퍼지볼트 스킴을 이용한 MoC 기반의 인증 방안 연구

김애영[O] 서승현 이상호
이화여자대학교 컴퓨터학과
kay@ewhain.net, seosh@ewhain.net, shlee@ewha.ac.kr

Study on Authentication Method Based on MoC Using Fuzzy Vault

Ae-Young Kim[O], Seung-Hyun Seo, Sang-Ho Lee
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

중요한 정보의 저장 및 보호하는 기능을 제공하는 스마트카드가 온라인/오프라인에서 대규모 응용에 사용되기 위해서는 강력한 사용자 인증이 요구된다. 이러한 요구는 생체정보의 사용으로 그 효과를 볼 수 있는데, 생체정보의 사용은 사용자 인증을 강력하게 할 뿐만 아니라 외우지 않아도 되는 편리한 비밀키를 제공한다. 동시에 중요한 개인정보인 생체정보 및 처리중의 정보를 스마트카드에 의해서 보호받는 MoC(Match on Card) 방식을 적용받게 된다. 그러나 기존의 MoC방식의 인증 및 키 추출과정에서는 생체정보를 추출하는 과정/방법이 키값의 획일성을 보장하지 못한다는 한계점을 그대로 가지고 있다. 따라서 본 논문에서는 퍼지볼트 스킴을 이용하여 키의 획일성을 확보하면서 생체정보에 대한 보호를 강화시키는 동시에 사용자 인증을 처리하는 방안을 연구하였다.

1. 서 론

온라인 및 오프라인에서의 다양한 서비스를 안전하게 이용하기 위해서는 기밀성과 더불어 사용자 인증이 제공되어야하며, 이를 위해 암호화 기법, 생체정보 인식과 스마트카드를 접목시킨 사용자 인증 기법들이 많이 사용되고 있다.

생체정보는 오프라인을 비롯해 비대면 온라인 거래에서의 사용자 인증을 더욱 강화시켜주며, 동시에 외울 필요 없는 패스워드도 제공해준다. 스마트카드는 뛰어난 저장용량으로 생체정보와 같은 개인의 정보를 비롯한 여러 정보를 스마트카드에 저장한다. 따라서 개인정보에 대하여 중앙 서버에의 관리가 아닌 스마트카드 사용자의 직접적인 관리로 안전성을 더욱 확보한다[1][2].

생체정보 기반의 키를 생성하여 인증이나 암호화에 이용하는 것은 비밀키 값과 관련된 값을 기억할 필요가 없는 편리성과 동일한 키 길이로 더 높은 안전성을 확보한다는 보안성을 장점으로 갖는다. 그러나 개개인의 생체정보인 특징점에서 키를 추출하는 것은 쉽지 않다. 생체인식에서 사용자 인증은 정확히 동일한 값의 비교가 아니라 기준 정보와 입력된 정보 사이의 유사도 측정으로 이뤄지므로, 매번 추출되는 생체정보는 매번 동일한 정보로 추출되기가 어렵다는 사실이 키 생성에 대한 획일성 보장의 어려움이며 부동성의 확보가 요구된다.

이러한 요구사항들을 충족하기 위한 기법으로 스마트카드 내에 등록된 정보로부터 비밀키를 추출하는 기법이 있고, 이 기법은 동시에 등록된 생체정보도 안전하게 보호한다. 하지만 생체정보는 인증을 위해 전송되는 과정에서 노출될 수 있으므로, 주기적으로 패스워드를 변경하듯이 등록된 생체정보도 주기적으로 재등록 해주어야 할 것이다. 생체정보의 재등록은 역시나 비밀키 생성에 대한 획일성 보장의 문제점이 있다.

따라서 본 논문에서는 이러한 단점을 보완하기 위하여 등록된 생체정보와 전송된 생체정보 사이의 유사도 측정만으로도 비밀키의 획일성을 보장할 수 있는 퍼지볼트 스킴을 생체인식 시스템의 위협요소를 최소화하는 스마트카드 기반의 MoC(Match on Card) 방식에 적용시키는 사용자 인증 방안을 연구하고자 한다. 퍼지볼트를 이용한 MoC기반의 인증은 등록된 생체정보에 대한 보안성, 등록정보의 변화에도 상관없는 비밀키의 획일성을 보장, 비밀키의 획득과 동시에 사용자 인증을 만족하는 효율성, 저장된 패스워드를 외울 필요가 없는 편리성 등을 제공하는 효과가 있다.

