Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.1085

트라이톤 패러독스를 이용한 생체인증의 고찰*

정 창 훈,[1†] 신 동 오,[1] 양 대 헌,[1] 이 경 희[2‡]
[1]인하대학교, [2]수원대학교

Study of Biometrics using Tritone Paradox*

Changhoon Jung,[1†] DongOh Shin,[1] DaeHun Nyang,[1] KyungHee Lee[2‡]
[1]INHA University, [2]The University of Suwon

요 약

음악 이론에서 트라이톤은 세 개의 온음(또는 여섯 개의 반음) 차이를 가지도록 구성된 음정을 말하며, 조화와 선율의 불협화음을 발생시킨다. 트라이톤 패러독스는 일종의 청각적 착각으로, 트라이톤을 들은 어떤 사람은 이것이 올라가는 연음으로 들리지만, 또 어떤 사람은 이를 내려가는 연음으로 들리는 현상을 말한다. 이 논문은 트라이톤 패러독스를 이용한 새로운 비정적 생체인증기법에 대해 검토하고, 사용자 실험을 통하여 이 기법의 유일성과 일관성을 분석한다. 그리고 이를 응용하여 키로깅, 어깨너머 훔쳐보기, 무작위 대입 등의 공격에 대해 안전한 몇 가지 인증 프로토콜을 제안한다.

ABSTRACT

In music theory, the triton is defined as a musical interval composed of three adjacent whole tones(or six semitones), which generates a harmonic and melodic dissonance. The triton paradox is an auditory illusion which is heard as ascending by some people and as descending by others. In this paper we examine an emerging non-static biometric technique that aims to identify users based on analyzing uniqueness and consistency through the user experiences. We also propose some authentication schemes which provides protection against key logging, shoulder surfing, and brute force attacks.

Keywords: Biometrics, Tritone Paradox, Authentication Protocol, Auditory Sense

I. 서 론

네트워크 통신의 발달로 인하여 사용자는 다양한 정보를 쉽게 제공 받을 수 있는 환경이 되었고, 최근 스마트폰의 발달로 인하여 언제 어디서든지 더 쉽게 정보에 접근 가능하게 되었다. 그러나 이러한 발전으로 인해 해커들은 사용자의 권한을 얻기만 한다면 자유롭게 다른 사용자의 정보를 얻을 수 있는 환경이 되었다. 이에 따라 사용자의 권한을 얻는 인증 프로토콜의 보안성을 높이기 위하여 많은 연구가 진행되어지고 있고, 특히 최근에는 인증 프로토콜에 생체인식을 결합하는 분야가 활발하게 연구되고 있다.

사람의 생체 정보 중 지문, 홍채, 얼굴, 음성, 정맥 등을 이용한 생체인증 시스템은 다양한 연구·개발이 이루어졌고, 일부는 상용화됨과 동시에 생체인증에 대한 다양한 공격 방법이 제시되었다. Matsumoto 등은 채취한 지문 자국뿐만 아니라 디지털 지문 이미지로부터 젤라틴 원료의 가짜 손가락을 만들고, 이를 열 한 종류의 지문 인식 시스템에서 테스트해보았다. 그 결과, 가짜 손가락은 68~100%의 확률로 지문 인증 시스템을 통과하였다[1]. Virginia 등은 홍채인증 시스템을 속이기 위해 종이

접수일(2015년 6월 19일), 수정일(2015년 8월 27일), 게재확정일(2015년 9월 22일)
* 이 논문은 이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (2014R1A1A2059852)
† 주저자, jcptk677@hotmail.com
‡ 교신저자, khlee@suwon.ac.kr(Corresponding author)

에 출력된 홍채 이미지를 이용하였다. 저자들은 본격적인 실험에 앞서 잉크젯, 레이저 프린터와 여섯 종류의 종이, 네 종류의 이미지 전처리 알고리즘을 이용하여 홍채인증 시스템을 속일 수 있는 최적의 조합 연구하였고, 그 결과 Open+TopHat 전처리를 거친 이미지를 고해상도 용지에 잉크젯 프린터로 출력하는 것이 가장 이상적이라는 사실을 찾아내었다. 실험에는 100 가지의 홍채와, 홍채 하나당 여덟 개의 이미지가 사용되었으며, 가짜 홍채만을 이용한 등록 및 인증 실험과, 진짜 홍채를 등록한 뒤 종이로 출력한 홍채 이미지를 이용한 인증 실험이 각각 진행되었다. 그 결과, 홍채 인증 시스템은 72%의 가짜 이미지를 정상 홍채로 인식하였으며, 50% 이상의 확률로 홍채 인증 시스템이 무력화 될 수 있다고 주장하였다[2].

이 논문은 트라이톤 패러독스를 이용한 청각 생체인증의 가능성과 그 시스템의 대해 논의한다. 트라이톤 패러독스(Tritone Paradox)란, 트라이톤 관계에 있는 두 연음을 들었을 때, 어떤 사람들은 올라가는 연음으로, 다른 사람들은 내려가는 연음으로 들리는 현상을 말한다. 이 논문에서는 트라이톤 패러독스를 응용한 새로운 생체인증 실험을 제안하고, 그 가능성에 대해 논의한다. 그리고 트라이톤 패러독스를 응용한 몇 가지 인증 프로토콜을 제안한다.

이 논문의 구성은 다음과 같다. 2장에서는 지문인식, 홍채인식을 이용한 인증 방법과 인증 프로토콜, 트라이톤 패러독스에 대해서 알아본다. 3장에서는 트라이톤 패러독스를 응용한 생체인증 실험과, 유일성과 일관성에 대해 논의한다. 4장에서는 트라이톤 패러독스를 이용한 인증 프로토콜을 제안한다. 마지막 5장에서는 결론과 향후 연구에 대해 논의한다.

