액추에이터를 활용한 사용자 인증 모듈 연구

서희석*, 김상연*, 윤인호**

요약

현재 다양한 휴대용 기기가 출시되면서 이를 활용해 업무를 처리할 수 있는 스마트워크가 보편화 되었다. 스마트워크의 경우 외부 원격지에서 회사 내부의 자원을 활용할 수 있기 때문에 정당한 사용자를 확인 할 수 있는 사용자 인증이 중요한 요소이다. 일반적으로 사용되는 사용자 인증으로는 사용자의 ID와 패스워드를 이용하는 방법이 있다. ID/PW를 이용한 사용자 인증은 인증정보를 사용자가 눈으로 보고 입력해야 한다. 이러한 사용자 시각에 의존한 사용자 인증의 경우 사용자가 인증 정보를 입력과정에서 훔쳐보기를 통한 패스워드 유출 위협이 존재한다.

본 연구에서는 훔쳐보기 위협에 대응하기 위해 액추에이터를 활용한 패스워드 입력 모듈을 설계하고 제작하였다. 액추에이터를 이용하여 사용자의 촉각을 통해 정보를 전달하고, 사용자로부터 입력을 받을 수 있다.

A Study on the User Authentication Module using Actuator

Hee-Suk Seo*, Sang-Youn Kim*, In-Ho Yun**

ABSTRACT

Today, a wide range of portable devices is released, it can handle tasks utilizing 'smart work' was a commonplace. In the case of smart work from a remote location outside the company's internal resources can be utilized. Smart work is an important element in the user authentication. Generally, user authentication, the user's ID and password is to use. These user authentication, the authentication information input by the user in the process of peeking through the password is leaked threat.

In this study, in order to respond to shoulder surfing attacks actuator utilizing the password input module is designed and manufactured. Actuators via the user's sense of touch to convey information, the information can be entered.

Key Words : Authentication, Password System, Actuator, Mobile, Haptic

* 한국기술교육대학교 컴퓨터공학부 교수 (✉histone@kut.ac.kr)

** 한국기술교육대학교 대학원 컴퓨터공학과 석·박사과정

· 제1저자(First Author) : 서희석 · 교신저자(Correspondent Author) : 김상연

· 접수일(2013년 7월 18일), 수정일(1차 : 2013년 8월 2일), 게재확정일(2013년 8월 8일)

Ⅰ. 서 론

인터넷을 활용하는 사용자의 증가와 컴퓨터 보급의 확대로 정보 보호의 중요성이 크게 대두되고 있다. 사용자 정보를 보호하기 위한 가장 기본적인 방법으로 사용자 인증이 있다. 사용자 인증이란 사용자가 제시한 신분의 타당성을 확인하는 절차로 사용자가 특정 시스템이나 자원에 접근을 허용할지 여부를 판단하는 중요한 지표가 된다[1]. 사용자 인증 방법으로는 크게 3가지 유형으로 이루어진다[2].

가장 기본적인 방법은 사용자가 알고 있는 지식을 기반으로 사용자를 인증하는 유형으로 대표적으로 사용자 ID/PW가 있다. 사용자가 알고 있는 ID/PW를 시스템에 저장한 ID/PW와 비교하여 시스템에 접근한 사용자의 신뢰성을 확보하는 방법이다.

다음 유형으로는 사용자가 소유하고 있는 것을 사용자 인증 매체로 활용하는 방법이다. 대표적인 인증 매체로는 스마트카드[3], OTP 장치를 들 수 있다.

마지막 사용자 인증 유형으로는 사용자의 신체 일부분을 이용하여 사용자의 신분을 사용하는 방법으로 사용자의 목소리, 홍채 등을 활용하여 사용자를 인증하는 방법이다.

사용자 인증을 다중으로 수행할수록 보안성은 높아지지만, 사용자가 불편함을 호소할 수 있다.

물리적인 장소에 출입을 통제하기 위해서 사용되는 사용자 인증의 경우 발급이 간편한 보안카드를 통해 사용자 인증을 수행한다. 물리적 시설에 대한 사용자 인증 방법으로 사용자의 신체의 일부를 활용하는 방법이 보안적인 측면에서 우수하지만 사용자의 생체 정보를 활용하기 때문에 관리적인 측면과 인증 장비, 관리비용 등의 금전적인 측면에서 효율적이지 못하기 때문에 잘 사용되지 않는다.

