Journal of the Korea Convergence Society
Vol. 8. No. 2, pp. 9-14, 2017
https://doi.org/10.15207/JKCS.2017.8.2.009

보안레벨 조절이 가능한 바이오메트릭 인증 기법

윤성현
백석대학교 정보통신학부

The Biometric Authentication Scheme Capable of Multilevel Security Control

Sunghyun Yun
Division of Information and Communication Engineering, Baekseok University

요 약 지문은 사람마다 고유하며 디지털 데이터로 표현할 수 있는 생체 정보이다. 지문은 사람 몸의 일부이기 때문에, 지문인식은 패스워드나 신분증을 이용한 방법보다 사용하기 편리하다. 더불어, 최근 보급되고 있는 스마트폰은 카메라 및 지문인식 센서가 내장되어 있어서, 바이오메트릭 인증에 대한 사용자의 수요가 증가하고 있다. 하지만 지문은 쉽게 복제가 가능하고 한 번 도용되면 해당 지문을 다시 사용할 수 없는 단점이 있다. 따라서, 바이오메트릭 데이터는 원본을 변형하여 등록 및 인증해야 한다. 기존의 패스코드 입력 방식은 지문인식 센서 외에 별도의 입력 모듈이 필요하기 때문에 경제성과 사용성이 떨어진다. 본 논문에서는 사용성과 경제성을 고려한 취소 가능한 바이오메트릭 인증 기법을 제안한다. 제안한 인증 기법은 취소 가능한 바이오메트릭 템플릿 생성, 바이오메트릭 템플릿 등록 그리고 사용자 인증 프로토콜로 구성되며, 사용된 지문 개수와 스캔 타임에 따라서 보안레벨을 조절할 수 있다. 더불어, 제안한 방법이 전사적 공격과 능동적 공격으로부터 안전함을 분석하였다.

• **주제어** : 지문인식, 취소 가능한 바이오메트릭 인증, 프라이버시, 다단계 보안, 보안 제어

Abstract A fingerprint is unique to each person and can be represented as a digital form. As the fingerprint is the part of human body, fingerprint recognition is much more easy to use and secure rather than using password or resident card for user authentication. In addition, as the newly released smart phones have built-in camera and fingerprint sensors, the demand for biometric authentication is increasing rapidly. But, the drawback is that the fingerprint can be counterfeited easily and if it's exposed to the hacker, it cannot be reused. Thus, the original fingerprint template should be transformed for registration and authentication purposes. Existing transformation functions use passcode to transform the original template to the cancelable form. Additional module is needed to input the passcode, so it requires more cost and lowers the usability. In this paper, we propose biometric authentication scheme that is economic and easy to use. The proposed scheme is consisted of cancelable biometric template creation, registration and user authentication protocols, and can control several security levels by configuring the number of fingerprints and scan times. We also analyzed that our scheme is secure against the brute-force attack and the active attacks.

• Key Words : Fingerprint Recognition, Cancelable Biometric Authentication, Privacy, Multilevel Security, Security Control

*Corresponding Author : 윤성현(shcrpt@gmail.com)
Received January 6, 2017 Revised February 9, 2017
Accepted February 20, 2017 Published February 28, 2017

1. 서론

최근 IoT, Fintech 기술의 보급으로 스마트폰을 활용한 다양한 서비스가 제공되면서, 이로 인한 보안 위협 또한 증가하고 있다. 특히 IoT와 같은 사물 간 통신은 헬스케어, 스마트 자동차 등과 같이 사회적 시스템에 직접 적용되기 때문에 보안 사고로 인한 인적, 물리적 피해가 발생할 수 있는 위험성이 매우 높다. 보안 위협을 최소화하기 위해서는 스마트 기기와 이를 이용하는 사용자에 대한 인증이 매우 중요하다 [1,2].

스마트폰은 전화기능 뿐만 아니라 여러 가지 다양한 프로그램을 실행할 수 있는 모바일 기기이다. 스마트폰은 금융, 레저, 스포츠 등과 같이 사회적 서비스에 필요한 많은 프로그램을 장소의 제약 없이 사용할 수 있게 한다. 특히, 인터넷 상거래 및 공공 서비스와 같이 사용자의 행위에 대한 법적 구속력이 요구되는 곳에서도 스마트폰을 이용하여 공인 인증서 기반의 서비스를 수행할 수 있다 [3].