II. 관련 연구

2.1 생체인식

생체인식이란, 사람이 가진 생체정보를 추출하고, 이를 판별이 가능한 형태로 데이터화하여 활용하는 것을 말한다. 생체인식의 대표적인 기술은 지문인식, 홍채인식, 얼굴인식, 음성인식, 정맥인식 등이 있으며, 생체 정보는 사람의 몸에서 물리적으로 분리되거나 변경되기 어렵기 때문에 타인에게 도용되거나 복제될 위험과 분실의 가능성이 모두 낮다는 장점을 가지고 있다.

그러나 통상적으로 이용되는 일반 비밀번호와는 달리, 생체인식에 사용되는 정보는 특정인을 지칭할 수 있을 만큼의 개인화된 정보이기 때문에 사생활 침해에 대한 우려와, 생체 인증을 통한 국가의 개인 통제 가능성이 문제점으로 제기되고 있다[3].

생체 정보를 인식하는 것은 사용자가 인식 시스템에 입력하는 생체 정보와 기존 데이터베이스에 저장되어 있는 정보의 일치 정도에 따라서 확률적으로 결정된다. 그러므로 어느 정도 잘못 인식되는 경우가 발생하게 되는데, 이러한 오인식률(EER, Equal Error Rate)은 자신의 정보를 타인의 정보라고 잘못 판단될 확률(FRR, False Reject Rate)과 타인의 정보가 자신의 정보라고 잘못 판단될 확률(FAR, False Accept Rate)에 의해 결정된다. 이 두 가지 요소에 의해서 생체 인식의 신뢰도가 결정되며 FAR과 FRR의 합이 낮을수록 인식률이 높다고 평가된다[4].

어떠한 분야의 생체인식이든 사람마다 가지고 있는 생체 정보들은 한 개인이 다른 사람들과 비교해보았을 때 현실적으로 완벽한 유일성과 일관성을 가지고 있는 것은 아니다. 사람마다 지문이나 홍채의 형태가 같을 수도 있기 때문에 현재 생체 인식에 대한 연구는 100%에 가까운 안전성을 목적으로 진행되어지고 있는 것이 현 실정이다[5].

2.1.1 지문인식

지문인식은 현재 생체인식 기술 중 가장 대중적으로 사용되고 있으며, 개개인마다 다른 손가락 지문을 판독하여 사용자를 인식하는 기술이다. 지문인식의 원리는 Fig. 1.처럼 지문의 융선과 골, 끝점, 분기점, 중심점 등을 활용하여 미리 저장되어 있는 사용자의 지문과 일치하는지를 비교하는 것이다.

지문을 인식하는 방법으로는 빛을 이용하는 광학식, 초음파를 이용하는 초음파식, 전기 용량의 차이를 이용하여 지문을 판독하는 정전용량방식이 있다.

지문은 변하지 않고 잃어버릴 위험이 없다는 장점 때문에 지문인식이 가장 보편적으로 사용되고 있으나 스캐너에 물이나 이물질이 묻은 경우, 간혹 지문이 닳아 없어지는 경우 오인식률이 높아진다는 단점이 있다[6]. 젤라틴을 원료로 하는 가짜 손가락 지문으로도 지문 인식 시스템을 통과할 수 있다는 사실이 알려진 이후로[1], 최근 출시되는 지문 인식 장치들은 전정용량 방식 등을 이용하여 손가락을 스캔하면

Fig. 1. Structure of fingerprint

서 동시에 실제 사람의 지문인지도 검사하는 기능을 갖추는 추세이다.

2.1.2 홍채인식

생체인식 분야에서 가장 높은 정확성으로 인해 우수한 기술로 인정받고 있으며, 따라서 주로 고도의 보안이 필요한 곳에 사용되는 것이 홍채인식이다[7]. 홍채 인식은 개개인마다 가지고 있는 고유한 홍채의 패턴을 판독하는 방법으로서, 홍채의 고유한 패턴은 생후 6개월 이내에 생성되어 2~3세 정도에 패턴이 완성된다. 이렇게 생성된 홍채의 패턴은 오랜 기간 변하지 않는다는 특징가지고 있기 때문에 생체인식 기술에 적용될 수 있다.

개개인마다 다른 홍채의 패턴을 인식하는 방법은 Fig. 2.처럼 사람 눈의 검정색 동공을 중심으로 홍채와 공막의 영역을 나눈 후 홍채의 무늬를 스캔함으로서 홍채를 판독하는 방법이 있다[8].

홍채 인식은 오랜 기간 동안 변하지 않으며 동일

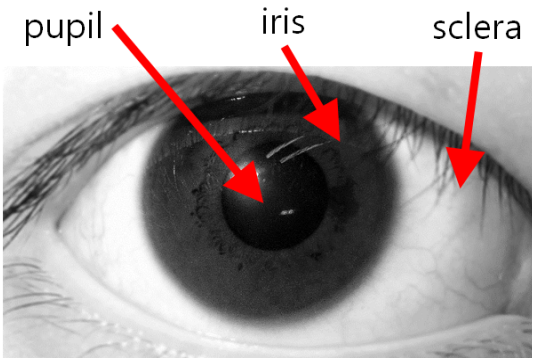


Fig. 2. Structure of eye

한 패턴을 지닌 홍채를 발견할 확률은 매우 낮기 때문에 보안성이 상당히 높다. 그러나 홍채인식 장치가 다른 생체인식에 장치에 비해서 운용비용이 높으며, 종이로 만든 가짜 홍채로 홍채 인증 시스템을 통과할 수 있음이 실험적으로 증명되어서[2] 최근에는 홍채 인식 뿐만 아니라 실제 사람의 홍채임을 검증하는 기법이 같이 사용되고 있다.

