퍼지서명볼트스킴을 이용한 인증 프로토콜
(An Authentication Protocol using Fuzzy Signature Vault Scheme)

문 현 이 † 김 애 영 † 이 상 호 ††
(Hyun-Yi Moon) (Ae-Young Kim) (Sang-Ho Lee)

요 약 본 논문에서는 경량화된 서명의 특징추출기법을 이용하여 사용자의 편의성 및 전자상거래의 효율성을 높일 수 있는 퍼지볼트스킴 기반의 인증 프로토콜을 설계한다. 서명은 간편하고 저렴한 생체정보 중 하나이기 때문에 전자상거래에서 보편적으로 사용되는 인증수단이지만, 전자상거래시 저비용의 안전성을 확보한 프로토콜의 부재라는 취약성을 가진다. 이러한 문제를 해결하기 위하여, 비밀정보를 정확하게 생성해내는 퍼지볼트스킴 및 서명의 특성에 적합한 특징추출기법을 설계하고, 이 특징추출 과정에서 적용된 매개변수들을 활용하여 서명 기반의 효율적인 인증 프로토콜을 설계한다. 본 프로토콜을 적용시의 효과는 1) 간편하고 저렴한 서명의 이용, 2) 서명처리 및 인증에 약 1초의 시간소비로 실시간 사용자 검증 가능, 3) 로그인 및 검증시 통신횟수 1회로 최저, 4) 사용자 인증과 동시에 비밀값 획득 등이다.

키워드 : 생체인식, 서명, 퍼지볼트스킴, 키생성, 전자상거래

Abstract In this paper, we design an authentication protocol based on Fuzzy Signature Vault Scheme using a light signature feature extraction method for user convenience and efficiency of electronic commerce. The signature is used broadly in electronic commerce because it is one of the simple and low-cost biometric items. However, signature has a problem that there are few low-cost and safe protocols. To solve this problem, we design a feature extraction method which is adequate for characters of signature and Fuzzy Vault Scheme. In addition, we design and analyze an efficient authentication protocol with some parameters used in this procedure. The followings are advantages when this protocol is applied to authentication procedure; 1) using convenient and low-cost signatures, 2) being possible to verify users with spending only about 1 second for signature processing and authentication, 3) one time on transmission for sign-in and verification and 4) getting user authentication with secret value at the same time.

Key words : Biometrics, Signature, Fuzzy Vault Scheme, Key generation, E-Commerce

1. 서 론

최근에는 기존의 암호시스템이 가지고 있는 단점을 보완하고 보안성을 강화하기 위하여 생체정보와 암호시스템을 결합한 보안기법들이 소개되고 있다. 본인인증을 위한 생체정보의 사용은 기존에 사용하던 암호와 같이 분실이나 도난의 우려가 없고, 사용자가 본인임을 보장할 수 있으며, 부인방지가 가능하다는 장점을 가진다. 암호시스템과 생체정보의 결합을 이용한 키추출 방식은 크게 두 가지로 나눌 수 있다. 첫 번째 방식은 입력된 생체정보와 데이타베이스에 저장된 생체정보의 정합을 통해 생체정보로부터 직접 키를 추출하는 방식이다. 두 번째 방식은 기존의 암호시스템에서 사용하는 기법으로 생성해놓은 키를 생체정보를 이용하여 숨기거나 유도하는 방식이다. 생체정보는 획득시마다 매번 같은 정보를

· 이 논문은 2007 한국컴퓨터종합학술대회에서 '퍼지서명볼트스킴을 이용한 인증 프로토콜'의 제목으로 발표된 논문을 확장한 것임

† 학생회원 : 이화여자대학교 컴퓨터학과
hyunyi02@ewhain.net
kay@ewhain.net
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
shlee@ewha.ac.kr

논문접수 : 2007년 10월 2일
심사완료 : 2008년 1월 23일

정보과학회논문지: 시스템 및 이론 제35권 제4호(2008.4)

얻기 힘들기 때문에 인식률이 높은 생체정보를 사용할지라도 키의 비트열이 완전히 일치하지 않는다. 그렇기 때문에 동일한 생체정보로부터 얻은 유사한 키의 비트열은 복호화가 불가능하여 기존의 암호시스템에 생체정보로부터 직접 추출한 키를 그대로 적용하는 것은 무리가 있다. 이러한 문제를 해결하기 위하여 Juels와 Sudan은 생체정보기반 암호시스템에 적합한 퍼지볼트스킴을 제안하였다[1].

