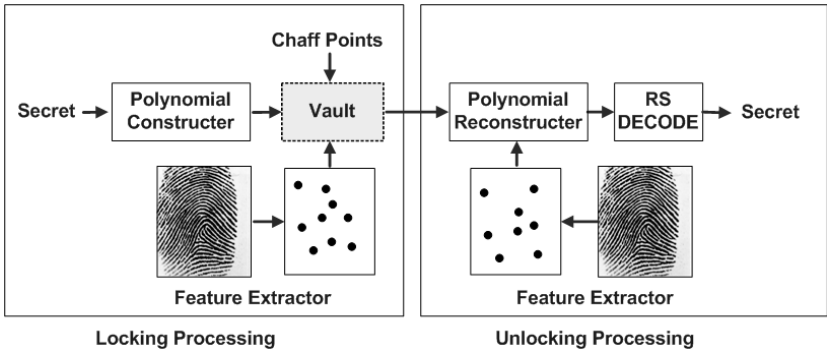
## II. 지문인식 시스템

### 2.1 지문인식

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




〔그림 2〕 지문 퍼지볼트 시나리오

지문을 이용한 특징점 기반 사용자 인증 시스템은 사용자 등록(enrollment) 과정과 사용자 인증(verification) 과정으로 수행된다. 사용자 등록 과정은 획득된 지문 영상의 품질을 향상시키기 위한 전처리 단계를 거친 후 특징추출 단계에서 특징점 정보들을 추출하여 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.

동록과정에서 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 복원할 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[5-7]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 가정 해보자. 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 $G$를 생성한다 (원소 개수가 $g$개인 집합 $G$를 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 $G$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 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 $G$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 지문퍼지볼트

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 라킹셋으로 인증과정의 특징점을 언라킹셋으로 대입하여 적용할 수 있다. 〔그림 2〕에 나

타난 바와 같이 지문퍼지볼트는 Locking과정과 Unlocking과정으로 구성되며, 각 단계에 대한 자세한 설명은 다음과 같다.

#### 2.3.1. Locking 과정

지문퍼지볼트의 Locking 과정은 다음과 같다.

① 사용자의 등록지문으로부터 $n$ 개의 특징점을 추출하고, 이를 진짜특징점(real minutiae)이라 정의한다.

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

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

$$p(x)=a_0+a_1x+\cdots+a_kx^k \tag{2}$$

$$S=(a_0\|a_1\|\cdots\|a_k) \tag{3}$$

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

$$\kappa=h(S) \tag{5}$$

③ 집합 $L$의 원소들을 $\mathrm{GF}(p^2)$ 의 원소로 변환하여 이 값을 $p(x)$ 상에 수식 7과 같이 사영(projection)하여 집합 $G_{\mathrm{L}}$ 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.

$$G_L=\{(g_i,v_i)|i=1,\cdots,n\},\ g_i=(x_i,y_i,\theta_i,t_i) \tag{6}$$

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

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

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

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

$$v_i=p(X_i)+\alpha_i,\ \ X_i=x_iX+y_i\in \mathrm{GF}(p^2),$$
$$i=n+1,\cdots,g \tag{9}$$

여기서, $\alpha_i$ 는 0이 아닌 임의의 수이다.

⑤ $G_{\mathrm{L}}$과 $C$를 원소의 순서가 무작위가 되도록 통합하여 집합 $G$를 구성한다.

$$G=\{(g_i,v_i)|i=1,\cdots,g\},\ g_i=(x_i,y_i,\theta_i,t_i) \tag{10}$$

⑥ 집합 $G$와 비밀정보 $S$의 해쉬값 및 다항식의 차수 $k$로 구성된 지문볼트($V$)를 저장된다.

$$V=\{(g_i,v_i),\kappa,k|i=1,\cdots,g\} \tag{11}$$

#### 2.3.2. Unlocking 과정

지문퍼지볼트의 Unlocking 과정은 입력 지문의 특징점으로부터 다항식을 복원하는 과정이다. 지문퍼지볼트의 Unlocking 과정은 다음과 같다.

① 입력지문으로부터 $m$개의 특징점을 추출한다.

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

② 집합 $U$와 Locking 과정에서 저장된 집합 $V$의 $g_{\mathrm{i}}$를 입력으로 지문정합을 수행하여 $t$ 개의 서로 일치하는 특징점들을 구하고, 이들 일치하는 특징점정보와 해당 $v_{\mathrm{i}}$ 값으로 구성된 집합 $M$을 생성한다.

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

이때, $M\subseteq G, t\le g$ 이다.

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

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

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

$$\kappa'=h(a_0'\|a_1'\|\cdots\|a_k') \tag{16}$$

④ $\kappa'$와 $\kappa$가 일치하면 본인으로 수락하고, 그렇지 않으면 거절한다.

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

지문퍼지볼트에서 일치하는 특징점의 개수가 $k+1$ 개 이상 존재할 경우 $k$차 다항식을 복원할 수 있다. 그러나 동일인의 지문을 이용하여 지문인증을 시도할 경우에도 일치하는 특징점의 집합인 $M$에 거짓특징점이 포함될 수 있으며, 이러한 거짓특징점은 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 진짜특징점이 필요로 한다[5].

