다중고유얼굴-볼트 기반의 인증 프로토콜

김애영, 이상호
이화여자대학교 컴퓨터공학과
e-mail:kay@ewhain.net, shlee@ewha.ac.kr

An Authentication Protocol base on MultiEigenface Vault

Ae-Young Kim, Sang-Ho Lee
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

본 논문에서는 다중고유얼굴 기반의 퍼지볼트를 이용하는 인증기법을 제안하였다. 다중고유얼굴을 형성하기 위한 중요정보는 사용자의 스마트카드에 저장하며, 이 정보들은 공유하려는 비밀정보 및 비밀키를 안전하게 보호하기위한 퍼지볼트 스킴에 적용하여 기존의 퍼지볼트 기반의 인증 프로토콜보다 한층 강화된 보안성을 확보하는 방안을 연구였다.

1. 서론

사용자 인증을 위해 적용 가능한 요소는 RSA 및 DES 등의 암호 알고리즘 기반의 암호화기법, 스마트카드 및 보안 USB 메모리 스틱과 같은 보안토큰, 지문 및 얼굴 등을 기반으로 하는 생체인식기법 등이 있다. 각각의 요소들로 사용자 인증 시스템을 구축하여 운영할 수도 있지만, 이들 중 2~3 가지의 요소를 효과적으로 조합한 사용자 인증 시스템은 편리성, 효율성, 안전성을 더욱 강화시킨다. 하나의 예를 들면, 생체정보에서 얻어낸 특징값을 기반으로 암호화기법에서 사용할 비밀키를 생성해내며, 이때 생성된 키는 안전한 장치에 저장 및 관리하는 것이다.

하지만 생체정보를 추출하는 과정 및 방법은 암호화키 값의 획일성을 보장하지 못하는 한계를 가지고 있으며, Biometric Hardening이나 Biometric Keying 기반의 키 생성 기법도 역시 이러한 한계를 극복하지 못했다. 이러한 한계를 해결하기위해 Juels and Sudan, Uludag and Jain 등에 의해 퍼지볼트기반의 키생성 기법이 제안되었다[4].

그러나 퍼지볼트스킴은 공개된 정보인 생체정보를 그대로 노출시켜 사용하므로 보안성을 유지하기가 어렵다. 생체정보는 공개되어있으나 비공개된 정보를 기반으로 하는 특징정보를 퍼지볼트스킴에 참여시킬 필요성이 있다.

따라서 본 논문에서는 다중고유얼굴 기반의 퍼지볼트 스킴을 이용하여 사용자 인증 프로토콜을 설계해본다. 즉, 다중고유얼굴에 반드시 필요한 정보들은 비공개적으로 스마트카드 및 서버의 안전한 데이터베이스에 저장하여 퍼지볼트를 생성할 때 사용하도록 하여 퍼지볼트스킴의 보안성을 확보하고, 동시에 사용자의 인증 및 비밀정보를 공유하는 유용한 프로토콜을 연구해본다.

2. 포즈별 다중고유얼굴 기반의 퍼지볼트

포즈별 다중고유얼굴은 포즈별로 분류되어있는 DB에 대해 다음과 같은 인식 과정을 통해 형성한다.

단계1. 학습영상은 포즈별(조명 없는 무표정, 웃는 표정, 조명 없는 엄한 표정, 오른쪽 조명, 왼쪽 조명)로 나누어 고유얼굴을 계산한다.

단계2. 테스트영상 한 장마다 포즈 종류의 수 * 테스트 영상의 수만큼의 거리를 계산한다.

단계3. 계산된 거리 값 중에서 가장 가까운(거리 값 0에 가까운) 영상을 해당 영상으로 채택한다.

단계4. 채택된 영상이 제대로 채택된 것인지 인식률을 계산한다.

이러한 인식 과정에서 인식 대상의 영상은 다중 고유얼굴과 각각 유사도를 측정하고, 그 측정값들 중에서 가장 유사도가 높은, 즉 가장 적은 거리 값을 갖는 영상과 같은 영상이라고 최종 인식된다. 이는 웃는 얼굴은 웃는 고유얼굴를 기준으로 하여야 최적의 인식률을 갖는다는 생각을 기반으로 한다. 다중고유얼굴기반의 인식은 포즈 종류의 수만큼 생성된 다중고유얼굴을 등록된 얼굴과 정합하여 수행한다. 위의 과정에서 다중고유얼굴의 계산은 단일고유얼굴의 계산과 마찬가지로 (그림1)과 같은 PCA 기반의 알고리즘을 적용하여 구한다.