저렴하고 간편한 생체정보인 서명은 모바일 및 유비쿼터스 컴퓨팅 기반의 상거래, PDA나 노트북과 같은 휴대용 기기 내의 데이타나 프로그램 보호 등에 간단한 보안장치로서 유용하게 사용된다. 그러나 신용카드나 모바일 카드 기반의 결제시스템에서 서명은 카드 소유자가 본인임을 증명하기 위한 필수 단계임에도 불구하고, 이 단계는 실시간 사용자 검증 보다는 추후 문제 발생시 법정에서의 사후 확인용으로 사용되는 소극적인 역할만을 제공한다. 따라서 좀 더 적극적인 카드 소유자의 인증을 위하여 실시간 검증이 가능한 서명단계가 필요하다. 다만 이 서명단계는 저렴하고 단순한 서명의 특성을 고려하여 보안성 강화에 따른 비용의 증가가 크지 않은 서명기반의 인증기법이 적용되어야 한다.

본 논문에서는 서명 기반의 사용자 인증을 위해 간단하고 계산량이 적은 경량화된 서명 특징추출기법을 제안하고, 이 기법을 이용하여 추출된 특징점 기반의 퍼지볼트스킴을 적용한 사용자 인증 프로토콜을 구성한다.

2. 관련연구

기존의 암호시스템은 입력 데이타가 1bit라도 달라지면 정확한 키를 추출해낼 수 없기 때문에 획득시마다 매번 달라지는 생체정보를 입력 데이타로 적용하기 힘들다. 퍼지볼트스킴은 Juels와 Sudan에 의해 제안된 생체정보기반 키 또는 비밀값 추출기법으로, 비밀값 또는 키를 생체정보를 이용하여 숨기는 암호화 단계와 숨겨진 비밀값을 생체정보로 풀어내는 복호화 단계로 구성된다. 이 때, 숨기거나 풀어내는 과정은 '다항식 재구성'의 원리를 기반으로 이루어지며, 퍼지볼트스킴의 안전성은 이 다항식의 재구성에 필요한 계산량에 기반한다[1].

최근 이러한 퍼지볼트스킴을 이용한 생체암호시스템이 많이 제안되고 있다. Uludag 등은 지문의 특징점을 퍼지볼트스킴에 적용하였다[2]. Freire-Santos 등은 서명 입력시간에 따른 좌표값 (x, y)와 서명시의 압력값에 대한 최대값과 최소값을 특징점으로 하여 퍼지볼트스킴에 적용하였다[3]. 그리고 Kholmatov 등은 서명의 교차점, 끝점, 곡선의 극점을 특징점으로 퍼지볼트스킴에 적용한 방식을 제안하였다[4]. 하지만 Freire-Santos 등의 기법은 서명이미지의 정규화, 잡음제거, 명암 평활화 등

그림 1 Kholmatov 등이 제안한 기법에서의 특징점의 예

전처리 단계가 복잡하고 계산량이 많다. 또한, 이 기법들은 서명하는데 걸리는 시간과 압력 등의 저장할 정보가 많기 때문에 계산능력이 낮은 소형 시스템에는 적용하기 힘들다는 단점이 있다. Kholmatov 등의 특징점 추출기법은 그림 1과 같이 교차점과 끝점, 곡선의 극점 등 지문에 사용되는 특징점을 사용하여 간편하게 특징점을 추출할 수 있다는 장점이 있지만, 서명 검증시 전수조사를 하기 때문에 처리시간이 매우 길다는 단점으로 실시간 인증을 하기에 한계가 있다.

본 논문에서는 적은 계산량으로 서명이미지의 특징을 효과적으로 추출·유도해줄 수 있는 경량화된 특징추출기법을 설계한다. 그리고 이 기법을 이용하여 추출한 서명의 특징점들을 퍼지볼트스킴에 적용하고, 이 퍼지서명볼트스킴을 기반으로 전자상거래 시스템에 활발하게 사용될 수 있는 효율적인 사용자 인증 프로토콜을 설계한다.

3. 서명인식

3.1 서명특징추출

본 논문에서 사용한 서명의 특징점은 서명의 끝점, 꺾어지는 점, 이어지는 선, 갈라지는 부분, 획이 교차한 부분, 단점의 6가지 종류이다. 그림 2(a)와 같은 서명이미지를 이용해서 이 특징점들을 추출하는 흐름은 다음과 같다.