2.1.3 다중 생체인식

다중 생체인식이란 하나의 생체정보를 이용하는 시스템이 아닌, 두 가지 이상의 생체정보를 이용하는 시스템이다[9]. 만약, 어떠한 사용자가 사고 등의 이유로 지문이 심하게 훼손되어 지문인식 시스템을 사용할 수 없을 경우에 다중 생체인식을 이용하여 이 문제점을 해결할 수 있다. 다중 생체인식은 지문과 얼굴의 생체정보를 모두 이용하거나, 홍채와 음성의 생체정보를 같이 이용하여 기존에 존재하던 단일 생체인식의 편리성, 보안성 및 신뢰성을 높일 수 있는 장점을 가지고 있다. 이 기술은 극히 낮은 오인식률을 요구하는 금융 분야에서 많이 쓰이고 있으며, 여러 생체정보를 이용하여야하기 때문에 다양한 생체정보를 인식하는 기술이 요구되고 있다.

2.2 인증 프로토콜

인증 프로토콜이란, 어떠한 네트워크 리소스 또는 서버에 접근하기 이전에 허가된 사용자임을 확인하는 절차이다. 인증 프로토콜의 종류로는 이미 널리 사용되고 있는 비밀번호 인증, OTP 인증, 보안카드 번호 인증, 생체 인증 등이 있다. 또한 QR코드와 스마트폰을 이용하여 키로깅 공격을 효과적으로 방어할 수 있는 인증도 개발되었으며[10], 사람이 서명을 할 때에 쓰는 모양, 쓰는 속도, 필체의 각도 등을 이용하는 서명인증도 연구되어지고 있다[11].

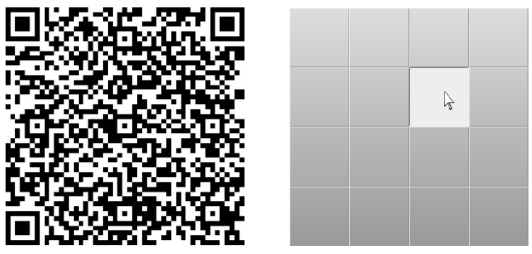


Fig. 3. QR code and clicking blank keyboard

Fig. 4. QR code scanning and keyboard on smartphone

2.2.1 QR코드와 스마트폰을 이용하여 키로깅 공격을 효과적으로 방어하는 인증 프로토콜

양대헌 등은 사용자가 PC에서 인증을 시도할 때에 스마트폰과 QR코드를 이용하여 키로깅 공격을 효과적으로 방어할 수 있는 인증 프로토콜을 제안하였다[10]. 이 프로토콜은 PC상의 사용자가 로그인을 위해 아이디를 서버에 전송하면, 서버는 Fig. 3.처럼 QR코드와 마우스로 클릭하여 입력할 수 있는 빈 키보드를 보여준다. 이때 Fig. 4.처럼 스마트폰을 이용하여 QR코드를 촬영하면 스마트폰에 키보드가 나타나게 되고, 사용자는 이 키보드를 참조하여 PC상에서 마우스로 비밀번호를 입력할 수 있게 된다. 그러므로 사용자는 로그인을 할 때 PC와 연결된 키보드를 사용하지 않고 스마트폰상의 출력된 키보드를 참조하여 마우스로 비밀번호를 입력할 수 있게 됨으로서 키로깅 공격을 효과적으로 방어할 수 있다.

2.2.2 서명 인증 프로토콜

서명 인증 프로토콜이란 Fig. 5.처럼 사용자가 서명을 하는 습관을 이용하여 인증을 하는 프로토콜이다[11]. 사용자는 오프라인 방식으로 서명을 종이에 작성한 후 스마트폰 카메라 등으로 촬영하여 입력을 하거나, 마우스, 태블릿, PDA, 서명 전용 디바이스 등으로 서명을 입력할 수 있다. 이렇게 입력된 서명에서 쓰는 속도, 필체의 각도, 획 순서, 서명의 모양 등의 여러 가지 정보를 추출 할 수 있고, 이전에 등록되어 있는 서명의 정보와 비교하여 진서명인지 모조서명인지 판별될 수 있다. 이러한 프로세스로 인증이 진행되며, 현재 서명 인증 프로토콜은 카드 결제, 택배 수령 확인 등에서 쓰이고 있으며 부인방지의 역할을 하고 있다.

Fig. 5. Example of signature authentication

2.2.3 생체 인증 프로토콜

생체 정보를 이용하여 특정인을 인증을 하는 시스템을 생체 인증 프로토콜이라고 말하며, 이때 사용되는 생체 정보는 유일성과 일관성을 가지고 있어야 한다.

생체인식을 이용한 인증 프로토콜은 손가락 지문을 이용하는 지문인식 인증, 눈의 홍채를 이용하는 홍채인식 인증 등이 있다. 이러한 생체인증 같은 경우는 키보드로 어떤 문자를 입력하는 것이 아니라 Fig. 6.처럼 지문이나 홍채의 형태를 대조하는 개념이기 때문에 키로깅, 어깨너머 훔쳐보기, 무작위 대입 등의 같은 공격을 방어하는데 효과적이다. 그러나 생체 정보를 인식하기 위하여 용도에 맞는 하드웨어를 별도로 구입해야 한다는 비용적인 문제와 각 인증 시스템에 따른 공격 기법도 다양해지고 있어 지속적인 연구 개발이 필요한 분야이다[1, 2].

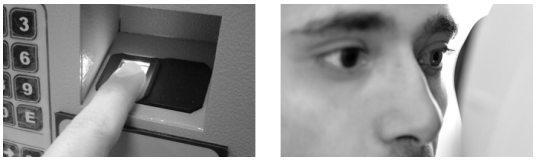


Fig. 6. Fingerprint and iris biometrics authentication

2.3 트라이톤 패러독스

트라이톤 패러독스는 일종의 청각적 착각으로, 트라이톤을 들은 어떤 사람은 이것이 올라가는 연음으로 들리지만, 또 어떤 사람은 이를 내려가는 연음으로 들리는 현상을 말한다[12].