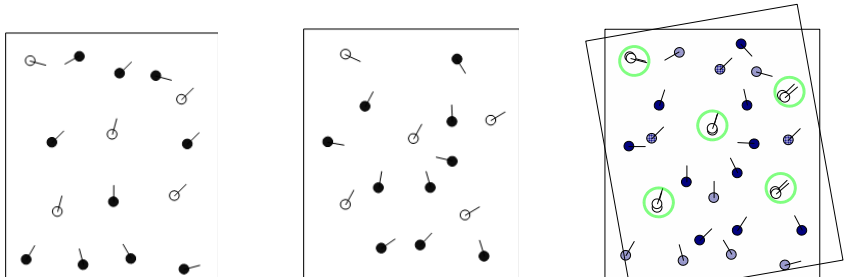
### 2.4 지문퍼지볼트의 상관관계 공격

앞서 언급하였듯이, 지문퍼지볼트 시스템의 보안성은 등록된 지문볼트로부터 진짜특징점과 거짓특징점을 구분하는 어려움에 기반을 둔다. 즉, 본인이 인증을 요청하였을 때에는 등록과정에서와 동일한 지문을 사용하기 때문에 지문볼트에서 진짜특징점을 분리하여 다항식 복원을 할 수 있다. 그러나 악의적인 공격자는 진짜특징점 정보를 알 수 없기 때문에 지문볼트로부터 $k+1$의 특징점을 선택한 후 다항식을 재생성하는 전수조사 공격(brute-force)을 시도 할 것이다. 이럴 경우 지문퍼지볼트의 공격 복잡도(complexity)는 수식 18과 같다. 수식 18은 지문볼트에서 정확하게 $k+1$개의 진짜특징점을 선택할 수 있는 확률이며, 거짓특징점을 많이 추가할수록 그리고 진짜특징점 개수에 가까운 다항식 차수를 사용할수록 복잡도는 향상된다.

$$Complexity\,1 = {}_{g}C_{k+1} / {}_{n}C_{k+1} \tag{18}$$

수식 18에 의한 공격 복잡도는 하나의 지문볼트가 공격자에게 유출되었을 경우에 공격자가 진짜와 거짓특징점을 분리할 수 있는 경우의 수이다. 그러나 동일한 지문으로부터 생성되는 두 개의 지문볼트를 취득함으로써 진짜특징점과 거짓특징점을 쉽게 구별할 수 있다는 상관관계 공격을 언급하고 다양한 실험결과가 발표되었다[8-10]. 〔그림 3〕은 상관공격에 의한 지문퍼지볼트의 공격 과정의 예를 보여준다. 〔그림 3〕에서 흰색 원과 검은색 원은 각각 진짜와 거짓특징점을 나타낸다. 〔그림 3(a)〕와 〔그림 3(b)〕의 진짜특징점들은 동일한 지문으로부터 추출되었기 때문에 약간의 천의(translation)와 회전(rotation)이 존재하지만 각 특징점들 간의 상대적인 구조는 유지됨을 알 수 있다. 〔그림 3(a)〕와 〔그림 3(b)〕의 진짜특징점에 임의로 생성된 거짓특징점을 추가하여 두 개의 지문볼트(vault A, vault B)를 생성하였다. 즉, 〔그림 3(a)〕와 〔그림 3(b)〕의 지문볼트들에서 진짜특징점의 기하학적인 구조는 유지되지만 거짓특징점은 상대적인 관련성이 없음을 알 수 있다. 〔그림 3(c)〕는 두 개의 지문볼트에 매칭과정을 수행한 상관관계 공격의 결과를 보여주며, 5개의 진짜특징점이 매칭되는 것을 알 수 있다. 실제 동일 지문영상으로부터 추출된 두 개의 진짜특징점 집합을 이용하여 상관관계 공격을 가했을 경우에는 수백 개의 거짓특징점이 추가되기 때문에 매칭되는 특징점들 중에는 진짜특징점 다수와 거짓특징점 소수가 추출된다. 따라서 상관관계 공격의 결과한 공격복잡도(수식 18)를 계산하면 상당히 낮아지게 된다.

기존의 상관공격을 방지하기 위한 연구들을 살펴보면 사용자의 지문정보와 더불어 비밀번호와 같은 부가적인 정보를 이용하였다[11,12]. 그러나, 이와 같은 방법은 사용자 인증 시스템에서 지문정보를 사용하는 가장 큰 장점인 편리성을 크게 훼손한다. 다른 방법으로는 사용자의 지문으로부터 추출한 진짜특징점을 변형하는 방법이다[13]. 즉, 하나의 진짜특징점과 가장 가까운 위치에 있는 진짜특징점을 이용하여 위치를 변경



(a) vault A (b) vault B (c) 상관관계공격 결과

〔그림 3〕 상관관계 공격의 예

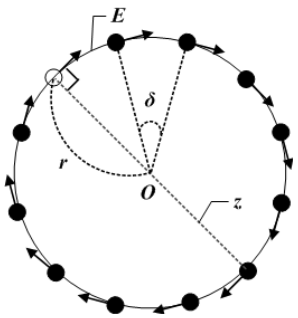
하는 것이다. 따라서, 퍼지볼트를 생성할 때 다른 지문정보로 변경된다. 그러나 이와 같은 방법도 여러 개의 응용에서 지문퍼지볼트를 생성할 경우, 진짜특징점의 개수가 줄 뿐만 아니라 지문퍼지볼트를 구성하는 지문정보들이 비슷한 모양을 갖게 될 것이다. 변경시키는 정보가 안전하다는 보장이 없기 때문에 진짜특징점을 유추할 수 있게 된다.

또한 무작정 많은 거짓특징점을 삽입한다면, 인식율의 저하, 수행시간의 증가 등 지문퍼지볼트 시스템의 실생활 적용이 힘들게 된다.