본 연구에서는 사용자가 알고 있는 정보와 사용자가 가지고 있는 매체를 활용하여 사용자의 촉각을 통해 정보를 제공하여 사용자를 인증할 수 있는 방법을 연구하였다. 기존의 액추에이터는 모바일에 적용하기 어려워[4] 모바일에 적합한 솔레노이드 타입의 리니어 액추에이터 제작하고, 제시한 액추에이터를 이용하여 사용자에게 특정 숫자를 제시하면 사용자가 알고 있는 PW에 맞게 입력을 받아 사용자 인증을 수행하는 모듈을 제작하였다.

Ⅱ. 관련연구

2.1 바이오 보안 토큰을 이용한 사용자 인증

바이오 보안 토큰을 이용한 프라이버시 보호형 사용자 인증 기법[5] 연구에서는 바이오 보안 토큰을 이용한 사용자 인증 기법을 제안하고 있다. 바이오 보안 토큰은 바이오 인식 센서와 바이오 인식 정보를 처리할 수 있는 MCU, 보안토큰으로 구성된 USB 형태의 하드웨어 기기를 통해 사용자 인증을 수행한다. 사용자 인증 시 바이오 인식 센서로부터 취득한 바이오 인식정보와 저장되어 있는 바이오인식 정보를 보안토큰 내부 MCU에서 매칭을 통해 사용자 인증을 수행한다.

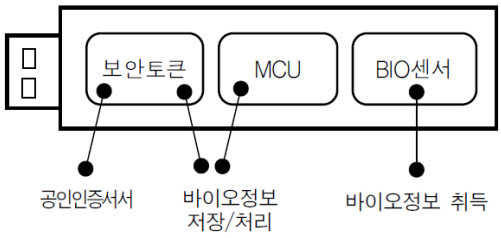

그림 1. 바이오 보안토큰의 구성
Fig. 1. The composition of bio-security tokens

바이오 보안 토큰을 이용한 사용자 인증 연구에서는 바이오 보안 토큰과 공인인증서의 연계 모델을 제시하고 있다. 하지만 바이오인식 정보는 개인을 고유하게 식별할 수 있는 개인정보이기 때문에 이에 대한

프라이버시 침해 우려로 인해 적용상의 제한이 존재한다. 또한 보안 토큰이 USB 형태로 제작되어 분실 우려가 존재한다.

2.2 음성 정보를 이용한 일회용 패스워드

스마트폰에서 음성 정보를 이용한 일회용 패스워드 기반 사용자 인증 메커니즘 설계 및 구현 연구[6]에서는 인증을 수행하는 사용자의 음성 정보를 이용하여 사용자 인증 방법을 제시하고 있다

스마트폰의 필수 요소인 마이크를 이용하여 사용자 인증에 사용될 수 있는 일회용 패스워드를 생성하는 메커니즘을 <그림 2>와 같이 설계하였다. 스마트폰의 마이크를 이용하여 사용자의 음성 정보를 취득한다. 취득한 사용자 음성정보는 서버에서 사용자의 음성 정보에 대한 검증을 수행한다. 공격자가 사용자의 음성 정보를 미리 획득하여 사용자 인증에 사용하는 것을 막기 위해서 인증에 사용되는 음성 정보는 서버로부터 수신 받은 PIN번호를 사용하여 안정성을 확보하였다.

사용자의 음성 정보를 이용하는 경우 주변 소음에 의해 취약할 수 있다는 단점이 존재한다. 따라서 음성

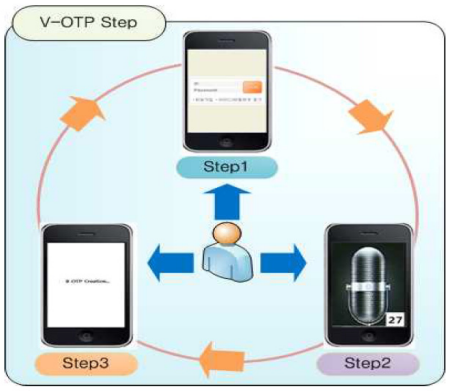

그림 2. 음성 정보를 이용한 OTP 생성
Fig. 2. OTP generation using voice information

정보를 취득하는 과정에서 주변 소음으로 인해 잘못된 음성 정보를 취득하게 되어 사용자 인증에 실패할 수 있다. 또한 사용자의 억양으로 인해서 서버에서 음성 정보를 올바르게 분석하지 못할 수 있다.

2.3 멀티터치 패스워드

멀티터치 환경에서의 다중 입력을 통한 패스워드 기반의 사용자 인증 기법[7] 연구에서 멀티터치를 활용한 패스워드 입력 방법을 제안하였다.