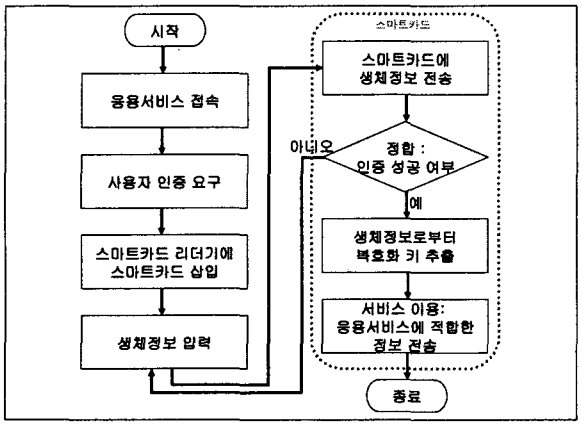
2. 생체정보를 이용한 스마트카드의 사용자 인증

스마트카드는 생체정보의 보안성을 높혀주며, 생체정보는 사용자 개인만의 비밀키를 제공하고 강화된 본인인증을 제공해준다. 생체정보가 스마트카드에 적용되어지는 방법은 생체정보를 온라인상의 데이터베이스 서버 대신에 스마트카드에 저장하고 관리하는 SoC(Save on Card)의 방법, 생제정보의 저장 및 관리뿐만 아니라 정합을 수행하는 기능을 포함한 MoC(Match on Card)의 방법, 그리고 센서가 스마트카드에 직접 장착되어 특징점을 추출하여 저장 및 정합을 수행하는 SSoC(Sensor on Card)의 방법으로 크게 세 종류가 있다.

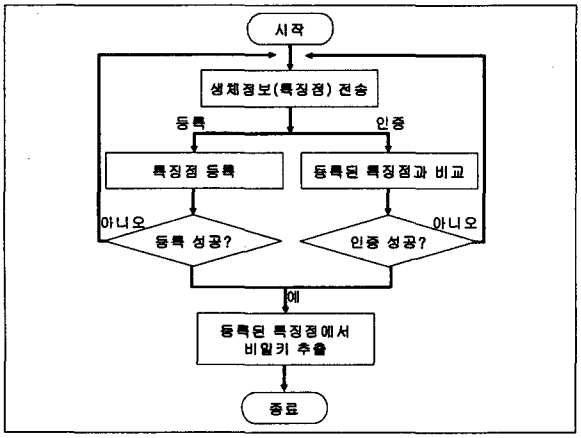
SoC의 방법은 유일성을 지닌 생체정보가 정합을 위한 카드 밖으로의 전송 시에 노출이 문제가 된다. SSoC는 스마트카드에 장착되기 위해 특수한 하드웨어인 고가의 센서가 장착되며, 영상처리와 같은 수행으로 높은 계산

* 이 연구과제는 정보통신 선도기반기술개발사업(국제공동)(IITA 4300-1000-1823호)을 수행 중인 (재)그래픽스연구원의 위탁연구과제로 수행되었음.

량이 요구되는 문제점이 있다. 따라서 스마트카드에 생체정보가 저장도 되어있고 정합도 되어 생체정보가 노출될 가능성이 가장 낮은 MoC방식을 채택한다. 응용 서비스 이용할 때 생체정보를 이용한 인증 과정은 [그림 1]과 같다[3].



[그림 1] 생체정보를 이용한 MoC 기반의 인증 과정



[그림 2] 등록 및 인증시의 생체정보 처리 과정

스마트카드를 처음 사용하는 사용자는 여러 서비스에 사용할 생체정보를 스마트카드에 등록한다. 또는 인증이나 인증서 등의 여러 응용서비스를 사용하는 사용자는 전송된 생체정보와 등록해놓은 생체정보의 비교를 받는다. 이 두 가지 과정 모두의 공통은 등록 및 인증이 성공적으로 이루어졌을 때 등록된 생체정보로부터 비밀키를 추출한다는 것이며, [그림 2]와 같다. 예를 들어 온라인상의 서비스를 이용하려는 사용자는 스마트카드 내에 저장된 인증서를 불러와야할 것이다. 이에 우선적으로 스마트카드의 사용자 확인을 위한 인증과정을 진행할 것이며, 이때 생체정보의 입력이 요구된다. 이후 인증이 성공되면 등록된 생체정보로부터 온라인 서비스를 받기 위한 인증서에 사용될 비밀키를 추출한다.