단계1 : 가로축 $m+1$, 세로축 $n+1$개의 픽셀로 구성된 서명 이미지를 획득한다.

단계2 : 흑백의 중간 값인 128을 임계값으로 하여 이진화한다.

1. *threshold* = 128
2. $i = 0, j = 0$
3. while $(i = n \ \& \ j = m)$
4. if $p(i, j) > threshold$
5. $p(i, j) = 1$
6. else $p(i, j) = 0$
7. end /* while */

단계3 : 불필요한 픽셀을 제거하기 위해 세선화한다.

단계4 : 세선화된 영상의 좌표값 (1, 1)을 시작점으로

해서 값이 1인 픽셀을 찾는다.

단계5 : 각각의 픽셀은 주변 픽셀을 포함한 3×3의 블록을 기본 단위로 하여 $cn(P)$를 계산한다.

단계6 : 특징점 분류기준과 비교하여 각 패턴별로 발생한 수를 센다.

그림 2는 위 알고리즘을 적용한 예로, (a)은 단계1, (b)는 단계2, (c)는 단계3을 적용한 결과이다. 단계1에서 타블릿을 사용하여 그림 2(a)와 같은 200×200 크기의 서명을 획득한다. 획득된 서명이미지의 자료구조는 그레이색상계열인 0~255사이의 값으로 구성된 200×200 크기의 배열이며 총 40,000개의 픽셀로 구성된다. 이 그레이색상의 중간 값인 128(*threshold*)을 기준으로 하여 각 픽셀의 값이 그보다 작으면 0, 크면 1을 부여하여 서명이미지를 이진화한다. 이러한 단계2의 이진화 과정에 따른 결과는 그림 2(b)와 같다. 이 그림 2(b)는 단계3의 세선화 과정을 이행하면 그림 2(c)와 같이 각 선이나 점이 한 픽셀로만 이루어져 가늘어진 서명이미지를 얻게 된다.

그림 2(c)의 세선화된 이미지에서 서명부분의 픽셀값은 1이며, 그림 3과 같이 검은색을 나타내는 픽셀이다. 따라서 단계4에서는 이 세선화된 이미지의 첫 픽셀부터 마지막 픽셀까지 총 40,000개의 픽셀을 검토하여 그 값이 1인 픽셀을 찾아 서명부분을 가려낸다.

그러면 단계5에서는 이 서명부분인 '1' 픽셀들에 대하여 각 픽셀들과 주변 '1' 픽셀들과의 관계를 차례로 확

(a) (b) (c)

그림 2 입력받은 서명 이미지와 이진화 및 세선화된 서명 이미지(200×200)

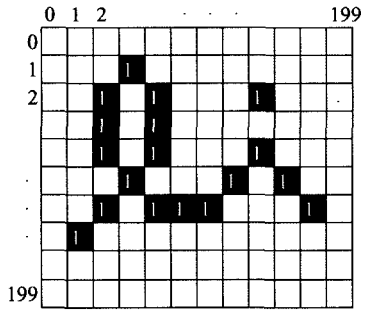

그림 3 세선화된 서명 이미지의 예

P_0	P_1	P_2
P_7	P	P_3
P_6	P_5	P_4

그림 4 각 픽셀의 구성

인하여 각 '1' 픽셀이 나타내는 특징을 6 가지 특징 중의 하나로 분류한다. 각 '1' 픽셀에 대하여 특징점 분류를 위한 기본 단위는 그림 4와 같은 3×3 크기의 블록이며, 중심 픽셀 P와 주변 픽셀을 그림 4와 같이 명명하고, 값이 '1'인 각 픽셀을 이 중심 픽셀 P에 위치시키고 식 (1)을 계산한다.