현재 많이 사용되고 있는 숫자 4자리 패스워드 입력은 0000 ~ 9999까지 10000개의 패스워드 범위를 가지고 있다. 이러한 방법은 전사 공격을 통해서 패스워드를 크래킹 할 수 있다는 단점이 존재 한다. 이러한 단점을 보완하기 위해서 '멀티터치 환경에서의 다중 입력을 통한 패스워드 기반의 사용자 인증 기법' 논문에서는 멀티 터치를 활용하여 <그림 3>과 같이 동시에 여러 개의 숫자를 사용자로부터 입력받아 사용자 인증을 수행한다. 기존의 싱글터치 패스워드 입력에 비해 입력의 복잡성을 높여 사용자의 패스워드를 추측/유추하기 어렵도록 설계하였다.

그림 3. 멀티터치 패스워드 시스템
Fig. 3. Multi-touch password System

2.4 필름형 햅틱 액추에이터

셀룰로오스 기반 필름형 햅틱 액추에이터 특성연구[8]에서는 휴대용 기기에 사용이 적합한 셀룰로오스

아세테이트 햅틱 액추에이터를 제안하고 있다.

필름형 햅틱 액추에이터를 제작하기 위해 셀룰로오스 아세테이트를 사용하여 2.5*5*0.1cm크기의 햅틱 액추에이터를 <그림 4>와 같은 구조로 제작 하고, 모바일 기기에 적용될 상황을 가정하여 제안한 액추에이터의 성능평가를 실시하고 Adhesive tape 지지대를 사용이 가장 좋다는 결과를 얻었다.

셀룰로오스 아세테이트를 사용하여 햅틱 액추에이터를 얇게 개발하였다. 기존에 액추에이터에 비해서 얇게 제작할 수 있는 장점으로 인해서 휴대용 모바일 기기를 적용이 용이하며 햅틱 감각을제공하여 휴대용 기기에 몰입감을 높일 수 있을 거라고 제시하고 있다.

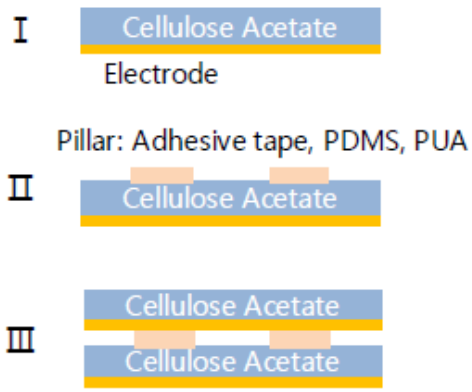

그림 4. 셀룰로오스 아세테이트 햅틱 액추에이터
Fig. 4. Fabrication of haptic actuator

III. 액추에이터를 활용한 패스워드 입력 모듈

3.1 액추에이터를 활용한 패스워드 입력 모듈 개요

일반적인 4자리 PIN 방식의 패스워드는 사용자가 패스워드 입력 부분에 제시된 숫자를 보고 패스워드를 입력한다. 이러한 방식의 패스워드 입력 방식은 사용자의 시각에 하게 된다. 사용자의 시각에 의존한 패스워드 입력 방식은 사용자가 패스워드를 입력하는 과정을 옆에서 훔쳐볼 수가 있다는 취약점이 존재한다.

본 연구에서는 이러한 사용자의 시각에 의존적인 패스워드 입력 모듈의 단점을 보완하기 위해 사용자의 시각이 아닌 촉각을 이용한 패스워드 입력 모듈을 제안한다. 사용자에게 촉각을 제공하기 위해한 방법으로 액추에이터를 활용한다.

사용자는 시각이 아닌 촉각을 통해서 패스워드에 사용된 숫자들을 제공받고 자신이 설정한 패스워드 숫자인 경우 액추에이터를 눌러 패스워드를 입력하게 된다. 이러한 촉각을 이용한 패스워드 입력 방식은 사용자가 패스워드를 입력하는 과정을 타인이 훔쳐보더라도 현재 액추에이터가 제시한 패스워드가 무엇인지 알 수 없어 훔쳐보기 공격에 강력하게 대응할 수 있다.

액추에이터가 사용자에게 제시하는 숫자를 순서를 각 자릿수를 입력할 때마다 다르게 제시하도록 설계하였다. 출력되는 숫자의 순서를 다르게 함으로써 사용자가 특정 숫자를 입력하는 시간을 불규칙하게 할 수 있다. 사용자에게 제시하는 숫자의 순서를 동일하게 할 경우 사용자가 패스워드를 입력하는데 소요되는 시간의 관찰하여 사용자가 입력하는 패스워드를 유추해 낼 수 있는 취약점을 해결할 수 있다.