전송된 특징점에서가 아닌 등록된 특징점에서 비밀키를 추출하는 것은 비밀키 생성의 획일성을 보장 받기 위함인데, 이는 등록된 생체정보가 다른 생체정보로 재등록되기 이전까지만 유효한 사실이다. 전송시의 누출 가능성은 주기적인 재등록을 요구할 것이며, 따라서 이 방법도 비밀키 생성의 획일성 보장에는 한계가 지적된다.

3. 퍼지볼트를 이용한 MoC 기반 인증기법

3.1 퍼지볼트 기반의 비밀키 생성

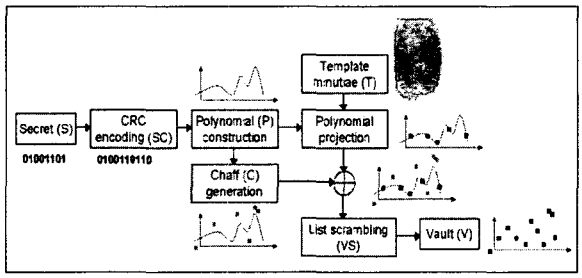
생체정보를 추출하는 과정·방법은 키 값의 획일성을 보장하지 못하는 문제점이 있으며, 비트 하나라도 달라지는 결과를 보이는 Biometric Hardening이나 Biometric Keying기법은 이러한 문제점을 지닌다.

그러나 퍼지볼트 기법은 이 문제점을 해결하고 보다 나은 보안성을 제공하기 위한 방안으로 등록된 생체정보와 유사한 정보를 입력으로 하는 다항식 풀이에 의한 비밀키를 얻는다. 이 기법은 생체정보에서 비밀키를 직접적으로 추출하는 소스가 아니라 비밀키를 보호하는 수단으로 사용한다.

퍼지볼트 알고리즘의 인코딩/디코딩 알고리즘은 다음과 같고 그 흐름은 [그림 3] 및 [그림 4]와 같다[4].

[볼트 인코딩 단계 (lock 단계라고도 함)]

① 128 비트의 비밀키 S를 선택한다.
② 디코딩 단계에서 에러 검사를 위해 사용될 16비트 CRC 코드를 비밀키에 연접한다.
③ ②에서 만든 144비트 키(SC)를 이용해서 8차 다항식을 만든다.
④ Chaff 값들을 임의로 생성하고, 지문의 특징점을 이용해서 genuine 값들을 생성한다.
⑤ ④에서 생성된 집합들을 합하여 원소들을 섞어 최종적 집합 V를 만들며, 이 집합이 볼트가 된다.

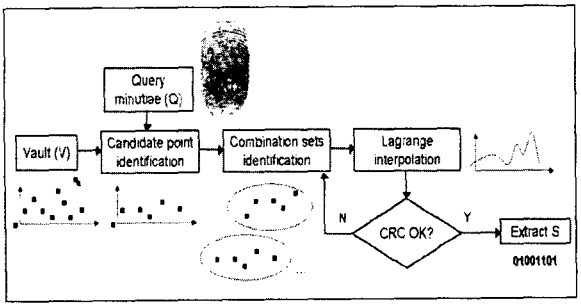


[그림 3] 퍼지볼트의 인코딩 부분

[볼트 디코딩 단계 (unlock 단계라고도 함)]

① 특징점 쿼리로 볼트를 풀기 위한 시도를 한다.
② 디코딩에서 사용될 가능한 모든 점을 찾는다.
③ D차 다항식을 디코딩하기 위해 D+1개의 점들에 대한 가능한 모든 조합을 찾는다.
④ ③에서 찾아낸 모든 조합들과 라그랑제 다항식 방법을 이용해서 D차 다항식을 재구성한다.

⑤ CRC 값을 이용해서 에러 검사가 끝나면, 얻어진 다항식을 이용해서 비밀키 S를 구해낸다.



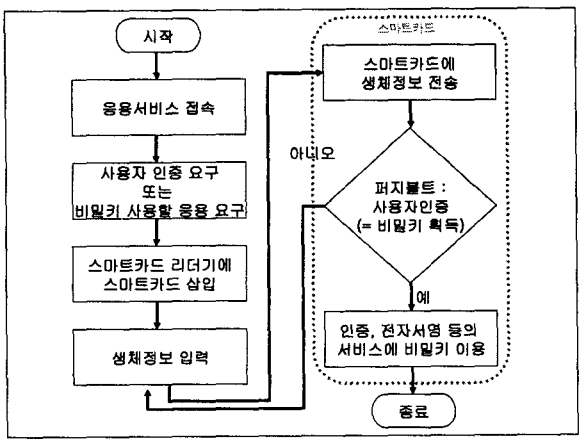
[그림 4] 퍼지볼트의 디코딩 부분

3.2 MoC 기반의 사용자 인증 시스템

본 논문에서 적용하고자 하는 MoC 기반의 사용자 인증 시스템은 [그림 1]과 같은 시스템이다. 센서가 연결 또는 장착된 스마트카드 단말기로부터 특징점으로 구성된 생체정보를 전송받아 인증 및 비밀키 획득을 위한 처리를 수행한다.