일반적으로 하나의 옥타브는 도(C), 레(D), 미(E), 파(F), 솔(G), 라(A), 시(B)로 구성되어 있으며, 각각의 음은 #과 ♭을 이용하여 반음을 올리거나 반음을 내릴 수 있다. 그리고 #을 이용하여 반음을 올린 음은 한음을 올린 음에서 ♭을 이용하여 반음을 내린 음과 같으며, 예를 들면 C#과 D♭은 같은 음을 뜻한다. 그러므로 하나의 옥타브는 반음을 포함하여 Fig. 7.처럼 12개의 음정으로 구성되어 있다. 여기에서 하나의 음과, 그 음으로부터 6반음(또는 3온음) 만큼 올리거나 내린 음의 조합이 트라이톤이 된다. .는 트라이톤의 다양한 예시를 보여준다. 이러한 트라이톤을 사람들에게 들려주었을 때 어떤 사람들은 그것을 올라가는 연음이라고 판단하고, 다른 사람들은 그것이 내려가는 연음이라고 판단한다.

Deutsch는 트라이톤 패러독스 현상이 사람 개개인이 가지고 있는 억양과 밀접한 연관이 있음을 밝혀내었다. 개인의 억양은 일반적으로 태어나고 성장한 지역에 따라 결정되므로, 같은 지역에서 자란 사람들은 트라이톤 패러독스의 결과 또한 같을 확률이 높아진다. 예를 들면, 특정 지역에 거주하는 미국인들에게 동일한 트라이톤을 들려주었을 경우, 그 연음이

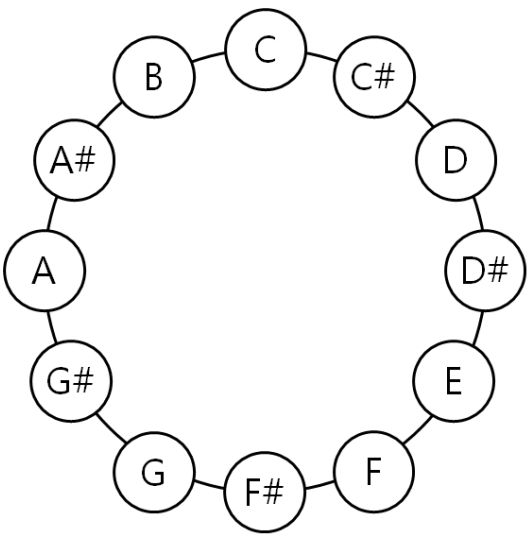


Fig. 7. Octave circle model

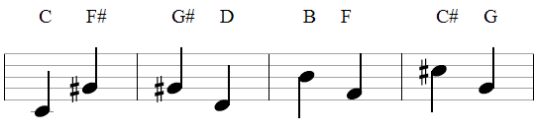


Fig. 8. Examples of tritones

올라가는 것인지, 내려가는 것인지에 대한 판단이 동일한 경우가 많았다. 하지만, 동일한 트라이톤을 영국인들에게 들려주었을 경우, 미국인들과 다른 판단을 내리는 경우가 많았다. 이는 미국과 영국의 억양 차이로부터 기인한 것이다[13]. 한국에서도 이와 유사한 실험이 진행되었는데, 그 결과 동일한 트라이톤을 들은 서울 사람들과 경상도 사람들의 대답이 서로 반대로 나타났다[14].

이 논문에서는 이와 같은 트라이톤의 특징을 생체인증에 적용하기 위하여 실험을 진행하고, 이것을 이용한 몇 가지 로그인 인증 프로토콜을 제안한다.

III. 트라이톤 패러독스를 생체 인증에 적용하기 위한 실험

어떠한 생체 정보를 이용하여 인증을 수행하려면 한 개체의 정보가 다른 것과 다르다는 유일성을 가져야하며, 그 속성이 변하지 않는다는 일관성도 가져야 한다. 따라서 우리는 트라이톤 패러독스가 갖는 유일성과 일관성을 파악하는 것에 중점을 둔다. 트라이톤 패러독스 현상의 핵심은 사람 개개인이 가지고 있는 억양에 따라 달라진다는 것이지만, 이 실험에서는 피실험자들의 결과가 유일하고 일관되는 점만 확인하는 것이 그 목적이므로 피실험자의 억양과 출생지, 성장지역 등에 대한 대한 조사는 진행하지 않았다.

우리는 실험을 진행하기에 앞서 트라이톤 패러독스에 대한 확률에 대해 고찰과 함께 실험 환경, 실험 시나리오, 실험 방법을 설정한다. 그리고 진행한 실험의 결과를 바탕으로 트라이톤 패러독스를 이용한 생체인증에 대해 논의한다.

3.1 트라이톤 패러독스의 확률적 고찰

어떠한 사람이 하나의 트라이톤을 듣고 대답할 수 있는 경우의 수는 올라가는 연음 또는 내려가는 연음이므로 2가 된다. 마찬가지로 두 개의 트라이톤을 순서대로 들려준다면 나올 수 있는 경우의 수는 4가 되므로, n개의 트라이톤에 대한 응답의 경우의 수는

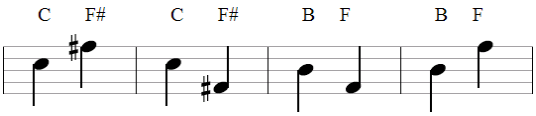


Fig. 9. An example of tritone cases based on one tone

2^n으로 정의된다.

Fig. 9.은 트라이톤이 발생되는 연음의 예시이다. 2옥타브 C는 F#과 조화를 이루어 올라가는 연음과 내려가는 연음을 구성할 수 있으며, 1옥타브 B는 F와 조화를 이루어 트라이톤을 유사하게 구성할 수 있다. 하나의 옥타브는 Fig. 7.처럼 총 12음으로 구성되어 있으므로 한 옥타브당 총 24개의 트라이톤을 만들 수 있으며, n개의 옥타브를 이용하는 경우 가질 수 있는 트라이톤은 총 $24n$개 이다. 따라서 n개의 옥타브와 m개의 트라이톤을 이용한다면 구성할 수 있는 시나리오는 총 ${}_{24n}C_m$개 이다.