이 그림 4와 같은 구성은 중심 픽셀 P에 대해 주변 픽셀 $P_0 \sim P_7$에 '1' 픽셀이 어떻게 분포해있는지를 확인하는 기본단위이며, 이 기본 단위에 적용되는 식 (1)은 $P_0 \sim P_7$과 P와의 상관도를 정량적인 수치로 내타낸 수식이다.

$$cn(P) = \frac{1}{2}\sum_{i=1}^{8}|val(P_{i \bmod 8}) - val(P_{i-1})| \qquad (1)$$

식 (1)에서 *val* 함수의 값은 1 또는 0으로 이진화된 각 픽셀의 값을 의미한다. 특징점의 분류는 $cn(P)$의 결과에 따라 나눌 수 있는데 서명의 끝점의 경우 $cn(P)$=1, 꺾어지는 점과 이어지는 선의 경우 $cn(P)$=2, 갈라지는 부분의 경우 $cn(P)$=3, 획이 교차하는 경우 $cn(P)$=4, 단점의 경우 $cn(P)$=0이다. 단, $cn(P)$의 값이 동일한 꺾어지는 점과 이어지는 선의 경우, 별도로 주변 픽셀의 차이 값을 계산하여 이차 분류한다.

이렇게 단계5에서 계산된 특징점별 값을 이용하여 단계6에서 패턴별로 분류된 특징점을 확인한다.

3.2 서명 기반의 퍼지볼트스킴

본 절에서는 위의 서명 특징추출기법을 사용하여 추출한 특징점과 추출과정에서 발생하는 고유한 매개변수 정보를 퍼지볼트스킴에 적용한다. 이 때, 키 또는 비밀값으로 사용할 비트 스트링 S와 다항식 검출을 위한 *CRC*(Cyclic Redundancy Check) 비트가 필요하다. 이 S와 *CRC*는 D차 다항식 P를 구성하기 위한 계수로 사용된다. 구체적인 서명 기반의 퍼지볼트스킴의 암호화 알고리즘은 다음과 같다.

암호화 알고리즘

1. 비밀 값 S를 선택한다.
2. *CRC* 비트를 S에 덧붙인다. ($S \mid CRC$)
3. S와 *CRC*를 덧붙인 값을 다항식 P의 계수 $c_n \ldots c_0$로 쪼개어 P를 구성한다.

$$P(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0$$

4. 패턴별로 분류된 특징점의 개수의 비율을 x_i로 하였을 때, x_i와 다항식에 x_i를 대입한 값 $P(x_i)$와의 순서쌍의 집합인 genuine point들의 집합 G를 만든다.

$$G = \{(x_1, P(x_1)), (x_2, P(x_2)), \ldots, (x_n, P(x_n))\}$$
$$x_i \neq x_k, i \neq k, i = 1, 2, \ldots, n$$

5. 집합 G에 속하지 않는 값들로 구성된 순서쌍의 집합인 chaff point들의 집합 C를 만든다. 이 때, chaff point의 개수는 genuine point의 개수보다 많아야 한다.

$$C = \{(c_1, d_1), (c_2, d_2), \ldots, (c_m, d_m)\}$$
$$d_j \neq P(c_j), j = 1, 2, \ldots, m$$

6. $V = G \cup C$인 볼트셋(vault set)을 생성한다.

$$V = \{(v_1, w_1), (v_2, w_2), \ldots, (v_{n+m}, w_{n+m})\}$$

볼트셋을 전달한 후 볼트셋을 수신한 수신자는 복호화 알고리즘을 이용하여 비밀 값을 찾아낸다. 퍼지볼트스킴의 복호화 알고리즘은 다음과 같다. 복호화 시의 서명은 동일한 사용자의 서명이지만 생체정보의 특성상 암호화시 입력한 서명과는 조금의 차이가 생기므로 구분을 위하여 *을 사용하여 표기한다.

복호화 알고리즘

1. 입력받은 서명이미지 또는 템플릿의 서명이미지를 이용해서 전송되어 온 볼트셋 V를 풀기위한 시도를 한다.
2. 입력받은 서명으로부터 n개의 특징점을 찾는다.

$$x^*_1, x^*_2, \ldots, x^*_n$$

2. 복호화 시 필요한 K개의 후보점들을 찾는다. $K \leq n$이면서 v_j와 같은 x^*_i 값이 나오면 후보점 목록에 추가한다.
3. D차 다항식은 $D+1$개의 점들이 모여야 구할 수 있으므로, K개의 후보점들에 대하여 $D+1$개의 가능한 부분집합을 조합한다. 이 때, $C(K, D+1)$개의 조합이 가능하다.
4. 각 후보 부분집합 내의 순서쌍으로 다항식 $P^*(x)$를 다음과 같이 재구성한다.

$$P^*(x) = c^*_n x^n + c^*_{n-1} x^{n-1} + \ldots + c^*_1 x + c^*_0$$

5. 약정된 크기가 되도록 $c^*_1 | c^*_0$를 형성하여 CRC 값을 확인한다.
6. $c^*_1 | c^*_0$가 CRC와 동일하면 해당 다항식 후보는 찾고자하는 다항식이다. CRC 값의 확인에 사용되었던 계수를 제외한 나머지 계수를 연접하면 비밀값 S를 획득하게 된다.