3.3 퍼지볼트를 이용한 MoC 기반의 인증 시스템

퍼지볼트는 사용자 본인의 생체정보만이 비밀키를 얻어낼 수 있는 문을 열기 때문에, 전송받은 생체정보를 퍼지볼트 기법에 의한 과정에 통과시켰을 때, 비밀키를 얻어낸다는 것은 동시에 사용자의 본인 확인도 되었다는 것을 의미한다. 이러한 특성을 이용하여 본 논문에서 구성한 사용자의 인증 과정은 퍼지볼트 기법을 이용한 MoC 기반의 인증 기법이며, [그림 5]와 같다.



[그림 5] 퍼지볼트를 이용한 MoC 기반의 인증 과정

[그림 5]와 같이 퍼지볼트를 이용하는 경우 퍼지볼트 연산에 사용될 생체정보는 센서로부터 직접 입력받아 전송받은 생체정보나 등록된 생체정보, 또는 필요에 의해 주기적으로 등록된 생체정보여도 비밀키에는 영향을 미치지 않고 항상 일정한 비밀키를 제공한다.

이 퍼지볼트 연산 부분은 보호하려는 중요한 정보나 사용하려는 비밀키의 등록에 대해서는 [그림 3]과 같은 흐름으로 진행되며, 인증과 동시에 비밀키의 획득이나 중요한 정보의 획득을 위해서는 [그림 4]와 같은 흐름으로 진행된다.

퍼지볼트 기법은 생체정보에서 직접 비밀키를 추출하는 것이 아니라 볼트로 포장된 비밀키로 접근하기 때문에, 비밀키의 획일성을 보장하지 못하는 문제를 해결함과 동시에 비밀키를 보호한다. MoC 방식은 사용자 인증하는 과정 및 비밀키의 획득을 얻어내는 과정에서 비정상적인 경로에 의해 발생 가능한 생체정보의 노출을 방지해준다. 따라서 퍼지볼트 기법을 이용한 MoC기반의 인증 과정은 사용자 인증을 강화시키면서 동시에 사용자에게 높은 편리성과 보안성을 제공하는데 효과적이다.

4. 결론 및 향후 연구과제

본 논문에서는 생체정보에 대해 스마트카드 상의 연산처리를 하는 MoC방식과 생체정보를 통해 키에 접근하는 퍼지볼트 기법을 기반으로 사용자 인증 및 키를 생성하는 기법을 설계하였다.

이 기법은 정당한 사용자만이 자신의 생체정보를 이용해 저장되어 있는 비밀키를 획득할 수 있기 때문에 키를 얻음과 동시에 사용자 인증이 진행된다. 따라서 생체정보로부터의 비밀키 획일성 확보뿐만 아니라, 인증을 거친 후 생체정보로부터 비밀키를 추출하는 연산이 별도로 필요하지 않아 전체적인 연산에 대한 효율성도 확보된다. 따라서 제안한 인증기법은 유용하고 강화된 생체인식 기반 보안 시스템을 설계하는데 유용하게 사용될 것으로 기대된다.

향후 연구과제로는 제안한 기법을 구현하고, 실제의 효율성과 안전성을 분석하여 개선하는 것이다.

참고문헌

[1] Y. Chang, W. Zhang and T. Chen, "Biometric-based cryptographic key generation," IEEE Conference on Multimedia and Expo 2004, Taipei , Taiwan , June 2004.

[2] J. Adams, Survey: Biometrics and Smart Cards, BTT, pp. 8-11, Aug. 2000.

[3] 지형근, 반성범, "생체정보를 이용한 인증서 발급 및 인증방법", 대한민국특허청 공개특허공보, 2005

[4] Uludag, Pankanti and Jain, "Fuzzy Vault for Fingerprints", 2005

[5] A. K. Jain, R. Bolle, and S. Pankanti, "Biometrics-Personal Identification in Networked Society," Kluwer Academic Publishers, 1999.