공인 인증서는 매 번 사용할 때 마다 패스워드를 입력해야하는데, 현실적으로 안전하면서 기억하기 쉬운 패스워드를 만드는 것은 매우 어렵다. 패스워드의 안전성을 높이면 패스워드를 기억하기가 어렵고, 기억하기 쉬운 패스워드를 사용하면 해커에게 쉽게 노출된다 [4].

바이오메트릭 데이터는 지문, 홍채와 같이 디지털 데이터로 수치화할 수 있는 고유한 생체 데이터를 의미한다. 지문은 사람 몸의 일부로 항상 가지고 다니기 때문에 이를 이용한 인증 기법은 패스워드 기반의 인증 기법과 비교하여 해킹 위험이 적고 사용 편의성이 높다 [5]. 아이폰을 비롯한 최근에 출시되고 있는 스마트폰은 자체적으로 지문인식 센서를 내장하고 있으며, 지문인증을 위한 별도의 API를 앱 개발자들에게 제공하고 있다 [6].

지문은 사람마다 고유하고 그 개수가 제한적이기 때문에, 지문이 위조되거나 노출되면 그 지문을 다시 등록할 수 없게 된다. 따라서, 사용자는 반드시 지문 원본을 변형하여 등록해야한다 [7].

일반적으로 지문 원본을 변형하는 함수들은 패스코드를 입력받아서 원본 템플릿을 변형한다 [8,9,10]. 패스코드는 사용자만 알고 있어야하고 키보드 또는 키패드로 입력하기 때문에 사용 편의성이 떨어지고 비용이 발생하게 된다.

지문위조는 사용자 지문과 똑 같은 모양의 지문을 복제하는 것이다. 주로 실리콘 또는 젤라틴을 이용하는데, 위조지문을 이용한 사용자 인증 성공률이 매우 높은 편이다. 위조지문 공격에 대응하기 위해서는 지문을 누르는 압력 또는 온도와 같이 사용자 특성을 반영하는 부가정보를 측정할 수 있도록 센서에 반영되어야한다. 이는 지문인식 센서의 단가를 높이기 때문에 경제성이 떨어진다 [11].

최근 바이오메트릭 센서가 내장된 스마트폰의 보급으로, 바이오메트릭 인증은 기존의 패스워드 기반의 인증 시스템을 대체할 수 있는 대중화된 인증 수단으로 자리잡을 전망이다. 최근의 바이오메트릭 인증과 관련된 연구는, 웨어러블 환경, 그리드 보안을 위한 접목과 같이 원천 기술보다는 응용 기술에 초점을 두고 있다 [12,13].

본 논문에서는 사용성과 경제성에 초점을 둔 취소 가능한 지문인증 기법을 제안한다. 제안한 방법은 취소 가능한 지문 템플릿 생성 및 등록 그리고 바이오메트릭 인증 프로토콜로 구성된다. 기존 연구는 원본 변형을 위하여 패스코드를 이용하기 때문에 사용하기 불편하고 패스코드 자체의 안전성에 의존해야한다. 본 연구에서는 패스코드 대신에 사용자가 지문 센서를 누른 시간을 초 단위로 인식하여 생성한 스캔 타임을 이용한다. 패스코드 입력을 위한 별도의 하드웨어 및 소프트웨어 모듈이 필요하지 않아서 경제적이다. 더불어, 사용자의 지문을 여러 개 등록할 수 있기 때문에, 해커가 추론해야할 경우의 수를 늘려서 전사적 공격에 안전하다. 또한, 제안한 방법은 지문 개수에 따라서 사용자 인증 레벨을 조정할 수 있기 때문에, 다양한 사회적 서비스에 응용될 수 있다.

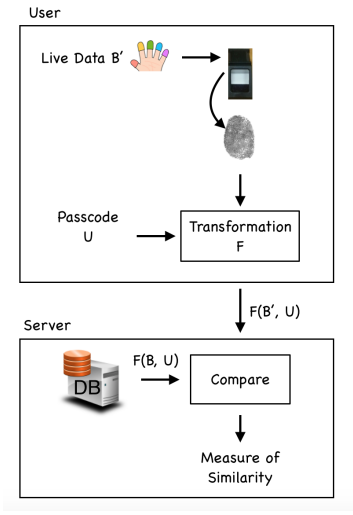
2장에서는 취소 가능한 바이오메트릭 인증 방법과 지문위조 기술에 대한 관련 연구를 알아본다. 3장에서는 제안한 바이오메트릭 인증 방법을 설명하고, 4장에서 안전성 분석을 한다. 5장에서는 결론을 제시한다.