3.2 실험 환경

n개의 트라이톤을 순서대로 들려주었을 때 나올 수 있는 사용자 응답의 2^n개이다. 이 논문에서는 10개의 트라이톤을 이용하여 1/1024 의 안전성을 갖는 트라이톤 생체인증에 대하여 사용자 실험을 진행하였다. 트라이톤 생체인증 실험의 피실험자는 페이스북과 트위터를 통해 모집되었으며, 실험은 총 두 차례에 걸쳐 온라인으로 진행되었다. 첫 번째 실험에서는 73명, 두 번째 실험에서는 62명의 피실험자가 실험에 참여하였다.

3.3 실험 시나리오

1~2옥타브 대역에서 10개의 트라이톤으로 구성 가능한 조합의 개수는 ${}_2\times 24C_{10}$으로, 약 6.5×10^9개가 넘는다. 우리는 첫 번째 실험에서 Fig. 10. 과 같은 트라이톤 패러독스 시나리오를 이용하였고, 두 번째 실험에서는 Fig. 11.과 같은 시나리오를 이용하였다. 하나의 음은 약 0.6초간, 하나의 트라이톤은 약 1.2초간 재생되며, 트라이톤의 재생 간격은 약 2초로 설정하였다.

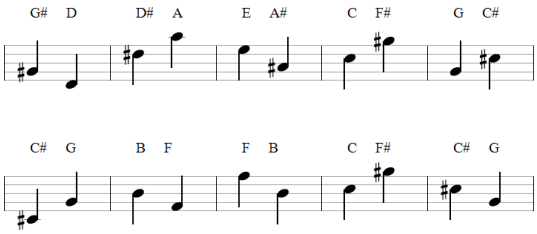


Fig. 10. First scenario of tritone paradox Experiment

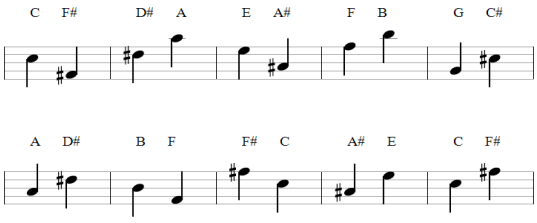


Fig. 11. Second scenario of tritone paradox Experiment

3.4 실험 방법

각 그룹 피실험자들은 준비된 실험 시나리오의 트라이톤을 순서대로 듣고, 설문지에 자신이 들은 바를 작성하였다. 우리는 트라이톤 패러독스가 유일성과 일관성을 갖는지 파악할 수 있도록 설문지를 구성하였다. 피실험자는 각 트라이톤을 듣고 그것이 올라가는 연음인지, 내려가는 연음인지를 선택하였고, 우리는 실험 데이터로부터 피실험자간 유일한 응답의 존재 여부를 파악하였다. 또한 이미 진행된 실험에 대해 다시듣기와 응답을 기록함으로써 일관성 있는 응답이 발생하는지를 살펴보았다. 그리고 실험 결과로부터 유일하면서도 일관성 있는 대답을 하는 사용자 그룹과 그렇지 않은 그룹을 분류하고, 그 비율을 확인하였다.

3.5 실험 결과

Fig. 12.와 Fig. 13.은 각각 첫 번째 실험과 두 번째 실험의 결과를 보여준다. 가로축은 실험에 이용된 트라이톤의 순서를 나타내고, 세로축은 각 트라이톤에 대해서 올라가는 연음 또는 내려가는 연음으로 선택한 사람들의 수를 나타낸다.

첫 번째 실험에서는 하나의 트라이톤에 대해서 치우쳐진 결과를 보였으나, 두 번째 실험에서는 분산된

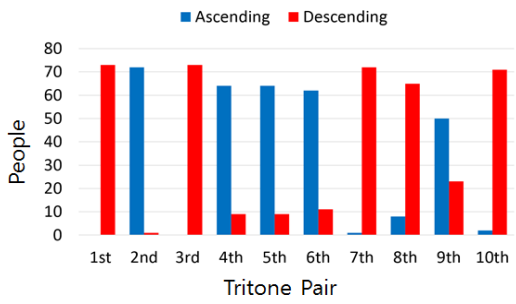


Fig. 12. The result of 1st experiment

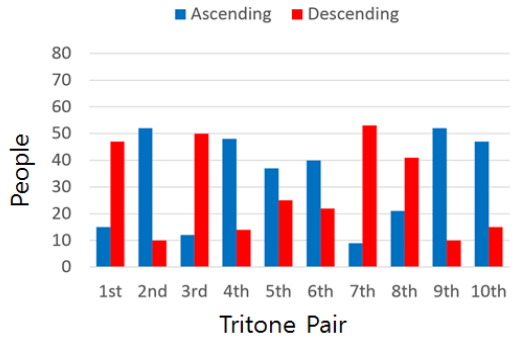


Fig. 13. The result of 2nd experiment

결과를 보인 경우가 많았다. Table 1.은 각 실험에 참여한 인원, 응답의 유일성 및 일관성, 이 두 속성을 모두 갖춘 경우, 그리고 FRR과 FAR의 비율을 보여준다.

73명의 피실험자가 참여한 첫 번째 실험에서 응답 결과가 유일한 사람은 16명이고, 응답 결과가 일관된 사람은 55명, 유일성과 일관성을 모두 보여준 피실험자는 10명이었다. 첫 번째 실험 결과, FRR은 25%, FAR은 79%라는 것을 알 수 있었고, 약 13%의 사람들만이 생체인증의 필요 요건을 갖춘 것으로 분석되었다.

하지만 62명의 피실험자가 참여한 두 번째 실험에서는 유일한 응답 결과를 보인사람이 37명, 일관된 응답을 보인 사람은 53명, 유일하면서도 일관된 사람은 34명이었다. 첫 번째 실험의 결과와 다르게 FRR은 15%, FAR은 41%로 낮아졌고, 약 55%의 사람들로부터 트라이톤을 이용한 생체인증의 가능성을 확인할 수 있었다.