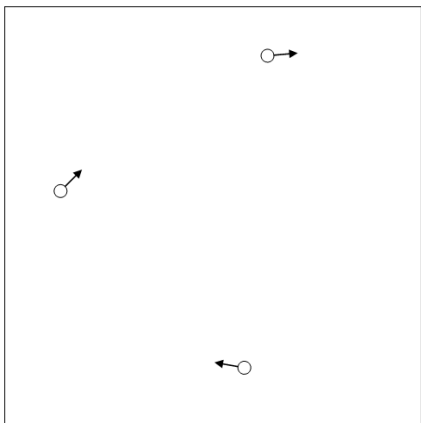
## III. 상관관계 공격에 강인한 지문퍼지볼트

### 3.1 진짜특징점 정보를 이용한 거짓특징점 생성

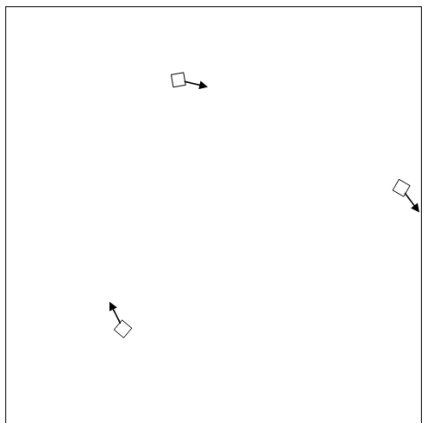
지문퍼지볼트가 상관공격에 취약한 중요한 요인은 진짜특징점은 항상 유사하게 추출되는 반면, 삽입되는 거짓특징점은 랜덤하게 불규칙적으로 추가됨으로써 각각의 응용마다 다르게 삽입 되는 것이다. 따라서 본 논문에서는 이러한 문제점을 해결하기 위해서 거짓특



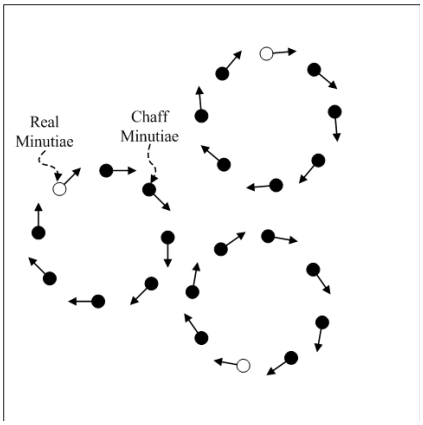

〔그림 4〕 제안된 거짓특징점 생성 방법;
(흰색 원 : 진짜특징점, 검은색 원 : 거짓특징점)



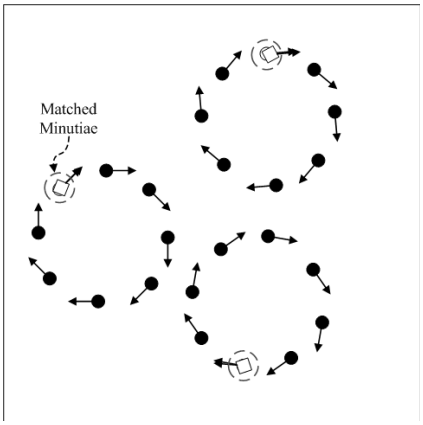
(a) 등록특징점



(b)인증특징점




(c) 지문볼트 1




(d) 지문퍼지볼트 시스템의 매칭결과

〔그림 5〕 제안한 방법의 지문퍼지볼트 시스템

징점을 임의로 추가하는 대신, 진짜특징점의 정보(방향, 좌표 등)에 기반을 두어 추가함으로써 진짜특징점과의 연관성을 가지도록 하였다.

〔그림 4〕는 본 논문에서 제안한 거짓특징점을 생성하는 방법을 보여주며, 다음과 같은 절차를 따른다.

① n 개의 진짜특징점의 집합 $L$에서 첫 번째 진짜특징점 $L_1$을 기준특징점(basis minutiae)으로 선택한다.
② $L_1$의 방향성 정보 $\theta_1$에 대하여 오른쪽으로 수직인 직선 $z$를 그린다.
③ 반지름 정보 $r$을 선택하여 ②번 과정에서 구한 직선 $z$상에 원점 $O$를 구한다.
④ 원점 $O$에 대해서 반지름 $r$을 가지며 $L_1$의 방향성 정보 $\theta_1$에 접원 $E$를 그린다.
⑤ 접원 $E$상에 $\delta$만큼 떨어진 간격으로 접원 $E$ 상에 거짓특징점을 생성하며 수식 2와 같은 정보로 구성된다. 거짓특징점의 좌표정보는 접원 상의 좌표값이며 각도정보는 거짓특징점의 좌표값에서 원의 접선의 방향을 가진다. 마지막으로 타입정보는 기준특징점 $L_1$과 동일한 값을 가진다. 기준특징점의 상대적인 정보를 이용하여 추가되는 거짓특징점은 기준특징점에 종속되기 때문에 수식 8의 거짓특징점을 수식 19와 같이 재정의 한다.

$$C(1)=\{(c_j(1),v_j(1))\mid j=1,\cdots,g(1)\},\quad c_j(1)=(x_j,y_j,\theta_j,t_j) \tag{19}$$

$$v_j(1)=p(X_j)+\alpha_j,\ \ X_j=x_jX+y_j\in \mathrm{GF}(p^2),\quad j=1,\cdots,g(1) \tag{20}$$

여기에서, $g(1)$은 기준특징점 $L_1$에 대하여 생성되는 거짓특징점의 개수를 의미한다.