3.2 슬레노이드 타입의 액추에이터

제안된 솔레노이드 타입의 리니어 액추에이터는 조립이 용이하도록 원통형의 구조로 개발되었다. 액추에이터의 외각을 담당하는 1개의 비 자성체 하우징(Stainless Housing)과 자속(Magnetic Flux)의 이동경로(Path)를 담당하는 스틸하우징(Steel Housing), 그리고 액추에이터 구동의 원동력이 되는 솔레노이드 코일(Solenoid Coil), 솔레노이드 코일을 고정시키고 도선을 밖에서 연결할 수 있도록 설계되어 있는 스틸커

버(Steel Cover), 스틸하우징 안에서 코일에 인가된 전류에 따라 위 아래로 상하운동을 하는 스틸플런저(Steel Plunger)로 구성된다.

제안된 액추에이터를 사용하여 <그림 5>과 같이 패스워드 입력 모듈을 구성하였다. 2*3 액추에이터 2개를 결합하여 4*3 Array 타입의 액추에이터를 구성하였다.

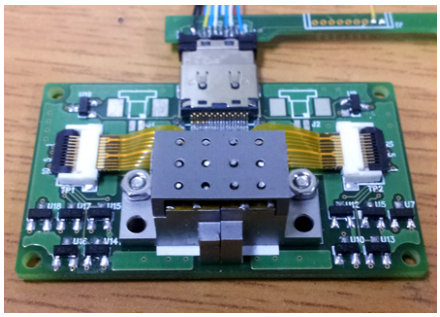

그림 5. 4*3 Array 타입의 액추에이터
Fig. 5. 4*3 Array-type actuator

액추에이터가 상하 운동할 때 레이저 변위센서를 사용하여 거리를 측정하여, 제작한 액추에이터 모듈이 사람의 임계치보다 높은 변위를 가짐을 확인하였다.

3.3 액추에이터 모듈의 구성

액추에이터의 조립의 용이성을 확보하기 위해서 분리하여 조립하였으며 실제 조립이 완성된 액추에이터는 12개의 핀이 각각 독립적으로 제어 가능하며, 각각의 핀들이 각자 다른 주파수로 동작 가능하다. 따라서 12개의 핀을 통해서 숫자 이외에도 문자, 도형, 점자의 사용이 가능하며, 상황에 따라 패스워드로 사용되는 문자의 수를 증가시켜 보안성을 높일 수 있다.

액추에이터의 크기를 15.4mm*9.2mm로 제작하여 <그림 6>과 같이 액추에이터 모듈을 케이스형태로 제작이 가능하다. 액추에이터의 크기를 소형화를 통해 모바일 기기에 적용이 용이하며, 기존에 보급된 모바일 기기에 케이스형태로 제작이 가능하다. 액추에이터의 소형화 및 모듈화를 통해 액추에이터를 활용한 패스워드 입력 모듈을 도입하기 소요될 수 있는 금전적 부담을 감소시킬 수 있다.

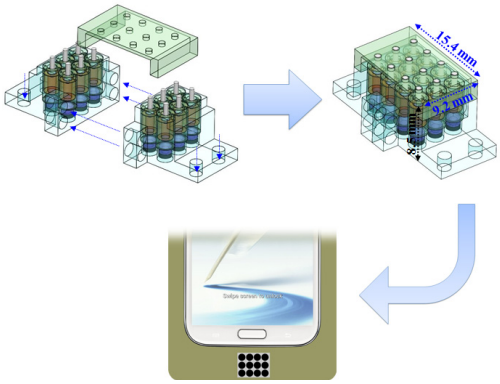

그림 6. 액추에이터 입력 모듈 구성
Fig. 6. Actuator Input Module Configuration

3.4 액추에이터를 활용한 패스워드 입력 모듈 구성

액추에이터를 활용한 패스워드 입력 모듈의 구성은 12개의 액추에이터를 제어하기 위한 <그림 7>과 같이 액추에이터 제어부, 사용자에게 제시할 숫자의 순서를 정하는 숫자 순서부, 그리고 사용자의 입력을 인식하는 인식부로 3부분으로 구성되어 있다.