각각의 포즈별 다중고유얼굴을 기반으로 전체 데이터에 대한 인식률을 확인한 결과는 <표 1>과 같다. 단일 고유얼굴에 비해 포즈별로 고유얼굴을 형성해 다중으로 인식에 참여시킨 결과가 인식률이 높다. 이는 포즈별 고유얼굴이 유효한 기준임을 나타낸다. <표 1>은 각 이미지의 전처리가 적용되지 않은 경우이며, 전처리를 적용하면 더 높은 인식률의 확보가 가능하다. (그림 2)는 이미지의 명함 평활화 전처리를 적용한 결과와의 비교이다.

$$E_i \leftarrow inverse(Wpca_i) * (f - M_i) \qquad (1)$$

고유값은 (그림 1)에서 $Wpca$로 표현되며, 이를 포즈별로 구하여 $Wpca_i$로 나타낸다. 다중고유얼굴 E_i은 식(1)에

의해 사용할 자신의 얼굴이미지 f에 $Wpca_i$을 이용하여 포즈별로 만든다. E_i는 스킴 내부에서 비밀정보 S를 인코딩/디코딩하는데 사용하여 S를 성공적으로 보호한다[3].

■ 파라미터:
a face space F, matrix of difference value $A = \{A_i, i=1 \text{ to } n\}$, average value M, covariance matrix C, a training set size n, eigenface $Wpca$ (weight principle component analysis), a number of components k

■ 사용된 메쏘드:
$avg(I)$ to calculate average of training face set$inverse(A)$ to calculate inverse value$norm(Wpca)$ to normalize$eigs(C, k)$ to calculate k-eigenface components

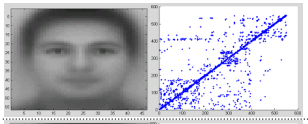
■ 입력값:
a training set $I = \{I_i, i=1 \text{ to } n\}$ ($I_i \in F$)

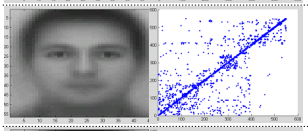
■ 알고리즘: 고유값 및 고유얼굴의 계산

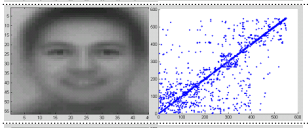
$M \leftarrow avg(I)$;
for i=1 to n do
  $A_i \leftarrow I_i - M$
$C \leftarrow inverse(A)*A$
$Wpca \leftarrow eigs(C, k)$;
$Wpca \leftarrow A * Wpca$
$Wpca \leftarrow norm(Wpca)$;
$E \leftarrow inverse(Wpca) * (f - M)$