2. 관련 연구

2.1 취소 가능한 바이오메트릭 인증

바이오메트릭 데이터는 사람마다 고유하고 그 개수가 제한되어 있기 때문에, 도용되면 재사용할 수 없다. 따라서, 원본 지문 템플릿을 데이터베이스에 직접 저장하면 안 되고, 원본 템플릿을 변형하거나 또는 암호화하여 데이터베이스에 저장해야한다 [14].

암호화 방법의 단점은 암호화된 템플릿을 복호화하는 과정에서 서버가 사용자의 원본 템플릿을 알게 되어 사용자 프라이버시를 침해할 수 있다는 것이다.



[Fig. 1] Cancelable Biometric Recognition Process

그림 1은 취소 가능한 바이오메트릭 템플릿 생성 단계를 보여준다.

단계 1: 사용자는 자신의 지문을 캡춰하여 이미지 질을 높이기 위한 이미지 처리를 한다.

단계 2: 사용자는 단계 1의 지문이미지로부터 특징점을 추출하여 템플릿을 생성한다.

단계 3: F 함수는 패스코드 U를 이용하여 원본 템플릿을 변형한다.

바이오메트릭 인증은 퍼지 기법을 이용하여, 입력된 데이터와 등록된 데이터의 유사성을 판정한다 [15]. 서버는 데이터베이스에 등록된 템플릿 F(B, U)와 사용자가 보낸 F(B', U)를 비교한다. 서버는 이 값과 미리 설정한 임계값(threshold value)을 비교하여 사용자 인증을 수행한다.

그림 1에서 사용자는 변형된 템플릿을 서버로 전송하기 때문에, 서버는 원본 템플릿을 알 수 없다. 따라서, 데이터베이스에 등록된 지문 템플릿이 노출되어도, 사용자는 패스코드를 변경하여 원본 지문을 재등록할 수 있다.

2.2 지문위조 공격

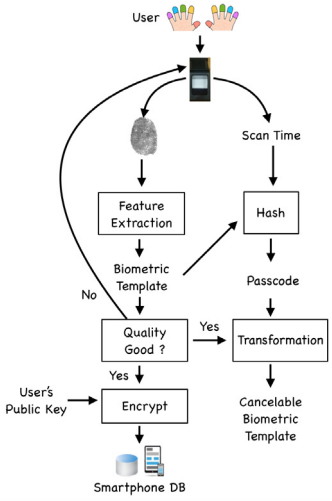
지문은 실리콘 또는 젤라틴과 같은 물질로 쉽게 위조할 수 있다. 유리나 플라스틱에 남겨진 잔여 흔적만으로도 지문 위조가 가능하며 그 인식률 또한 매우 높은 편이다 [16].

이에 대응하려면 지문의 온도, 지문을 누른 압력과 같이 사용자 특성을 반영하는 지표를 추가 인증해야한다. 온도를 이용한 방법은 입력된 지문의 온도를 측정하여 이 값이 생체 온도로 설정한 일정 범위 내에 포함되는지 여부를 판별하는 것이다. 빛을 이용한 방법은 피부에 빛을 투과시켜서 나타나는 광감쇠 현상을 측정하여 사용자의 특성을 판별하는 방법이다 [17]. 이러한 지문인식 기법은 주변 환경에 민감하여 오차율이 높다. 또한, 위조지문의 온도를 생체 온도로 유지 시키면 위조지문과 생체 지문을 식별하지 못하게 된다.

3. 제안한 기법

제안한 바이오메트릭 인증 기법은 취소 가능한 바이오메트릭 템플릿 생성, 템플릿 등록 그리고 사용자 인증 프로토콜로 구성된다.

3.1 취소 가능한 바이오메트릭 템플릿 생성



[Fig. 2] Cancelable Biometric Template Generation

그림 2는 취소 가능한 바이오메트릭 템플릿을 생성하는 단계이다.

단계 1: 사용자는 열 개의 지문 중에서 등록에 사용할 지문 한 가지를 선택한다.