4. 서명기반 인증프로토콜 설계

퍼지볼트스킴을 이용한 서명기반의 인증프로토콜은 다음과 같이 등록단계, 로그인 단계, 검증단계로 나누어 살펴볼 수 있다.

등록단계

본 단계는 그림 5와 같은 흐름으로 사용자를 클라이언트 시스템에 등록하는 단계이다. 사용자는 일반 ID생성방식에 따라 사용자 ID_i를 결정하고, Diffie-Hellman의 키교환과 같은 보안채널(secure channel)을 통하여 사용자 ID_i를 서버로 전송한다. 그림 5의 ▭→는 안전한 채널, ⟶는 일반채널을 의미한다. 서버는 클라이언트로부터 사용자의 ID_i를 받은 후, 사용자의 CRC_i 값을 결정한다. 이 때, CRC_i 값으로는 임의의 수를 부여한다. CRC_i가 결정이 되면 서비스의 종류 및 요구되는 보안 수위에 따라 적합한 다항식의 차수 D_i 값을 결정하고, 위에서 사용한 서명 특징추출기법으로부터 추출한 특징점들 중 어떤 정보를 사용할지 결정하기 위한 매개변수 F_p를 정한다. 서버에서 정한 CRC_i, D_i, F_p 값은 사용자 ID_i와 마찬가지로 안전한 보안채널을 이용하여 클라이언트로 전송된다. 클라이언트는 전송받은 CRC_i, D_i, F_p 값을 저장하고, 사용자로부터 서명 이미지 S_i를 획득한다. 서명 이미지는 이미 노출되었다고 가정하여 공개된 정보로 취급하므로 특별히 보안채널을 이용할 필요가 없다. 클라이언트는 사용자 ID_i와 획득한 서명 이미지 S_i를 포함하는 msg1을 일반채널을 통해 서버로 전송한다. msg1을 전송받은 서버는 사용자 ID_i와 앞서 결정한 CRC_i, D_i, F_p 값들과 서명 이미지 S_i를 데이타베이스에 저장한다. 이 때, 서버의 데이타베이스는 안전한 데이타베이스 시스템에 위치한 것으로 가정한다.

로그인 단계

본 단계는 그림 6과 같은 흐름으로 해당 사이트의 서비스를 받기 위하여 등록된 ID로 접속하는 단계이다. 로그인을 위하여 클라이언트의 사용자는 서버로 사용자의 ID_i를 포함한 시작 메시지를 보낸다. 서버는 사용자