⑥ 나머지 모든 진짜특징점을 기준특징점으로 사용하여 ②~⑤ 단계를 반복적으로 수행하면 거짓특징점 집합 $C$를 생성하고 총 거짓특징점의 개수는 $g$개가 된다. $v_j(i)$는 수식 9의 $v_i$와 동일한 의미를 가지며, $C(i)$에서 $i$는 진짜특징점의 인덱스이다.

$$C=\{C(i)\}=\{(c_j(i),v_j(i))\mid i=1,\cdots,n,\ j=1,\cdots,g(i)\},\quad c_j(i)=(x_j,y_j,\theta_j,t_j) \tag{21}$$

$$g=g(i)*n \tag{22}$$

〔그림 5〕는 본 논문에서 제한된 지문퍼지볼트 시스템의 실행 예를 보여준다. 〔그림 5(a)〕와 〔그림 5(b)〕는 각각 등록특징점과 인증특징점이다. 〔그림 5(c)〕는 본 논문에서 제안한 지문퍼지볼트 시스템의 지문볼트를 보여준다. 〔그림 5(c)〕에서 보는 바와 같이 〔그림 5(a)〕의 등록특징점에 대해서 거짓특징점을 추가하여 지문볼트를 생성하였다. 〔그림 5(d)〕는 지문퍼지볼트 시스템에서 사용자 인증과정을 수행한 결과로써 〔그림 5(c)〕와 〔그림 5(a)〕를 정렬하여 일치하는 특징점이 가장 많은 경우를 나타낸다. 즉, 〔그림 5(a)〕와 〔그림 5(b)〕가 동일인의 지문으로부터 추출된 특징점이기 때문에 지문볼트에서 진짜특징점과 매칭되어 본인으로 인증하는 것을 볼 수 있다.

본 논문에서 제안된 방법은 수식 18에 의한 전수조사 공격 복잡도를 높이기 위해서 반지름($r$)과 간격($\delta$)을 조절하여 추가되는 거짓특징점의 개수를 조절할 수 있다. 또한, 거짓특징점이 지문영상 밖에 위치하여 추가되지 못하는 것을 피하기 위해 지문영상은 변경하지 않고 영상의 크기만을 확장하여 사용한다.

### 3.2 거짓특징점의 중첩 허용

일반적으로 지문인식 시스템에서 등록지문 특징점과 인증지문 특징점은 정렬과정을 거친 후 특징점의 좌표값과 각도에 대해서 허용오차 이내에 존재하는 특징점 쌍의 비율로써 유사도를 결정한다[1]. 따라서, 기존의 지문퍼지볼트 시스템에서는 임의로 생성된 거짓특징점이 좌표에 대한 허용오차($\Delta x$, $\Delta y$)이내에 다른 특징점이 존재한다면 추가하지 않고 새로운 거짓특징점을 생성하여 추가한다. 이는 일반적인 지문영상에서는 존재할 수 없는 특징점의 패턴이 발생하여 거짓특징점이 노출될 수 있고, 허용오차 이내에 생성된 거짓특징점에 의해 인식율이 저하될 수 있기 때문이다.

본 논문에서는 〔그림 6〕에서 보는 바와 같이 거짓특징점이 허용오차 이내에 추가되는 중첩을 허용한다. 〔그림 6(a)〕와 같이 세 개의 진짜특징점이 있을 때, 기준특징점을 a, b, c의 순서로 선택하여 거짓특징점을 생성한다고 가정해보자. 제안한 방법의 지문퍼지볼트 시스템에서는 〔그림 6(b)〕와 같이 동일한 규칙을 가지고 거짓특징점을 생성하여 하나의 기준특징점에 대해서 동일한 개수의 거짓특징점이 생성된다. 〔그림 6(b)〕의 점선 사각형이 좌표에 대한 허용오차라고 할

때 허용오차 이내에 다른 특징점이 존재하더라도 거짓 특징점이 추가된다. 그러나, 기존의 지문퍼지볼트 시스템은 〔그림 6(c)〕처럼 좌표에 대한 허용오차 이내에 다른 특징점이 존재한다면 거짓특징점을 추가하지 않는다. 이는 나중에 선택된 기준특징점은 추가되는 거짓특징점의 개수가 적어 보안성에 문제점이 있다.

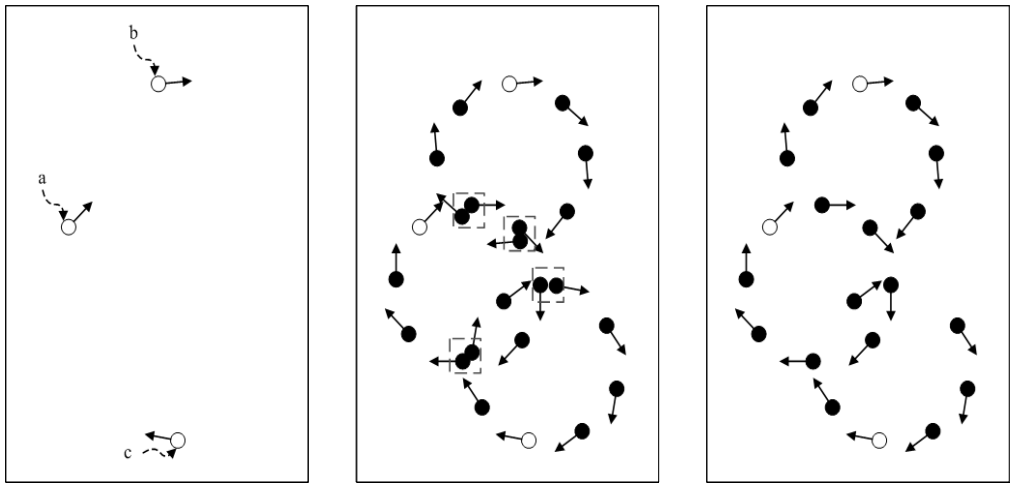
### 3.3 제안한 방법의 안전성

본 논문에서 제안한 지문퍼지볼트 시스템은 수식 18의 공격복잡도에 추가적으로 수식 23에 의한 공격복잡도를 가진다.