액추에이터를 제어하는 액추에이터 제어부는 12개의 핀을 독립적으로 제어하기 위해서 각각의 액추에이터에 대한 정보와 액추에이터의 배열 정보를 가지고 있으며 사용자에게 제시하는 숫자의 순서를 정하는 숫자 순서부에서 정한 숫자 순서를 참조하여 액추에이터를 제어한다.

숫자 순서를 정하는 순서부에서는 사용자가 패스워드를 입력과정에서 훔쳐보기를 통해서 패스워드를 입력하는데 걸리는 시간을 유추하여 패스워드를 알아낼

수 있는 위협이 존재한다. 패스워드 유추 위협을 제거하기 위해서 각 단위마다 사용자에게 제시되는 숫자의 순서를 불규칙하기 위해 사용된다.

사용자 입력 인식부에서는 사용자의 입력 여부를 판단한다. 사용자의 입력여부를 판단하기 위해 액추에이터가 이동한 거리의 변화를 측정한다. 인식부는 사용자가 입력한 값을 저장하여 인증 시스템에 전달하는 역할을 수행한다.

그림 7. 액추에이터를 활용한 패스워드 입력 모듈 구성
Fig. 7. The actuator consists of a password input module

3.5 액추에이터 패스워드 입력 모듈을 활용한 사용자 인증 과정

솔레노이드 타입의 리니어 액추에이터로 제작한 4*3 Array 타입의 액추에이터를 활용하여 제작된 패스워드 입력 모듈은 설계하였다. 설계한 액추에이터는 사용자 인증을 위해서 사용자가 패스워드를 입력하는 과정에 활용된다. 사용자 인증을 요구하는 시스템은 액추에이터로 랜덤한 숫자를 출력하도록 요구한다. 액추에이터를 시스템으로부터 제공받은 숫자를 사용자가 인지할 수 있도록 각각의 액추에이터를 동작 시킨다.

사용자는 액추에이터로 제공받은 숫자를 인지하여 사용자가 설정한 패스워드인 경우 액추에이터를 눌러 패스워드 입력을 수행한다. <그림 8>은 액추에이터를 활용한 패스워드 입력 모듈을 통해서 사용자 인증을 수행하는 과정을 도식화 하였다.

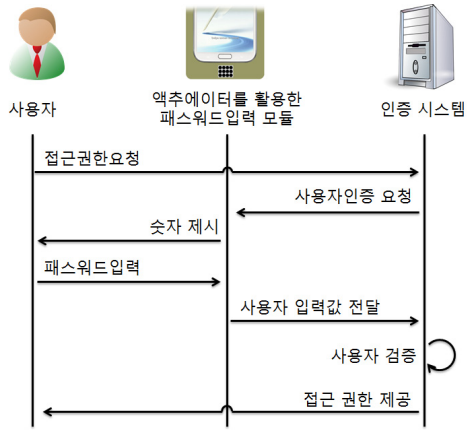

그림 8. 액추에이터 패스워드 입력 모듈을 활용한 사용자 인증 과정
Fig. 8. Actuator utilizing user authentication a password input module courses

사용자가 시스템에 특정 자원 혹은 권한을 요청하면 시스템은 사용자 인증을 수행하기 위해서 패스워드 모듈을 활용하게 된다. 패스워드 모듈은 사용자가 숫자를 인지할 수 있도록 액추에이터를 동작 시킨다. 이때에 사용자에게 전달하는 숫자를 랜덤하게 제공하여 사용자가 특정 숫자를 입력할 때 소요되는 시간을 불규칙하게 제시하여 보안성을 강화하였다.

사용자는 액추에이터로 제공받은 숫자를 인지하여 사전에 사용자가 설정한 패스워드에 맞게 액추에이터를 눌러 패스워드 입력을 수행한다.

액추에이터 패스우드 입력 모듈은 사용자로부터 입

력받은 패스워드를 시스템에 전달하고, 시스템은 전달 받은 패스워드를 활용하여 사용자 인증을 수행한다. 사용자 인증에 성공하면 시스템은 사용자가 요구한 접근권한을 사용자에게 부여하여 시스템의 자원을 사용하거나 권한을 획득 할 수 있다.