단계 2: 사용자는 지문인식 센서에 사용자 지문을 스캔하고 누른 시간을 측정한다. 지문인식 센서

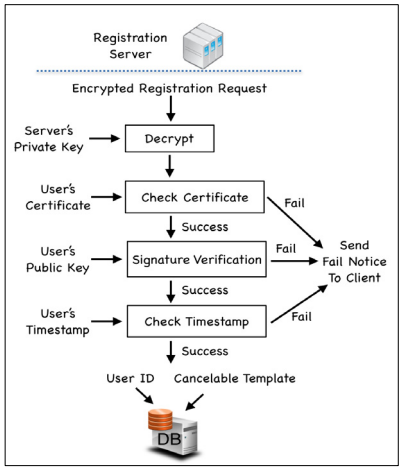
는 1초마다 진동 또는 비프 음을 발생하도록 프로그램 한다.

단계 3: 사용자는 캡춰된 지문이미지로부터 특징점을 추출하여 바이오메트릭 템플릿을 생성한다. 이미지 품질이 좋으면 단계 4로 이동한다. 그렇지 않으면 단계 1로 이동한다.

단계 4: 사용자는 스캔 타임과 바이오메트릭 템플릿을 함께 해쉬하여 패스코드를 생성한다.

단계 5: 사용자는 패스코드를 이용하여 자신의 템플릿을 변형한다.

3.2 바이오메트릭 템플릿 등록



[Fig. 3] Biometric Template Registration Process

그림 3은 바이오메트릭 템플릿을 등록하는 단계이다.

단계 1: 사용자는 사용자 ID, 인증서, 타임스탬프, 바이오메트릭 템플릿을 패키징한다.

단계 2: 사용자는 자신의 개인키로 단계 1에서 만들어진 메시지를 서명한다.

단계 3: 사용자는 서버의 공개키로 단계 2의 서명과 메시지를 암호화 한다.

단계 4: 사용자는 단계 3에서 암호화된 메시지를 서버로 전송한다.

단계 5: 서버는 자신의 개인키로 암호화된 메시지를 복원한다.

단계 6: 서버는 복원된 메시지에 포함된 사용자 PKI 인증서를 검증한다. 서버는 인증서 검증에 성공하면 단계 7로 이동하고, 그렇지 않으면 실패 메시지를 사용자에게 전송하고 프로토콜을 종료한다.

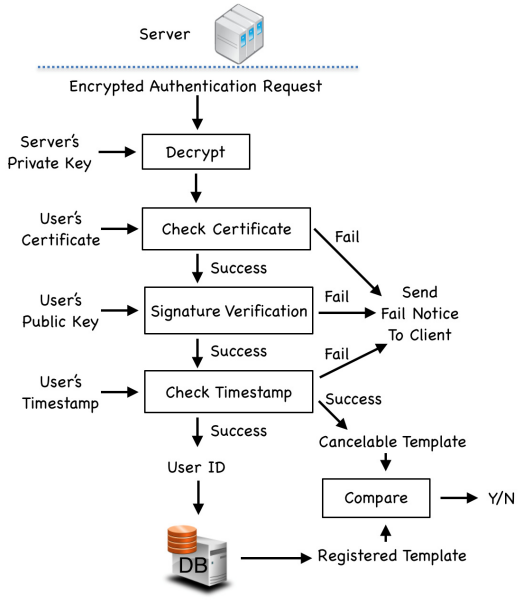
단계 7: 서버는 사용자 PKI 인증서에 있는 공개키로 사용자의 서명을 검증한다. 서버는 서명 검증에 성공하면 단계 8로 이동하고, 그렇지 않으면 실패 메시지를 사용자에게 전송하고 프로토콜을 종료한다.

단계 8: 서버는 사용자가 보낸 타임스탬프가 일정 시간 범위에 있는지를 검증한다. 서버는 타임스탬프 검증에 성공하면 단계 9로 이동하고, 그렇지 않으면 실패 메시지를 사용자에게 전송하고 프로토콜을 종료한다.

단계 9: 서버는 사용자 ID와 취소 가능한 바이오메트릭 템플릿을 데이터베이스에 등록한다.

3.3 사용자 인증

그림 4는 서버에서 사용자를 인증하는 단계를 보여준다.



[Fig. 4] Biometric User Authentication Process

단계 1: 서버는 사용자가 보낸 암호화된 인증 패키지를 복원한다.