$$Complexity\,2 = (g(i)+1)^{k+1} \tag{23}$$

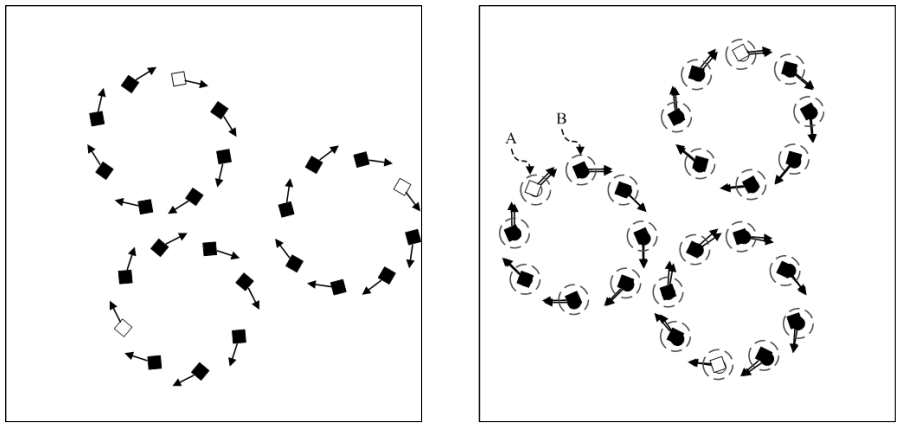
기존의 지문퍼지볼트 시스템의 거짓특징점은 진짜 특징점에 의존성 없이 임의로 추가되기 때문에 전체 지문볼트에서 $k+1$개의 진짜특징점을 선택하는 경우의 수가 공격복잡도이다. 반면, 본 논문에서 제안한 지문퍼지볼트 시스템에서 거짓특징점은 진짜특징점을 기준으로 추가되기 때문에 〔그림 5(c)〕에서 보는 것과 같이 하나의 진짜특징점과 $g(i)$개의 거짓특징점이 그룹을 형성하게 된다. 따라서 $(g(i)+1)$개의 특징점으로 구성된 그룹에서 하나의 진짜특징점을 선택하고, 같은 방법으로 $k+1$개의 그룹에서 진짜특징점을 선택하면 지문퍼지볼트 시스템을 공격할 수 있다.

〔그림 7〕은 본 논문에서 제안한 지문퍼지볼트 시스템에 상관관계 공격을 가한 결과를 보여준다. 〔그림 7(a)〕는 〔그림 5(b)〕로부터 생성된 지문볼트이다.