Table 1. Result of experiment

	1st Exp.	2nd Exp.
Total people	73	62
Uniqueness	16 (21%)	37 (59%)
Consistency	55 (75%)	53 (85%)
Uni and Con	10 (13%)	34 (55%)
FRR	18 (25%)	9 (15%)
FAR	57 (79%)	25 (41%)

두 번의 실험 결과, 트라이톤의 종류나 들려주는 순서에 따라 결과가 달라지는 모습을 관찰할 수 있었다. Fig. 10.에서 볼 수 있듯이 네 번째와 아홉 번째의 트라이톤은 모두 2옥타브의 올라가는 C~F#로서 동일한 것이다. 그러나 사용자의 응답 결과는 Fig. 12.과 같이 서로 다른 결과를 나타내었다. 첫 번째 실험의 4차 트라이톤에 대한 응답은 올라가는 연음이라고 대답한 비율이 약 88%로 상당히 높으나, 9차 트라이톤에서 그것이 올라가는 연음이라고 대답한 비율은 약 68%이다. 트라이톤은 그 자체가 패러독스이므로, 같은 트라이톤이라 하더라도 다르게 반응하는 이유를 상세하게 파악하는 것은 매우 어려운 일이다. 하지만 어떤 트라이톤의 진행방향을 판단에 영향을 주는 요인을 분석하고, 그로부터 유일성과 일관성이 모두 높은 트라이톤의 조합을 구성하는 것은 또 다른 연구주제가 되므로, 이에 대한 분석 및 연구는 추후 연구로 남긴다.

IV. 트라이톤 패러독스를 이용한 인증 프로토콜의 고찰

두 번의 실험을 통하여 확인된 사실은 트라이톤을 유일하면서도 일관성 있게 듣는 사람이 존재한다는 것이다. 비록 이 논문의 실험 결과는 지문, 홍채, 정맥, 얼굴 등을 이용한 생체인증에서의 유일성과 일관성[7]을 보장해주지는 못하지만, 잘 만들어진 트라이톤에서는 다른 생체인증에서 요구되는 만큼의 유일성과 일관성을 보일 가능성도 충분히 있다고 판단된다. 이 장에서는 트라이톤 패러독스가 유일성과 일관성을 보장한다는 가정 하에 몇 가지 인증 프로토콜을 제안한다.

4.1 주 패스워드 인증 프로토콜

사용자는 서버에 가입할 때 회원 정보와 비밀번호, 그리고 서로 다른 다섯 개의 트라이톤 시나리오에 대한 응답을 서버에 등록한다. 이 때 비밀번호로 등록할 수 있는 문자는 대·소문자를 포함하는 영문자

와 키보드의 문자키 위쪽에 위치한 숫자 그리고 그에 대응되는 특수문자로 제한된다. 즉, a~z, A~Z, 1~0 그리고 숫자에 해당하는 특수문자인 !, @, # ~ (,)이다. 또한 하나의 트라이톤 시나리오는 1옥타브와 2옥타브로부터 생성될 수 있는 트라이톤 중 비밀번호의 길이만큼(예를 들면 10자리) 무작위로 선택되어 구성된다.

인증 요청시 사용자는 우선 아이디를 서버에 입력한다. 서버는 해당 사용자의 비밀번호와 다섯 개의 트라이톤 시나리오 중에 무작위로 하나를 선택하여 아래와 같은 연산을 수행한다.

- 사용자가 등록한 비밀번호의 첫 째 문자가 소문자이고, 첫 째 트라이톤 응답이 올라가는 연음이라면 소문자를 대문자로 변경한다. (a→A) 유사하게, 첫 째 문자가 숫자인 경우에는 특수문자로 변경한다. (1→!)
- 사용자가 등록한 비밀번호의 첫 째 문자가 대문자이고, 첫 째 트라이톤 응답이 내려가는 연음이라면 대문자를 소문자로 변경한다. (A→a) 유사하게, 첫 째 문자가 특수문자인 경우, 숫자로 변경한다. (!→1)
- 사용자가 등록한 비밀번호의 첫 째 문자가 소문자이고, 첫 째 트라이톤 응답 또한 내려가는 연음이라면 이 문자는 변경하지 않는다. (a→a) 이 규칙은 첫 째 문자가 숫자인 경우에도 동일하게 적용된다. (1→1)
- 첫 째 문자가 대문자이면서 첫 째 트라이톤 응답이 올라가는 연음인 경우에도 해당 문자는 변경하지 않는다. (A→A) 이 규칙은 첫 째 문자가 특수문자인 경우에도 동일하다. (!→!)
- 위와 같은 연산을 비밀번호의 길이만큼 반복한다.

위와 같은 규칙에 따라 사용자의 비밀번호를 트라이톤과 결합하면 트라이톤이 올라가는 연음인 경우 대문자 또는 특수문자로 변경되며, 내려가는 연음인 경우 소문자 또는 숫자로 변경된다.

Table 2.는 비밀번호가 트라이톤 시나리오 결과와 연산되어 변경되는 예를 보여준다. 만약 사용자가 회원가입 시 등록한 비밀번호가 aBCDe1@#$5이고, 트라이톤 시나리오의 결과를 ↑↓↑↓↑↓↑↓↑↓처럼 답했다면, 비밀번호는 AbCdE1@3$5로 변경된다. 이 때 ↑기호는 올라가는 연음으로 응답한 것을 뜻하고, ↓기호는 내려가는 연음으로 응답한 것을 뜻한다.