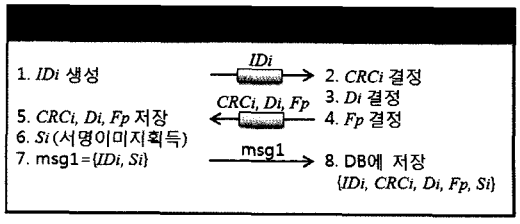

그림 5 제안한 인증프로토콜의 등록단계

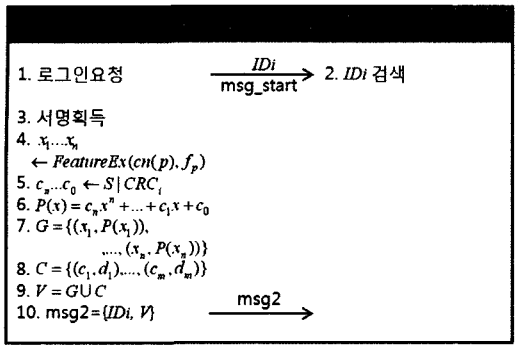

그림 6 제안한 인증프로토콜의 로그인단계

의 ID_i를 검색을 하고 msg2를 받을 준비를 한다. 클라이언트 시스템은 사용자로부터 서명을 획득하고, 사용할 특징점 종류에 대한 정보인 F_p를 이용하여 획득한 서명 이미지로부터 F_p에 해당하는 특징점을 추출한다. 비밀값 S와 CRC_i를 덧붙인 후 이를 계수로 사용한 다항식 $P(x)$을 만든다. 그리고 추출된 특징점을 x_i로 하여 다항식에 x_i를 대입한 값 $P(x_i)$를 계산하여 순서쌍 $(x_i, P(x_i))$를 형성한다. 이 순서쌍들의 집합으로 genuine set G를 만든다. 집합 G와 겹쳐지지 않는 임의 순서쌍인 Chaff point들을 형성하여 chaff set C를 만든다. chaff set C와 genuine set G의 합집합인 vault set V를 만든 후 사용자의 ID_i와 vault set V를 msg2로 하여 서버로 전송한다.

검증단계

본 단계는 그림 7과 같은 흐름으로 서버에서 사용자의 신원을 인증함과 동시에 비밀값을 획득하는 단계이다. 서버는 클라이언트로부터 전송받은 ID_i와 vault set V 그리고 서버의 데이타베이스에 저장된 서명이미지 S_i와 특징점 추출을 위한 매개변수 F_p를 이용하여 특징점 $x^*_1 \ldots x^*_n$를 생성하고, 이 특징점과 유사한 D+1개의 점으로 구성된 모든 가능한 조합을 구한다. 이 조합을 이용하여 찾고자 하는 다항식의 후보인 D차 다항식 $P^*(x)$를 재구성한다. 재구성된 다항식의 계수 중에서 1

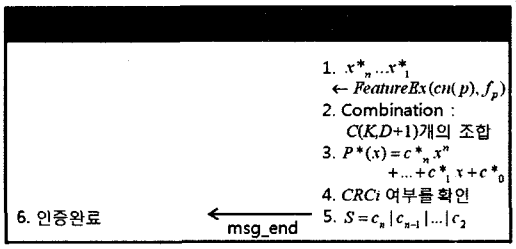

그림 7 제안한 인증프로토콜의 검증단계

차항과 상수항인 $c^*_1 | c^*_0$ 값을 서버에 저장된 CRC_i와 같은 값인지를 비교·확인한다. 비교 결과가 참인 경우 해당 후보 다항식이 찾던 다항식이 된다. 이 최종 다항식을 구성하는 각 계수를 모아 연접시켜 비밀 값 S를 획득하면 인증 및 비밀값 획득이 완료된다.

5. 효율성 및 안전성 분석

5.1 시간분석

제안하는 프로토콜의 실험은 200×200(픽셀)의 서명 이미지를 타블렛으로 직접 입력 받아 수행하였고, Intel Pentium 4 CPU 2.8GHz의 시스템에서 MATLAB을 이용하여 구현하였다. 서명획득시간을 제외한 서명 이미지의 이진화 및 세선화와 특징점추출, 퍼지서명볼트스킴 구성에 걸리는 시간을 측정해본 결과는 표 1과 같다. 표 1의 수행시간은 실험에 실제 사용된 서명들에 대한 각 단계별 시간에 대한 평균값이다.

표 1 제안하는 프로토콜 수행시간(sec)

이진화	세선화	특징점추출	퍼지볼트스킴	전체수행시간
0.25	0.56	0.02	0.23	1.06

5.2 안전성 분석

- 비밀 값 S를 알아내기 위한 전수조사를 통한 공격
  1. CRC_i의 길이를 CRC_LEN이라고 할 때, CRC_i를 알아내기 위한 비교연산의 수행은 2^{CRC_LEN}번이다.
  2. D차 다항식에서 차수 D_i를 알아내기 위한 비교연산의 수행은 D번이다.
  3. F_N개의 패턴 중 n개의 특징점을 선택한 프로토콜일 때, F_p를 알아내기 위한 비교연산의 수행은 $C(F_N, n)$번이다.
  4. 전체 볼트 집합 V의 크기로부터 D+1개의 genuine point들의 값을 알아내기 위한 비교연산의 수행은 $C(V, D+1)$번이다.

전체 경우의 수

$$2^{CRC\_LEN} \times D \times C(F_N, n) \times C(V, D+1)$$

만약, CRC_LEN이 16이고, 차수 D는 8, F_N이 43, n이 20, V의 크기가 200일 때, 전체 경우의 수는 $2^{16} \times 8 \times C(43,20) \times C(200,9)$이고, 이로부터 0.50×10^{18}번의 비교 연산이 필요하다.