단계 2: 서버는 패키지에 포함된 사용자의 PKI 인증서를 검증한다. 서버는 인증서 검증에 성공하면 단계 3으로 이동하고, 그렇지 않으면 실패 메

시지를 사용자에게 전송하고 프로토콜을 종료한다.

단계 3: 서버는 사용자의 PKI 인증서에 있는 공개키를 이용하여 서명을 검증한다. 서버는 서명 검증에 성공하면 단계 4로 이동하고, 그렇지 않으면 실패 메시지를 사용자에게 전송하고 프로토콜을 종료한다.

단계 4: 서버는 패키지에 포함된 타임스탬프가 일정 시간 범위에 있는지를 검증한다. 서버는 타임스탬프 검증에 성공하면 단계 5로 이동하고, 그렇지 않으면 실패 메시지를 사용자에게 전송하고 프로토콜을 종료한다.

단계 5: 서버는 패키지에 포함된 사용자 ID를 검색하여 데이터베이스에 등록된 사용자 템플릿을 가져온다.

단계 6: 서버는 단계 5의 템플릿과 패키지에 포함된 템플릿을 비교하여 유사도를 판단한다. 서버는 유사도 값이 설정된 임계 값 이상이면 올바른 사용자로 인증하고, 그렇지 않으면 인증에 실패했음을 사용자에게 알린다.

4. 분석

제안한 바이오메트릭 템플릿 생성, 등록 및 인증 프로토콜에 대해서 전사적 공격과 능동적 공격으로부터의 안전성을 분석한다.

4.1 전사적 공격

전사적 공격은 모든 경우의 수를 대입하여 암호문 또는 비밀번호를 알아내는 방법이다. 제안한 방법에서 스캔 타임은 초 단위로 측정되는데 10초를 최대 시간으로 가정하면 총 10 가지 경우가 발생한다.

사용자는 자신의 열 개 지문 중에 하나를 이용하여 등록 프로토콜에 참여한다. 해커가 전사적 공격을 하기 위해서는 (지문, 스캔 타임) 조합을 알아야한다. 해커가 10개 지문을 모두 위조한 경우라고 가정하면, 해커가 전사적 공격을 성공할 확률은 $1/10^2$이 된다.

기존의 아이디와 패스워드를 이용한 방법은 컴퓨터 프로그램만으로 전사적 공격이 가능하다. 따라서, 보안성을 높이려면 패스워드의 길이가 길어야하고, 또한 쉽게 예측할 수 없도록 만들어야한다. 반면, 바이오메트릭 인증은 사람이 직접 개입하기 때문에, 전사적 공격에 대한 안전성이 상대적으로 높다.

제안한 방법에서 보안 레벨을 조정하려면 등록할 지문의 개수를 늘려주면 된다. 예를 들어서, 두 개의 (지문, 스캔 타임) 조합을 이용한다면 경우의 수가 10^4이 되고, 해커가 수작업으로 최대 10,000번 비교를 시도해야한다. n 개의 지문을 등록하게 되면 경우의 수는 10^{2^n}이 된다. 이와 같이, n 값을 조정하면 다양한 응용에 맞게 보안 레벨을 조절할 수 있다.

4.2 능동적 공격

일반적으로 클라이언트-서버 환경에서는 재전송 공격과 MITM 공격(Man In The Middle)에 대한 안전성이 보장되어야한다.

재전송 공격은 해커가 서버로 전송된 메시지를 중간에 가로채서 보관하고 있다가, 이 메시지를 서버로 다시 보내어 사용자 인증을 시도하는 공격이다.

3.3절의 사용자 인증 단계에서 사용자는 매 세션 마다 타임스탬프 정보를 패키지에 포함하여 서명하고, 서버는 매 세션 마다 타임스탬프가 유효한지 검증하기 때문에, 재전송 공격의 위험을 최소화할 수 있다.

MITM 공격은 해커가 클라이언트에게는 서버인 것처럼, 서버에게는 클라이언트인 것처럼 가장하는 공격이다. 제안한 프로토콜에서 사용자와 서버는 PKI 인증서 기반으로 디지털 서명을 한다. 해커가 가장에 성공하려면 인증서에 있는 공개키와 쌍을 이루는 클라이언트와 서버의 개인키를 알아야한다. 공개키 암호 알고리즘의 안전성이 보장되면, 제안한 프로토콜은 MITM 공격으로부터 안전하다.