Table 2. Operation result example of password and tritone paradox

Case	Password
Original(Registered)	aBCDe1@#$5
↑↓↑↓↑↓↑↓↑↓	AbCdE1@3$5
↑↓↑↓↑↑↑↑↑↓	AbCdE!@#$5
↑↓↓↓↑↓↑↑↓↓	AbcdE1@#45
↑↑↓↓↑↓↑↑↓↓	ABcdE1@#45
↑↓↓↓↑↓↑↓↓↓	AbcdE1@345

서버는 이렇게 연산된 비밀번호를 버퍼에 저장한 후에, 연산에 사용된 첫 째 트라이톤을 사용자에게 들려준다. 사용자는 이를 듣고 올라가는 연음이면 대문자(또는 특수문자)로, 내려가는 연음이면 소문자(또는 숫자)로 비밀번호의 첫 글자를 입력한다. 비밀번호의 첫 글자 입력을 완료하면 이어서 두 번째 트라이톤이 재생되고, 사용자는 그것을 듣고 전과 같은 방법으로 비밀번호를 입력한다. 이 과정은 비밀번호의 길이만큼 반복된다. 이 과정을 거쳐서 사용자는 자신이 회원가입 할 때 등록한 비밀번호와는 다른 비밀번호를 서버에 전송하게 된다.

그 다음, 서버에서는 사용자로부터 전송받은 비밀번호와 기존에 연산되어 버퍼에 저장되어 있던 비밀번호를 비교하여 일치한다면 사용자를 성공적으로 인증하고, 실패한다면 인증을 거부한다. 만약 사용자가

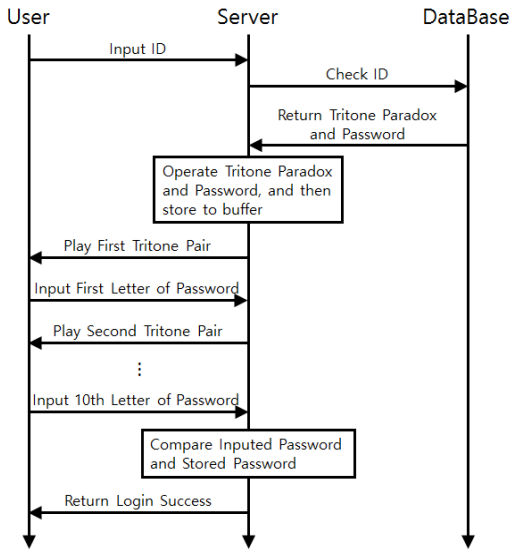


Fig. 14. Process of main password authentication protocol

가입 할 때 답했던 것과 같이 트라이톤 패러독스를 일관되게 듣고 원래의 비밀번호를 앞서 말한 방식대로 변경하여 입력하였다면 로그인은 성공하게 된다.

Fig. 14.는 트라이톤 패러독스를 응용한 주 패스워드 인증 프로토콜을 보여준다. 이러한 인증 과정에서 공격자가 사용자의 비밀을 훔치기 위해서는 사용자가 입력한 비밀뿐만 아니라 사용자가 들은 트라이톤, 그리고 사용자와 동일한 트라이톤의 해석 능력이 요구된다. 따라서 키로깅, 어깨너머 훔쳐보기, 무작위 대입 등의 공격이 어려워진다.

4.2 보조 수단으로서의 트라이톤 인증 프로토콜

트라이톤 패러독스는 앞서 제시한 주 패스워드 인증 프로토콜 외에도 다양한 인증 프로토콜에 적용되어 사용될 수 있다. 다음은 사용자가 비밀번호를 분실한 경우, 사용자를 인증하기 위한 보조 수단으로서의 트라이톤 인증 프로토콜을 적용하는 방법에 대해 설명한다.

Fig. 15.는 비밀번호 보조 수단으로서의 트라이톤사용자 인증 프로토콜을 보여준다. 사용자는 서버에 가입할 때 회원 정보, 아이디, 비밀번호, 이메일과 서로 다른 다섯 개의 트라이톤 시나리오에 대한 응답을 서버에 등록한다. 하나의 트라이톤 시나리오는 임의의 길이를 가질 수 있으며, 이 논문에서는 그 길이를 10이라고 가정한다.

사용자가 비밀번호를 분실한 경우, 비밀번호 찾기 화면으로 이동하여 자신의 아이디와 회원가입시 등록했던 이메일 정보를 함께 입력한다. 서버는 사용자가 입력한 아이디를 검색하여 회원 정보를 조회하고, 입력한 이메일 정보가 등록되어있는 이메일 정보와 일치하는 경우 회원가입시 입력했던 다섯 개의 트라이톤 시나리오 중 한 시나리오를 무작위로 선택하여 사용자에게 들려준다. 사용자의 응답이 회원가입시 입력한 응답과 일치하는 경우 서버는 사용자에게 비밀번호를 이메일로 전송하는 등의 방법으로 알려준다.

현재 많은 국내 웹사이트는 비밀번호 찾기 질문/답변 등을 이용한 2차 패스워드를 이용한다. 예를 들면, 회원가입 시 '자신의 보물 제 1호는?' 같은 질문을 주고 사용자는 그것의 답을 패스워드 찾을 때 이용한다. 이와 같은 2차 패스워드는 공격자가 사용자와 친분이 있는 경우 쉽게 공격당할 수 있다. 하지만 트라이톤 패러독스를 이용한 인증 방법을 이용한다면, 공격자가 트라이톤 시나리오를 듣고 사용자와

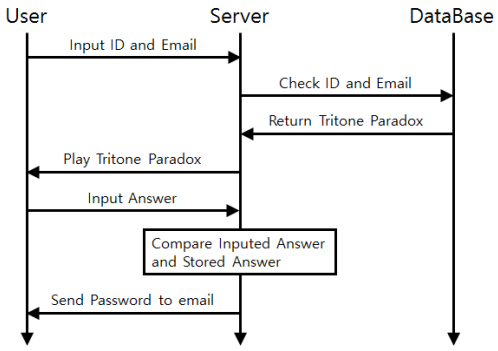


Fig. 15. Process of authentication protocol by using tritone paradox for finding password

같은 판단을 내릴 수 있는 능력이 있어야 하는데, 이는 쉽지 않다. 게다가 사용할 때마다 입력하는 답이 달라지므로 기존에 사용하는 2차패스워드 보다 보안성이 향상될 수 있다.