- 서명의 특징점이 노출되었을 때

이는 클라이언트의 로그인 단계에서 $FeatureEx$ 함수의 계산을 통해 얻어내는 특징점인 $x_1 \ldots x_n$이 알려질

경우이다. 본 논문에서 프로토콜에 적용할 서명의 특징점은 공개될 수 없도록 보안채널을 통해서 전송하며, 일반적으로 공개되어도 상관없는 서명 이미지는 일반채널로 전송한다. 제안한 프로토콜에서 특징점 추출을 위한 매개변수인 F_p는 안전한 채널 및 보안 알고리즘을 통해 전달되도록 구성되었으며, 이 데이타는 보안 데이타베이스시스템과 같이 안전한 장치에 저장·보관됨을 가정한다. 즉, F_p를 사용하여 서버와 클라이언트에서 직접 특징점을 추출하도록 프로토콜이 구성되었기 때문에 특징점이 노출되는 경우는 F_p가 저장된 데이타베이스 시스템과 서버의 시스템의 보안이 깨졌을 때이므로, 이는 본 가정에 위배된다.

• 서명이 노출되었을 때

서명은 이미 공개된 정보이다. 하지만 서명을 알고 있거나 위조할 경우에도 CRC_i, D_i, F_p 값을 알 수 없으므로, 이 세 값을 알지 못하는 경우에는 위와 같은 전수조사를 통한 공격과 동일한 계산량이 필요하다.

6. 결 론

본 논문에서는 낮은 비용, 적은 계산량, 축소된 단계를 확보하여 효율적인 서명의 특징추출기법을 설계하고 이 기법으로 생성된 특징점을 이용한 퍼지볼트스킴을 기반으로 유비쿼터스 상거래에 적합한 사용자 인증 프로토콜을 설계하였다. 이 인증 프로토콜은 기존의 전자상거래 시스템에서 인증단계 없이 사용하던 서명 시스템에 실시간 인증이 가능하도록 보안성을 확보하였다. 또한 이러한 프로토콜은 전자상거래에서 실시간 사용함에 무리 없음을 실험을 통해 확인하였다. 그리고 이 프로토콜은 인증과 동시에 별도의 처리 없이 비밀값의 공유가 효율적으로 이루어짐을 확인하였다.

향후 이 인증프로토콜을 유비쿼터스 및 모바일 환경에 적합한 시뮬레이터에 구현하여, 유비쿼터스 상거래 시스템과 같은 서비스에서의 사용자 인증을 실험해 볼 필요가 있다. 또한, 다항식의 차수 D의 결정 및 chaff point들의 집합을 구성시 각 서비스별로 필요한 차수와 chaff point의 개수에 대한 고찰이 필요하다.

참 고 문 헌

[1] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," in *Proc.* IEEE International Symposium on Information Theory, pp. 408, 2002.

[2] U. Uludag, S. Pankanti and A. Jain, "Fuzzy Vault for Fingerprints," in *Proc.* AVBPA, LNCS, Vol. 3546, pp. 310-379, 2005.

[3] A. Kholmatov and B. Yanikoglu, "Biometric Crypto-system Using Online Signatures," in *Proc.* ISCIS, LNCS, Vol.4263, pp. 981-990, 2006.

[4] M. Freire-Santos, J. Fierrez-Aguilar and J. Ortega-Garcia, "Cryptographic Key Generation using Handwritten Signature," in *Proc.* SPIE, Vol.6202, pp. 225-231, 2006.

문 현 이

2006년 8월 이화여자대학교 컴퓨터학과 학사. 2006년 9월~현재 이화여자대학교 컴퓨터학과 석사과정. 관심분야는 정보보호, 인증, 생체정보

김 애 영

2000년 2월 한신대학교 정보시스템공학과 학사. 2003년 2월 이화여자대학교 컴퓨터학과 석사. 2003년 3월~현재 이화여자대학교 컴퓨터학과 박사과정. 관심분야는 인증, 개인정보보호, 생체정보, 스마트카드

이 상 호

1979년 서울대학교 계산통계학과 이학사 1981년 한국과학기술원 전산학과 이학석사. 1987년 한국과학기술원 전산학과 공학박사. 1990년 미국 일리노이대학교 전산학과 방문교수. 현 이화여자대학교 컴퓨터학과 교수