5. 결론

본 논문에서는 사용자 편의성과 경제성을 고려한 취소 가능한 바이오메트릭 인증 기법을 제안하였다. 제안한 방법은 바이오메트릭 템플릿 생성, 등록 그리고 사용자 인증 프로토콜로 구성되고, 전사적공격, 재전송 공격, MITM 공격으로 부터 안전하다. 기존의 취소 가능한 바이오메트릭 인증 기법들은 사용자가 별도로 패스코드를 입력해야 해서 사용성이 떨어지는데, 제안한 방법은 스캔 타임을 이용하여 패스코드를 만들어 냄으로써 사용이 편리하고 경제적이다.

ACKNOWLEDGMENTS

이 논문은 2016년도 백석대학교 대학연구비에 의하여 수행된 것임

REFERENCES

[1] G. J. Lee, K. H. Lee, “A Study of Security Threats in Bluetooth v4.1 Beacon based Coupon Convergence Service,” Journal of the Korea Convergence Society, Vol. 6, No. 2, pp. 65-70, 2015.

[2] J. K. Mun, J, M, Kim, “Modify of extended API for Smart-TV security,” Journal of the Korea Convergence Society, Vol. 5, No. 2, pp. 1-6, 2014.

[3] M. Stamp, Information Security: Principles and Practice 2nd Edition, Wiley-Inerscience, 2011.

[4] S. Y. Kim, K. S. Jang, S. J. Lee, “Study on Password Security,” Journal of Digital Forensics, No. 8, pp. 28-39, 2011.

[5] H. Li, K. Toh, L. Li, Advanced Topics in Biometrics, World Scientific, 2011.

[6] Apple Support, Use Touch ID on iPhone and iPad, https://support.apple.com/en-us/HT201371.

[7] N. K. Ratha, J. H. Connell, R. M. Bolle, “Enhancing security and privacy in biometric-based authentication systems,” IBM Systems Journal, Vol. 40, No. 3, pp. 614 - 634, 2001.

[8] V. M. Patel, N. K. Ratha and R. Chellappa, "Cancelable Biometrics: A review," IEEE Signal Processing Magazine, Vol. 32, No. 5, pp. 54-65, 2015.

[9] ITU-T X.1088, A Framework for biometric digital key generation, ITU-T, 2008.

[10] S. H. Yun, “The One Time Biometric Key Generation and Authentication Model for Portection of Paid Video Contents,” Journal of the Korea Convergence Society, Vol. 5, No. 4, pp. 101-106, 2014.

[11] Paul F. Roberts, “7 ways to beat fingerprint biometrics,” ITworld, http://www.networkworld.com/article/2293129/data-center/120606-10-ways-to-beat-fingerprint-biometrics.html, 2013.

[12] Y. S. Lee, “Security Enhancement to an Biometric Authentication Protocol for WSN Environment,” Journal of Information and Security, Vol. 16, No. 6, pp. 83-88, 2016.

[13] G. Jaspher Willsie Kathrine, E. Kirubakaran,. “Biometric Authentication and Authorization System for Grid Security,” International Journal of Hybrid Information Technology, Vol. 4, No. 4, pp. 43-58, 2011.

[14] Rathgeb, Uhl, “A survey on biometric cryptosystems and cancelable biometrics,” EURASIP Journal on Information Security, http://jis.eurasipjournals.com/content/2011/1/3, 2011.

[15] S. H. Lee, “Relation between Certainty and Uncertainty with Fuzzy Entropy and Similarity Measure,” Journal of the Korea Convergence Society, Vol. 5, No. 4, pp. 155-161, 2014.

[16] J. S. Lee, J. H. Kim, J. S. Chae, B. S. Lee, “A Detection Method of Fake Fingerprint in Optical Fingerprint Sensor,” Journal of Korea Multimedia Society, Vol. 11, No. 4, pp. 492-503, 2008.

[17] H. S. Choi, “The Trend of Technology on Count--erfeiting Biometric Data,” The Magazine of the IEIE, Vol. 33, No. 1, pp. 64-72, 2006.

저자소개

윤 성 현(Sunghyun Yun) **[종신회원]**

- 1994년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학석사)
- 1997년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학박사)
- 1998년 3월 ~ 2002년 2월 : LG전자 중앙연구소 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수

<관심분야> : 모바일 보안, 바이오메트릭 인증, DRM, 전자선거