(a) 진짜특징점 (b) 제안한 방법에 의한 거짓특징점 생성 (c) 기존의 거짓특징점 생성

〔그림 6〕 중첩이 허용된 거짓특징점 추가의 예



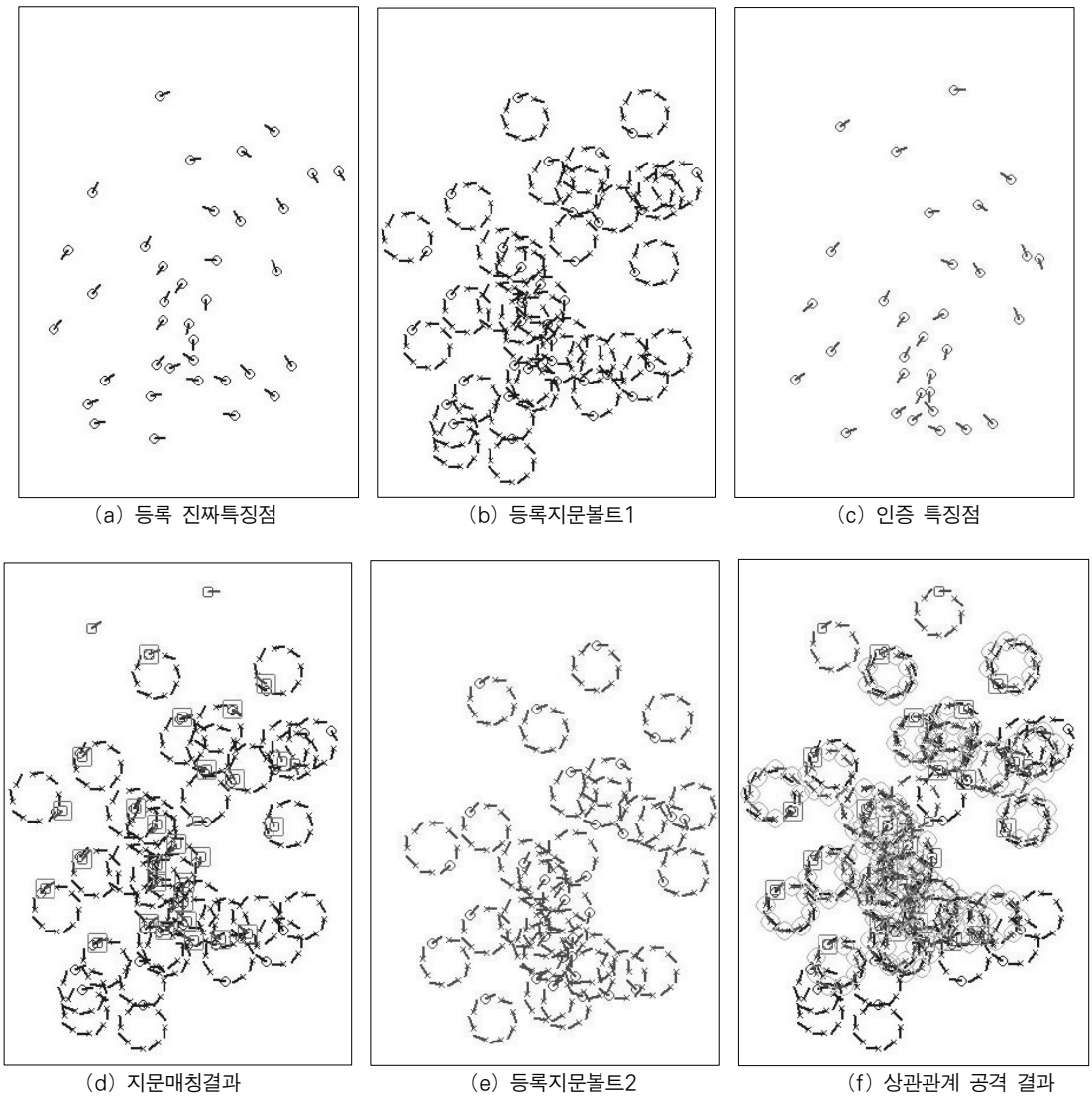

(a) 지문볼트 2 (b) 상관관계 공격 결과 1

〔그림 7〕 제안된 지문퍼지볼트 시스템의 상관관계 공격

〔그림 7(b)〕는 동일한 지문으로부터 생성된 두 개의 지문볼트(〔그림 5(c)〕와 〔그림 7(a)〕)에 대하여 정확하게 정렬된 상관관계 공격의 예를 보여준다. 〔그림 7(b)〕에서 보는바와 같이 올바르게 정렬된 상관관계 공격의 결과는 진짜특징점 뿐만 아니라 거짓특징점 또한 매칭되는 특징점 쌍으로 나오기 때문에 공격자는 상관관계 공격으로 진짜특징점을 분리할 수가 없다. 특히 본 논문에서 제안한 지문퍼지볼트 시스템은 상관관계 공격에서 진짜특징점인 A에 의한 정렬이나 거짓특징점인 B에 의한 정렬결과가 동일하기 때문에 두 개의 지문볼트의 지문매칭으로는 진짜특징점 정보를 알 수 없다.

## IV. 실험결과

본 논문에서 제안한 지문퍼지볼트 시스템의 성능을 측정하기 위하여 FVC2002 DB1 Set A[14]를 사용하였다. FVC 2002 실험환경과 동일하게 본인정합은 8장의 이미지 각각에 대해서 나머지 이미지와 정합을 수행하였으며, 한번 등록된 것은 이후의 정합에는 사용하지 않았다. 타인정합은 각 손가락의 첫 번째 이미지만 사용하였는데, 본인정합과 마찬가지로 100장의



(a) 등록 진짜특징점 (b) 등록지문볼트1 (c) 인증 특징점

(d) 지문매칭결과 (e) 등록지문볼트2 (f) 상관관계 공격 결과

〔그림 8〕 상관관계 공격에 강인한 지문퍼지볼트 시스템의 실험 결과

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.

〔그림 8〕은 본 논문에서 제안한 상관관계 공격에 강인한 지문퍼지볼트 시스템의 실험결과를 보여준다. 〔그림 8(a)〕는 FVC2002 DB1 Set A의 1_1.tif 지문으로부터 추출된 진짜특징점을 보여준다. 〔그림 8(b)〕는 〔그림 8(a)〕를 숨기기 위해 생성된 지문볼트이며 "O"와 "X"는 각각 진짜와 거짓특징점을 의미한다. 거짓특징점을 생성할 때 사용된 반지름($r$)과 간격($\delta$)은 각각 20과 8이다. 또한, 거짓특징점을 추가할 때 중첩을 허용하기 때문에 〔그림 8(b)〕와 같이 하나의 진짜특징점에 대해서 동일한 개수의 거짓특징점이 추가된다. 지문인증 과정에서 동일인의 지문인 1_2.tif 영상에서 특징점(〔그림 8(c)〕)을 추출한 후, 등록된 지문볼트(〔그림 8(b)〕)와 매칭한 결과가 〔그림 8(d)〕이다. 〔그림 8(d)〕에서 보는 바와 같이 동일한 지문이기 때문에 진짜와 거짓특징점으로 구성된 지문볼트에서 대부분 진짜특징점들이 매칭되어 본인으로 판정된다.

다음으로, 본 논문에서 제안한 방법이 상관관계 공격에 효과적으로 대응하는지 여부를 검증한다. 상관관계 공격을 위해서는 두 개의 등록된 지문볼트가 필요하기 때문에 동일 지문인 1_1.tif와 1_2.tif에서 추출된 진짜특징점에 거짓특징점을 각각 추가하여 두 개의 지문볼트(〔그림 8(b)〕, 〔그림 8(e)〕)를 생성한다. 공격자가 획득한 두 개의 지문볼트를 매칭하는 상관관계 공격의 결과가 〔그림 8(f)〕이다. 본 논문에서는 거짓특징점을 랜덤하게 추가하지 않고 진짜특징점의 상대적인 정보를 이용하여 추가하였기 때문에 〔그림 8(f)〕에서 보는 바와 같이 진짜특징점 외에 다수의 거짓특징점 또한 일치하는 특징점으로 인식된다. 따라서 상관관계 공격을 이용하여 등록된 지문볼트에서 진짜특징점을 구분할 수 없다.