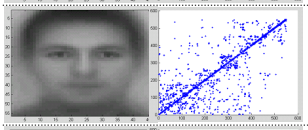
(그림 1) 고유얼굴 구하는 알고리즘

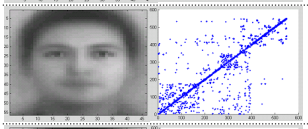
<표 1> 포즈별 인식률

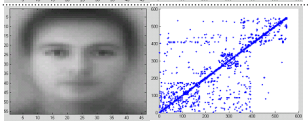

<전체기반 단일고유얼굴>
인식률: 403/550 = 73.27%

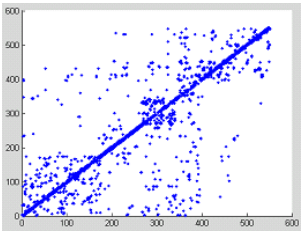

<포즈1기반 단일고유얼굴>
인식률: 403/550 = 70.55%

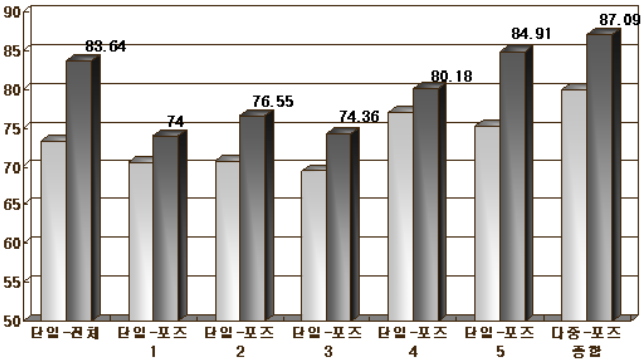

<포즈2기반 단일고유얼굴>
인식률: 403/550 = 70.73%


<포즈3기반 단일고유얼굴>
인식률: 403/550 = 69.46%


<포즈4기반 단일고유얼굴>
인식률: 403/550 = 77.09%


<포즈5기반 단일고유얼굴>
인식률: 403/550 = 75.27%


<다중고유얼굴>
인식률: 440/550 = 80%



(그림 2) 히스토그램 비적용 및 적용 결과

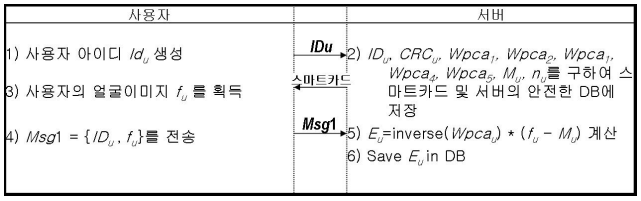
이미 실험을 통하여 얼굴인식에서의 다중 고유얼굴의 유효성을 확인하였기 때문에, 퍼지볼트스킴에서 볼트로 충분히 사용가능하다. 다중 고유얼굴 기반의 퍼지볼트를 생성하기위하여, 포즈별 고유얼굴 E_i, 비밀키나 비밀정보 S, 유효한 다항식을 검출하기위해 사용하는 값 CRC (cyclic reduncancy check value)이 필요하다. 144비트인 비밀정보 S와 16비트인 검출값 CRC는 연접한 후 16비트씩으로 쪼개어 순서대로 8차 다항식의 계수로 여긴다. 그리고 이 다항식과 고유얼굴들 E_i을 이용하여 Genuine set과 Chaffpoint set을 만들고, 이를 섞어 최종적인 볼트를 형성한다. 다중 고유얼굴 기반의 볼트는 공개영역인 인터넷에서 공개되어도 고유얼굴을 만들어낼 수 있는 $Wpca_i$가 없이는 그 안에 숨겨진 비밀정보를 획득할 수가 없다.

이와 같이, 단일 고유얼굴을 이용한 퍼지볼트 스킴과 마찬가지로, 본 논문에서의 다중 고유얼굴을 이용한 퍼지볼트스킴도 Uludag et al.이 제안한 퍼지볼트스킴의 흐름을 따른다[4]. 다중 고유얼굴을 이용한 퍼지볼트스킴은 그 다중성때문에 특정 정보 없이 비밀정보 S를 찾기위한 조합의 경우수를 증가시킴으로 다중고유얼굴 기반의 볼트의 이용은 보안성을 더욱 향상 시킨다.

3. 다중고유얼굴-볼트 기반의 인증 프로토콜

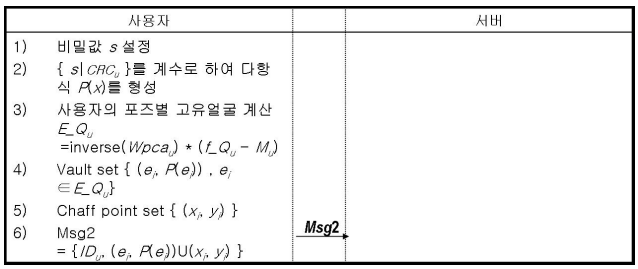
기존의 인증 프로토콜에서 생체인식의 사용은 부인봉쇄 제공으로 강화된 보안 서비스를 확보하고, 외우지 않아도 되는 편리함을 제공한다. 하지만 생체인식은 매회 획득하는 정보의 값이 한 비트라도 달라지는 특성을 가지고 있고, 이를 해결하기위한 방법으로 퍼지볼트스킴이 등장했다. 다항식을 풀어내는 문제에 기반을 둔 퍼지볼트 스킴은 다항식 풀이가 어렵도록 많은 경우의 수를 확보해야하는

데, 이는 생체정보의 특징점에 의존해 해결한다. 그러나 실제 대부분의 생체정보는 공개정보이므로, 있는 그대로의 정보를 이용한 퍼지볼트스킴은 보안성을 유지하기가 어렵다. 생체정보는 공개되어있으나 비공개된 정보를 기반으로 하는 특징정보를 퍼지볼트스킴에 참여시킬 필요성이 있다. 본 논문에서 다중고유얼굴 기반의 퍼지볼트스킴은 포즈별로 고유얼굴E_i를 형성하는 필수 정보인 포즈별 고유값 $Wpca_i$를 비공개정보로 여기고, 이 $Wpca_i$는 스마트카드 및 서버의 안전한 DB에 저장하여 퍼지볼트를 생성할 때 사용하도록 하여 퍼지볼트스킴의 보안성을 확보한다[1, 2].