Ⅳ. 결 론

본 연구에서는 액추에이터를 활용한 패스워드 입력 모듈을 제작하고 성능평가를 실시하였다. 기존의 사용자 인증에 주로 사용되는 패스워드 연구들은 사용자의 시각에 의존한 형태의 연구가 주를 이루고 있다. 이러한 연구들은 일반인에게는 매우 유용하지만, 신체가 불편한 사용자에게는 적용하기 어렵다는 점과 패스워드 입력과정에서 발생 할 수 있는 훔쳐보기 공격에 매우 취약한 단점이 존재한다. 본 연구에서는 액추에이터를 활용하여 패스워드 입력과정에서 발생할 수 있는 훔쳐보기 공격에 강한 보안성을 확보하였다. 또한 액추에이터가 사용자에게 제시하는 숫자의 순서를 매번 변경하여 사용자가 숫자를 입력하는 시간을 불규칙하였다. 사용자가 숫자를 입력하는 시간을 변경함으로써 패스워드를 입력하는데 소요되는 시간을 측정해 패스워드를 유출 할 수 있는 위협을 제거하다.

액추에이터를 활용한 패스워드 입력 모듈은 모바일 기기에서 사용 가능할 수 있는 크기로 제작되었다. 모바일 기기 이외에도 ATM, 도어락 등 다양한 기기에 적용이 가능하다. 이는 기존의 패스워드를 통한 사용자 인증 방법에 적용이 가능하다.

본 연구에서는 기존에 주로 연구되던 시각에 기반한 패스워드 입력 방법이 아닌 사용자의 촉각을 활용한 패스워드를 입력 모듈을 연구하였다. 본 연구를 시작으로 사람의 다양한 감각을 활용한 패스워드 입력 방법에 대한 연구가 활발히 진행되었으면 한다.

참고문헌

[1] Anita K. Jones, “Password Authentication with Insecure Communication”, Communications of the ACM, vo.24, no.11, 1981, pp.770-772

[2] Robert Morris, Ken Thompson, “Password security: a case history”, Communications of the ACM, vol 22 no11, 1979.

[3] Hyun Seok Kim, Ju Bae Kim Yeon Oh Jeong Keun Hee Han, Jin Young Choi, “Formal Analysis of Authentication System based on Password using Smart Card”, Journal of KIISE : Computer Systems and Theory, vol.36, no.4, 2009, pp. 304-310

[4] Wang, Q., and Hayward, V., “Compact, Portable, Modular, High-performance, Distributed Tactile Transducer Device Based on Lateral Skin Deformation,” 2006 Symp. on Haptic Interfaces for Virtual Environment and Teleoperator Systems IEEE VR, Arlington, VA, 67-72, March, 2006.

[5] Yong Nyuo Shin, Myung Geun Chun “A Privacy Preserving User Authentication Using Biometric Hardware Security Module”, Journal of KISSC vol.22, no.2, 2012, pp.347-355.

[6] Sik Wan Cho, Hyung Woo Lee, “Design and Implementation of Voice One-Time Password(V-OTP) based User Authentication Mechanism on Smart Phone”, The KIPS Transactions:PartC, vol.18C, no.2, 2011, pp.79-88

[7] Seung hwan Ju, Hee Suk Seo, “Password Based User Authentication Methodology Using Multi-Input on Multi-Touch Environment”, Journal of KSS, vol.20, no.1, 2011, pp. 39-49

[8] K. B. Kim · J. kim · S. Y. kim, G. Y. Yun, “Characterization of cellulose based film type haptic actuator”, Conference of KSPE, 2012, pp.15-16

감사의 글

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2010- 0021951).

본 연구는 한국기술교육대학교 지능융합클러스터의 지원으로 수행된 연구임.

저자소개

서희석(Hee Suk Seo)

2000년 성균관대학교 산업공학과 학사
2002년 성균관대학교대학원 전기전자 및 컴퓨터공학과 석사
2005년 성균관대학교대학원 전기전자 및 컴퓨터공학과 박사

2005년～현재 한국기술교육대학교 컴퓨터공학부 교수
※ 관심분야 : 모델링&시뮬레이션, 네트워크보안, 보안 시뮬레이션, USN

김상연(Sang Youn Kim)

1997년 KAIST 자동화 및 설계공학 (공학석사)
2002년 ~ 2003년 가상현실 연구센터 연구원
2005년 KAIST 기계공학 (공학박사)
2005년 ~2006년 삼성종합기술원 책임연구원

2007년～현재 한국기술교육대학교 컴퓨터공학부 교수
※ 관심분야 : Haptic Rendering, Tactile Display, Virtual Reality, HCI

윤인호(In Ho Yun)

2012 한국기술교육대학교 컴퓨터공학부 (공학사)

2012~ 현재 한국기술교육대학교 석박사과정
※ 관심분야 : Haptic, MR Fluid, Miniature kinaesthetic Actuator