〔표 1〕 1_1.tif 와 1_2.tif의 지문퍼지볼트 실험결과, 8차 다항식 사용

| | | 지문 | 진짜특징점 개수 | 거짓특징점 개수 | 매칭된 특징점 개수 |
|---|---|---|---|---|---|
| 기존 지문퍼지볼스 시스템[15] | 지문 인증 | 1_1.tif | 37 | 200 | 진짜 : 26<br>거짓 : 1 |
| | | 1_2.tif | 32 | - | |
| | 상관관계 공격 | 1_1.tif | 37 | 200 | 진짜 : 30<br>거짓 : 8 |
| | | 1_2.tif | 32 | 200 | |
| 제안한 방법 | 지문 인증 | 1_1.tif | 37 | 259 | 진짜 : 27<br>거짓 : 0 |
| | | 1_2.tif | 32 | - | |
| | 상관관계 공격 | 1_1.tif | 37 | 259 | 진짜 : 27<br>거짓 : 187 |
| | | 1_2.tif | 32 | 224 | |

〔표 2〕 1_1.tif 와 1_2.tif의 공격복잡도, 8차 다항식 사용

| | | 진짜특징점 개수 | 거짓특징점 개수 | *Complexity* 1 (수식 18) | *Complexity* 2 (수식 23) |
|---|---|---|---|---|---|
| 기존 지문퍼지볼스 시스템[15] | 지문볼트 | 37 | 200 | $4.4 * 10^7$ (=C(237,9)/C(37,9)) | - |
| | 상관관계 공격 | 30 | 8 | $1.1 * 10^1$ (=C(38,9)/C(30,9)) | - |
| 제안한 방법 | 지문볼트 | 37 | 259 | $3.4 * 10^8$ (=C(296,9)/C(37,9)) | $(7+1)^9$ |
| | 상관관계 공격 | 27 | 187 | $4.6 * 10^8$ (=C(214,9)/C(27,9)) | - |

〔표 3〕 지문퍼지볼트 시스템 인식성능 실험 결과

| Parameter | 기존 지문퍼지볼트 시스템[15] | | | 제안 방법 | | |
|---|---|---|---|---|---|---|
| 평균 특징점 개수 | 27.95 | | | 27.95 | | |
| 다항식 차수 | Chaff (고정) | FAR (%) | GAR (%) | Chaff (평균) | FAR (%) | GAR (%) |
| 8 | 200 | 0.12 | 86.93 | 220.05 | 0.6 | 91.17 |

지문 1_1.tif와 1_2.tif에 대한 지문퍼지볼트 시스템의 지문인증과 상관관계 공격 실험을 정리하면 〔표 1〕과 같다. 지문인증은 1_1.tif의 진짜특징점에 거짓특징점을 추가하여 지문볼트를 만들고 1_2.tif의 특징점으로 사용자 인증을 시도하는 것이며, 상관관계 공격은 지문 1_1.tif와 1_2.tif 각각에 대해서 지문볼트를 생성하고 두 개의 지문볼트에서 일치하는 특징점쌍을 획득하는 실험이다. 〔표 1〕에서와 같이 기존의 지문퍼지볼트 시스템의 경우 200개의 거짓특징점을 임의로 추가하였으며, 지문인증 실험은 26개의 진짜특징점이 매칭되어 8차 다항식에 대해서 본인인증을 성공하였다. 그러나 상관관계 공격 실험에서 30개의 진짜특징점과 8개의 거짓특징점이 매칭되어 공격자는 8차 다항식을 재생성하기 위해 9개의 진짜특징점을 쉽게 선택할 수 있다. 본 논문에서 제안한 지문퍼지볼트 시스템은 지문 1_1.tif에 대해 259개의 거짓특징점이 추가되어 지문볼트를 생성하고 지문인증의 결과 진짜특징점이 27개 매칭되어 사용자를 인증하였다. 상관관계 공격에서는 1_2.tif에 대해서 224개의 거짓특징점을 추가하여 새로운 지문볼트를 생성하였다. 수식 22와 같이 진짜특징점의 개수에 의해 거짓특징점의 개수가 결정되어 서로 다른 개수가 추가되며, 본 실험에서는 반지름($r$)과 간격($\delta$)이 각각 20과 8로 설정되어 하나의 진짜특징점에 대해 7개의 거짓특징점이 추가되었다. 제안한 방법에 대한 상관관계 공격결과는 진짜와 거짓특징점이 각각 27개와 187개가 매칭되어 공격자는 상관관계 공격 결과로부터 진짜특징점의 선택이 용이하지 않다.

〔표 2〕는 〔표 1〕의 실험결과에 대한 공격복잡도를 보여준다. 즉, 등록과정에서 진짜와 거짓특징점으로 구성된 지문볼트의 공격복잡도와 상관관계 공격에 의해 매칭되는 특징점을 이용한 공격복잡도를 나타낸다. 추가되는 거짓특징점의 개수가 다르기 때문에 절대적인 비교는 할 수 없으나, 등록된 지문볼트의 공격복잡도(수식 18)는 기존 시스템과 제안한 방법이 비슷하다. 그러나 상관관계 공격에 의한 공격복잡도는 기존 시스템과 제안한 방법이 각각 $1.1 * 10^{1}$과 $4.6 * 10^{8}$이다. 따라서 제안한 방법은 공격복잡도의 저하가 없어 상관관계 공격에 강인하다는 것을 알 수 있다. 제안한 방법에서 수식 23에 의한 등록된 지문볼트의 공격복잡도는 $8^{9}$이 되어 안전성의 저하가 없음을 알 수 있다.