V. 결 론

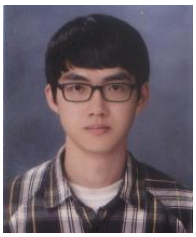
트라이톤 패러독스는 어떠한 트라이톤 관계에 있는 연음을 사람마다 다르게 들을 수 있는 현상이다. 이 논문에서는 트라이톤 패러독스를 이용한 청각 생체인증에 대하여 그 가능성을 고찰하고 응용 프로토콜을 제안하였다. 트라이톤 패러독스와 결합한 비밀번호 입력 프로토콜은 적용한다면, 사용자는 비밀번호를 입력할 때마다 다른 비밀번호를 입력하게 되어 키로깅, 어깨너머 훔쳐보기, 무작위 대입 등의 공격을 방어할 수 있을 것이다. 또한 스피커를 이용하여 사용자가 트라이톤 패러독스를 듣기만 하면 되기 때문에 별도의 하드웨어를 필요로 하는 다른 생체인증에 비하여 구축비용이 저렴할 것이다. 추후 연구를 통하여 트라이톤 패러독스의 유일성과 일관성을 확보한다면, 이 논문에서 제안하는 방법은 비밀번호 인증뿐만 아니라 PC 인증, 스마트폰 인증, 금융 인증, 다중 생체인증[9] 등의 다양한 범위에 적용될 수 있을 것으로 기대된다.

References

[1] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, "Impact of Artificial "Gummy" Fingers on Fingerprint Systems," Proceedings of

SPIE, Vol. 4677, pp. 275-289, Apr. 2002.
〔2〕 R.A. Virginia, T.G. Pedro, A.F. Fernando, G. Javier, F. Julian and O.G. Javier, "Direct Attacks Using Fake Images in Iris Verification," Lecture Notes in Computer Science, Vol. 5372, pp. 181-190, 2008.
〔3〕 K. Cho, "A Legislative Study on the Protection of Biometric Information," Korean Public Law Association, Vol. 37, No. 1-2, pp. 181-200, Oct. 2008.
〔4〕 S. Kim, "A Study on Authentication Technics Using Biometrics," Master Thesis, Graduate School of Hanyang University, Feb. 2006.
〔5〕 G. Yadav and C. Kant, "Biometric Security: A Grand Challenge," International journal of Computer Science & Communication, Vol. 4, No. 2, pp. 27-31, Sep. 2013.
〔6〕 W. Eom and I. Jeon, "Development for Reliability Quality and Performance Evaluate Model of Fingerprint Recognition System," Journal of Korea Contents Association, Vol. 11, No. 2, pp. 79-87, Feb. 2011.
〔7〕 A.K. Jain, K. Nandakumar and A. Nagar, "Biometric Template Security," EURASIP Journal on Advances in Signal Processing, Vol. 2008, No. 113, Jan. 2008.
〔8〕 B. Lee, "A Study on the High-speed Iris Recognition System," Master Thesis, Graduate School of Kyung Hee University, Aug. 2011.
〔9〕 D. Moon, S. Jung, T. Kim, Y. Chung and K. Moon, "An Watermarking Algorithm for Multimodal Biometric Systems," Korea Institute of Information Security and Cryptology, Vol. 15, No, 4, pp. 93-100, Aug. 2005.
〔10〕 D. Nyang, A. Mohaisen and J. Kang, "Keylogging-resistant Visual Authentication Protocols," Transactions on Mobile Computing, Vol. 1, No. 8, pp. 2566-2579, Nov. 2014.
〔11〕 R. Plamondon and G. Lorette, "Automatic Signature Verification And Writer Identification - The State Of The Art," Pattern Recognition, Vol. 22, No. 2, pp. 107-131, 1989.
〔12〕 D. Deutsch, "A Musical Paradox," Music Perception, Vol. 3, No. 3, pp. 275-280, 1986.
〔13〕 D. Deutsch, "The Tritone Paradox: An Influence of Language on Music Perception," Music Perception, 8, pp. 335-347, 1991.
〔14〕 W. Suh and B. Hong, "The tritone paradox : Its presence and form of distribution in Korean people," Psychological Science, Vol. 7, No. 1, pp. 65-74, 1998.

〈저자소개〉



정 창 훈 (Changhoon Jung) 학생회원
2014년 9월~현재: 인하대학교 컴퓨터정보공학과 석사과정
〈관심분야〉 정보보호, 인증프로토콜, 생체인증, HCI

신 동 오 (DongOh Shin) 학생회원
2010년 2월: 인하대학교 컴퓨터정보공학과 학사
2012년 2월: 인하대학교 컴퓨터정보공학과 석사
2012년 9월~현재: 인하대학교 컴퓨터 정보공학과 박사과정
〈관심분야〉 인터넷 보안, 네트워크 보안, 금융 보안

양 대 헌 (DaeHun Nyang) 종신회원
1994년 2월: 한국과학기술원 과학기술대학 전기 및 전자공학과 학사
1996년 2월: 연세대학교 컴퓨터과학과 석사
2000년 8월: 연세대학교 컴퓨터과학과 박사
2000년 9월~2003년 2월: 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재: 인하대학교 컴퓨터정보공학과 교수
〈관심분야〉 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안

이 경 희 (KyungHee Lee) 정회원
1993년 2월: 연세대학교 컴퓨터과학과 학사
1998년 8월: 연세대학교 컴퓨터과학과 석사
2004년 2월: 연세대학교 컴퓨터과학과 박사
1993년 1월~1996년 5월: LG소프트(주) 연구원
2000년 12월~2005년 2월: 한국전자통신연구원 선임연구원
2005년 3월~현재: 수원대학교 전기공학과 부교수
〈관심분야〉 바이오인식, 정보보호, 컴퓨터비전, 인공지능, 패턴인식