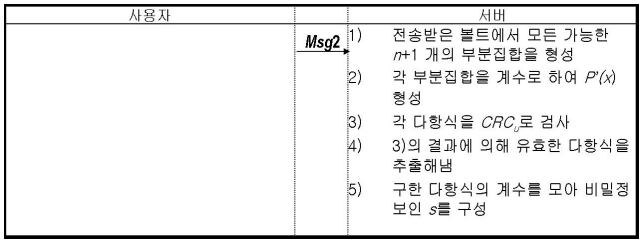


(그림 3) 등록단계: 포즈별 고유값 $Wpca_i$와 스마트카드 발급

다중고유얼굴기반의 볼트를 이용한 인증 프로토콜에서, 이 포즈별 $Wpca_i$를 저장한 스마트카드를 발급받기위한 등록과정은 (그림 3)과 같다. 사용자는 스마트카드를 발급받자마자 공개정보인 자신의 얼굴이미지와 자신의 아이디를 인터넷을 통해 보낸다. 그러면 서버는 얼굴이미지를 그대로 저장하는 것이 아닌 이미 저장해놓은 사용자의 정보를 이용하여 고유얼굴을 생성한 뒤 이 값을 저장한다.



(그림 4) 로그인단계: 포즈별 고유얼굴기반의 로그인



(그림 5) 검증단계: 포즈별 고유얼굴기반의 디코딩

스마트카드를 발급받은 후 사용자 인증을 위한 로그인하는 단계는 (그림 4)와 같다. 스마트카드에 저장된 고유값 $Wpca_i$과 퍼지볼트스킴을 이용하여 비밀정보를 인코딩한 결과로 볼트집합을 형성한다. 기존의 인증 프로토콜과는 달리 본 인증 프로토콜에서 인증을 위한 통신은 적은 메시지를 단 한번만 전송하는 효율성을 갖는다.

전송받은 볼트와 서버에 저장된 사용자의 얼굴 및 고유얼굴을 생성하기 위한 정보들을 이용하여 스마트카드를 소유하고 있는 사용자를 인증하는 단계는 (그림 5)과 같다. 이 검증단계에서도 추가로 요구되는 전송 메시지가 없어 통신량 면에서도 효율적이다.

본 인증 프로토콜은 다음과 같은 이유로 기존의 인증 프로토콜보다 보안성을 더욱 확보하고 있다.

- ■ 다중 고유얼굴을 사용하여 다항식을 찾기위한 부분집합이 생성되는 경우의 수를 높임
- ■ 공개정보인 얼굴을 그대로 이용하는 것이 아니라 고유얼굴을 생성하기 위한 정보를 비공개로 유지함
- ■ 인증과 동시에 별도의 과정없이 비밀정보(비밀키)를 공유하여 계산량 및 취약점을 줄임
- ■ 메시지의 전송 수를 줄여 인터넷상의 취약점 줄임
- ■ 다항식 형성을 위한 정보를 사용자별로 부여하여 형성 가능한 다항식의 경우 수를 높임

5. 결론 및 향후 연구과제

본 논문에서는 얼굴인식에서 유효한 여러 종류의 고유얼굴을 생성하는 기법을 고려하여, 사용자 인증 프로토콜을 구성해보았다. 다중 고유얼굴을 기반으로 인증을 위한 볼트를 생성하기 때문에 얼굴인식 하나로 인한 여러 가지의 생체인식 수행의 불편함을 해소하였으며, 인증 과정에 참여할 여러 가지 고유얼굴로 확보하고 있어 볼트 및 다항식 생성을 위한 경우의 수는 여전히 높게 확보하였다. 이러한 인증기법은 유용한 생체인식 기반의 보안 시스템을 형성할 것이다.

향후 연구과제로는 통계적 • 수학적으로 보안성 및 효율성을 분석, 모바일환경에서의 시뮬레이션을 구현하여 실제적인 보안상의 취약점을 확인 및 분석, 또는 다중 고유얼굴과 다른 생체인식과의 조합은 어떠한 결과를 나타내는지를 연구하는 것이다.

참고문헌

[1] J. Borst, B. Preneel and V. Rijmen, "Cryptography on Smart Cards," Computer Networks, Vol. 36, 2001.
[2] H. Dreifus and J. T. Monk, Smart Cards: A Guide to Building and Managing Smart Card Applications, John Wiley & Sons, 1998.
[3] A. Kim, H. Moon and S. Lee, "Design of Fuzzy Eigenface Vault Scheme for Enhanced Security," In Proc. of APIS, 2007.
[4] U. Uludag and A.K. Jain, "Fuzzy Fingerprint Vault," Proc. Workshop: Biometrics: Challenges Arising from Theory to Practice, 2004.
[5] A. Kim and S. Lee, "Authentication Protocol using Fuzzy Eigenface Vault based on MoC," In Proc. of ICAT, 2007.