〔표 3〕은 FVC 2002 DB1 Set A를 이용하여 본 논문에서 제안한 지문퍼지볼트 시스템의 성능 실험결과를 보여준다. 기존의 지문퍼지볼트 시스템의 경우 200개의 고정된 거짓특징점을 추가하여 지문볼트를 만드는 반면, 본 논문에서 제안한 시스템은 진짜특징점의 개수에 따라 결정되므로 평균 220.05개의 거짓특징점이 추가되었다. 8차 다항식에 대해서 FAR과 GAR이 각각 0.6%와 91.17%를 보여 GAR이 상당히 향상되었다.

## 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 지문퍼지볼트에 관한 연구가 활발히 진행되고 있다. 그러나 지문퍼지볼트 시스템이 상관관계 공격에 취약하다는 심각한 문제가 있다. 본 논문에서는 거짓특징점을 임의로 추가하지 않고 진짜특징점의 정보를 이용하여 추가함으로써 상관관계 공격에 강인한 지문퍼지볼트 시스템을 제안한다. 본 논문에서는 패스워드 등의 부가적인 정보를 필요로 하지 않고 거짓특징점의 생성 방법만을 변경하였기 때문에 지문을 이용하여 사용자를 인증하는 시스템의 장점을 그대로 유지할 수 있다. FVC2002 DB1 Set A의 지문 이미지를 사용하여 실험한 결과 높은 인식성능을 유지하면서 상관관계 공격에 강인함을 보였다.

## 참고문헌

〔1〕 D. Maltoni, et al., Handbook of Fingerprint Recognition, Springer, Sep. 2003.

〔2〕 A. Jain, R. Bole, and S. Panakanti, "Biometrics: Personal Identification in Networked Society," Kluwer Academic Publishers, Feb. 1999.

〔3〕 R. Bolle, J. Connell, and N. Ratha, "Biometric Perils and Patches," Pattern Recognition, Vol. 35, pp. 2727-2738, 2002.

〔4〕 A. Juels, M. Sudan, "A Fuzzy Vault Scheme," Proc. of IEEE International Symposium on Information Theory, pp. 408-409, May. 2002.

〔5〕 T. Clancy, et al., "Secure Smart-

card-based Fingerprint Authentication," Proc. of ACM SIGMM Multim., Biom. Met. & App., pp. 45-52, Nov. 2003.
〔6〕 U. Uludag, S. Pankanti, A.K. Jain, "Fuzzy Vault for Fingerprints," Proc. of Audio-and Video based Biometric Person Authentication, Vol. 5, pp. 310-319, Jul. 2005.
〔7〕 Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, D. Ahn, "Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault," LNCS 3822 - CISC, Vol. 1, pp. 358-369, 2005.
〔8〕 W. Scheirer and T. Boult, "Cracking fuzzy vaults and biometric encryption," IEEE Biometrics Research Symposium at the National Biometrics Consortium Conference, pp. 1-6, Sep. 2007.
〔9〕 A. Kholmatov, et al, "Secret sharing using biometric traits," Proc. of SPIE in Biometric Technology For Human Identification III, Vol. 6202, Apr. 2006.
〔10〕 A. Kholmatov and B. Yanikoglu, "Realization of correlation attack against the fuzzy vault scheme," Proc. of SPIE, vol. 6819, pp. 68190O - -68190O-7, Mar. 2008.
〔11〕 U. Uludag and A. K. Jain, "Securing fingerprint template: fuzzy vault with helper data," *Proc. of IEEE Workshop on Privacy Research In Vision*, pp. 163-169, Jun. 2006.
〔12〕 K. Nandakumar, A. Nagar, and A. K. Jain, "Hardening fingerprint fuzzy vault using password," Proc. of International Conference on Biometrics, LNCS 4642, pp. 927 - 937, Aug. 2007.
〔13〕 채승훈, 문대성, 문기영, 반성범, "correlation 공격에 대응하는 지문 퍼지볼트 시스템에 대한 연구," 정보통신분야학회 합동학술대회 논문집, pp.93-96, 2009년 11월.
〔14〕 http://bias.csr.unibo.it/fvc2002/databases.asp
〔15〕 문대성, 최우용, 문기영, "다중 다항식을 이용한 지문 퍼지볼트," 한국정보보호학회논문지, 제19권, 제1호, pp.125-133, 2009년 2월.

## 〈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, 지능형비디오감시

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

정 용 화 (Yongwha Chung) 종신회원
1984년 2월: 한양대학교 전자통신공학과 학사
1986년 2월: 한양대학교 전자통신공학과 석사
1997년 2월: 미국 Univ. of Southern California 전기공학과(컴퓨터공학 전공) 박사
1986년~2003년: 한국전자통신연구원 생체인식기술연구팀장
2003년 9월~현재: 고려대학교 컴퓨터정보학과 교수
〈관심분야〉 생체인식, 정보보호, 생체정보보호

김 성 영 (Sung-Young Kim ) 정회원
1994년 2월: 부산대학교 컴퓨터공학과 졸업
1996년 2월: 부산대학교 컴퓨터공학과 공학석사
2003년 8월: 부산대학교 컴퓨터공학과 공학박사
2004년 3월 ~ 현재: 금오공과대학교 컴퓨터공학부 부교수
〈관심분야〉 영상처리, 비디오정보처리, 컴퓨터비젼

김 정 녀 (Jeong Nyeo Kim) 종신회원
1987년 2월: 전남대학교 전산통계학과 졸업
2000년 2월: 충남대학교 컴퓨터공학과 석사
2004년 2월: 충남대학교 컴퓨터공학과 박사
1996년: OSF/RI 공동연구 파견(미국)
2005년: Univ. of California, Irvine Post-Doc.
1988년 ~ 현재: 한국전자통신연구원 휴먼인식기술연구팀장 책임연구원
관심분야: 시스템・네트워크보안, 보안 OS, 바이오정보보호 등