Fuzzy Extractor를 이용한 무아레 생체인증 개선 방안

백승진*, 안예찬*, 강혁**, 전유부***, 이근호*
*백석대학교 정보통신학부
**워싱턴 대학교 컴퓨터학과
***순천향대학교 컴퓨터소프트웨어공학과
E-mail: doong9078@naver.com, yechan821@bu.ac.kr,
kanghyeok74@gmail.com, jeonyb@sch.ac.kr, root1004@bu.ac.kr,

Improvement of Moire Biometrics using Fuzzy Extractor

Seung Jin Beak*, Ye-Chan Ahn*, Hyok Kang**, You-Boo Jeon***, Keun-Ho Lee*
*Division of Information Communication, BaekSeok University
**Department of computer science, University of Washington
***Computer Software Engineering, SoonChunHyang University

요 약

최근 생체인식 서비스가 지속적으로 보급되고 있으나 그에 대한 보안의 문제에 대해서는 개선되고 있지 않는 상황이다. 본 논문에서는 생체인식 보안에 대해서 개선방안을 제안하고자 한다. 무아레 생체 인증의 보안성을 개선하기 위하여 퍼지 추출기를 이용해 무아레 생체 인증의 보안성을 효율적으로 개선하고, 기존에 있던 무아레 생체 인증 보안성과 퍼지 추출기를 이용한 무아레 생체 인증의 보안을 비교하는 방향을 제시한다.

1. 서론

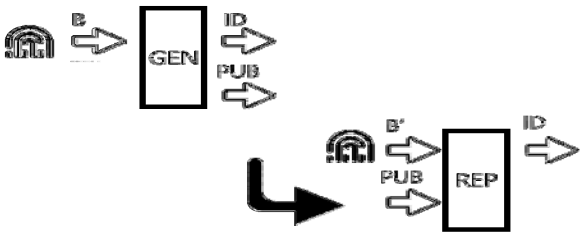
최근 생체인식 기반 프로토콜이 발전하면서 지문, 홍채 인증으로 보안을 해제하는 시대가 왔으나 지문인식의 경우 생체인식 서비스 중 가장 쉽게 접할 수 있는 서비스이다. 쉽게 접할 수 있는 만큼 편의성 부분에서도 높은 유연성을 보이며, 본인이 아닌 경우 열기가 힘든 장점이 있다. 하지만 누군가 생체정보에 대한 자료가 있다면 누구나 인증해서 악용할 수가 있다. 이러한 부분을 개선하고자 무아레 방식을 이용하여 악용하는 문제점을 보안할 수 있으나 무아레 인증 방식만으로는 완벽한 생체 인증 및 보호를 할 수 없으므로 퍼지 추출기법을 이용해 생체정보 인증에 대한 취약한 부분에 대해 개선하고, 또한 생체정보에 인증하는 부분에 있어서 암호화시켜 서버에 보관하고 사용자의 생체정보를 관리하게 되면 인증하는 과정에서 높은 정확성을 띄우게 된다. 따라서 기존의 생체인증 정보 인증 방안보다 높은 정확성을 띄울 수 있는 개선방안을 제안하고자 한다.

2. 관련연구

2-1. 무아레

무아레는 최소 두개 이상의 패턴이 겹쳐서 생기는 현상으로 간섭무늬를 표현하는 단어로도 사용된다. 또한 무아레 현상은 크게 두 가지로 나누어서 볼 수 있다[1]. 물결무늬형태와 주사선 형태로 나눌 수 있으며, 물결무늬 무아레는 사진을 찍거나 이미지센서에 의해 해상도가 넘어가는 경우 발생한다. 주사선형태의 경우 LED 전광판의 색상 표현방법으로 인해 발생한다.

2-2. Fuzzy Extraction

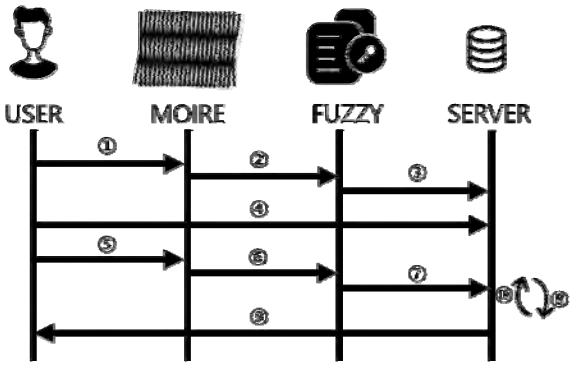


(그림 1) 퍼지 추출기법

퍼지(Fuzzy)는 개념이 적용되어 있지 않거나 적용되지 않은 불문명한 상태나, 표현하기에 있어 애매한 상태를 결과 값으로 근삿값으로 구분지어 놓는 논리이다, 값을 표현하고자 할 때 참 혹은 거짓으로 표현하는 이진논리의 형태를 벗어나서 수학적으로 표현하는 개념이고, 퍼지 추출기법(Fuzzy Extraction)은 Fuzzy에서 인간의 사고방식이나 판단의 애매함을 수학적 사실로 증명하는 방식을 말한다. 또한 이 방식을 추출기법에 적용하여 사용할 경우 생

체정보를 랜덤 스트링으로 바꿀 수 있다. 이 특징을 이용하여 변형된 내용을 이용하여 생체정보를 암호학적 기법에 사용할 수 있다. 이 방식은 Gen과 Rep이라는 효율적인 생성자로 구성되어 있으며, 처음 입력한 생체정보와 논리적으로 입력 값에 의해서 항상 같은 R을 생성해주기 위해 P를 사용하고, 생체정보의 유동적인 특성으로 인해 변형되어도 발생하는 에러에 대해 어느 정도 내성을 가지고 있다고 할 수 있다[2,3]. 퍼지 추출기법을 이용한 인증 스킴은 절차에 따라서 R 과 P를 생성하고 인증하는 과정에서 P를 이용하여 정상적인 R을 도출해내므로, 건강이나 환경에 의해 조금씩 차이가 나는 생체정보도 정상적으로 인증을 할 수 있게 된다[4].

3. 개선방안



(그림 2) 퍼지 추출기를 퍼지 추출기를 이용한 무아레 생체인증 개선 방안

현재 상용화 되어 있는 생체인식기반을 보면, 생체정보가 가지는 그 자체만으로도 높은 보안성과 정확성을 지니지만, 생체정보는 제 3자에게 유출 당하면 비밀번호처럼 바꾸지 못하기 때문에 매우 위협적이다. 여기서 추가적으로 보안기술을 접목하여 한층 더 높은 생체인식 보안 기술을 이용한다는 것이다. 만약 생체정보가 유출 당했을 경우 새로운 퍼지 추출기를 이용한 인증 정보를 생성하는 장점이 있다. 현재 활성화가 잘 되어있는 생체인식들의 단점을 살펴보면 이렇다. 지문의 경우 훼손 및 복제가 가능하고, 홍채 인식의 경우 절차가 복잡하며, 사용이 불편하고, 인식기 비용 고가, 대용량 특징 백터(256Byte)방식 이라는 단점들이 있다. 하지만 생체인식 특성상 변형될 수 있는 상황에 대해서 인식률이 낮아 질수 있지만 추가적인 퍼지 추출기법을 더하게 되면 안전하면서 활용성이 높은 생체인식 기법이 된다. (그림 1) 의 그림을 보면서 설명을 하자면 ①~③은 등록을 하는 과정을 나타낸 것 이고, ④~⑨은 인증과정을 나타낸 것 이다.

① 유저는 무아레 인증을 하기 전 등록되어 있는 정보가 없으므로 생체정보를 등록한다.
② 등록되어 있는 정보가 없으므로 Fuzzy에 생체정보를 전송한다.
③ Fuzzy는 생체정보를 암호화시켜 Server에 저장하고 인증한다.
④ 사용자는 서비스 이용을 위해 인증을 요청한다.
⑤ 사용자는 무아레 인증을 한다.
⑥ 무아레는 입력된 정보를 생체정보로 변형시킨다.
⑦ Fuzzy에서 변환하여 변환된 값을 Server로 전송한다.
⑧ Server에 등록되어 있던 정보와 인증을 요청한 사용자의 생체정보를 비교한다.
⑨ 인증을 요청한 값과 입력된 값이 일치하면 사용자를 인증한다.
⑩ 만약 입력된 값과 인증을 요청한 값이 다르면 다시 확인을 하여 처리한다.

4. 개선방안 분석

생성자 G와 R은 Generate와 Reproduce를 의미하고, B는 Biometrics이라고 할 때, 공식 Gen(B)) = (R, P)를 이용하여 생체정보 B를 정규화 된 랜덤 스트링인 R과 헬퍼 스트링 P를 생성한다. R = Rep(B', P)공식을 통해 같은 사용자가 다른 B'를 입력해도 P를 이용해서 정상적인 R 을 생성해낼 수 있게 된다[2]. 이점을 통해서 생체정보의 유동적인 특성으로 인해 변형되어도 발생하는 에러에 대해 어느 정도 내성을 가지고 있고 높은 정확성으로 인해 인증하는 과정에서도 문제가 없게 되므로 보다 실용적이면서 활용분야가 다양해질 것이다.

5. 결론

현재 생체인식 서비스를 보면 그중에서도 지문 및 홍채인식에 대한 서비스만 늘어나고 있으며, 본인만이 가지는 서비스도 암호화되어 보관이 되어야 하고 생체인증의 장점을 활용하고 체계적인 인증 스킴 알고리즘이 개발되어 생체인식 서비스의 정확성 향상에 대한 개선방안을 제안하였다. 퍼지 추출기를 이용한 무아레 인증 기법은 아직 많은 연구가 되지 않았다. 하지만 퍼지 추출기법에서도 좀 더 정확한 자료를 분석하고 비교하기위한 알고리즘 개발이 필요하며, 추후 국가적인 차원에서 후속 연구가 필요하다.

감사의 글

2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 NRF-2016R1D1A3B03935976).

참고문헌

[1] Weon-Jae Ryu, Young-June Kang, “Shape Measurement Method by using Moire Phenomenon”, Journal of the Korean Society for Precision Engineering, Vol. 22, No. 4, pp. 7-12, 2005.
[2] Younsung Cho, Dongho Won, Security Enhanced User Authentication Scheme with Key Agreement

based on Fuzzy Extraction Technology, Vol. 17, No. 3, pp 1-10, 2016.

[3] Young-Do Joo, Young-Han An, Improvements of a Dynamic ID-Based Remote User Authentication Scheme, Vol.9, No.1, pp. 303-310

[4] Hyeok Kang, Byung-Rae Lee, Tae-Yun Kim, Data Encryption Using the Moire Pattern, Vol. 28, No. 2, pp 670-672, 2001