키로깅 방지를 위한 가상키보드 시스템

백금옥[1], 임철호[2], 손진곤[3]

A Virtual Keyboard System for Preventing Keylogging

Geum Ok Baik[1], Cheol Ho Lim[2], Jin Gon Shon[3]

요 약

웹 서비스에서 개인인증을 받기 위해 사용자가 입력하는 개인정보들은 키로거(key logger)등의 해킹 툴에 의해 수집되어 다양한 방식으로 악용될 수 있다. 이러한 문제점을 해결하기 위해 그동안 다양한 방법들이 제시되었고, 그 중 대표적인 방법이 가상키보드 방법으로 마우스를 이용하여 문자를 입력함으로써 키로깅을 근본적으로 차단하는 방법이다. 그런데 현재 주로 사용되는 가상키보드는 문자를 임의로 배열함으로써 가독성이 떨어져 입력시간이 지연되는 단점이 있다. 본 논문에서는 순차적인 문자배열을 유지하면서도 회전이 가능한 회전형 가상키보드 시스템(R-VKS ; Rotary-type Virtual Keyboard System)을 제안한다. R-VKS는 시각적 추상화를 기반으로 하여 설계되고 구현되었다. R-VKS는 훔쳐보기(shoulder surfing) 공격에 대한 한계는 완벽하게 극복하지 못하였지만 기존의 가상키보드보다 입력속도를 향상시켜 사용자의 편의성을 증진시켰다는데 의의가 있다.

핵심어 : 키로깅 방지, 가상키보드, 시각적 추상화, 회전형 가상키보드 시스템

Abstract

When a user of web services needs to be authenticated, he or she has to provide personal information usually by typing into given blank fields on the web. The personal information can be captured by some hacking tools, such as key logger program, and used improperly and maliciously. Various ways have been suggested to solve such a problem of leaking personal information. The typical example is a virtual keyboard that a number or a character is input only by a mouse instead of a real keyboard, resulting in blocking such a hacking risk basically. The most popular virtual keyboard is an array of numbers and/or characters randomly allocated by a random number generator. However, the numbers and/or characters allocated by random cannot provide readability rather than a sequential array so that input time of user is delayed. In this paper, a Rotary-type Virtual Keyboard System (R-VKS) based on visual abstraction theory has been suggested to overcome this weakness and to maintain appropriate levels of security. The proposed R-VKS has improved user friendliness by rising input speed, whereas it does not completely overcome the limitation of shoulder surfing attacks.

Keywords: keylogging prevention, a virtual keyboard, visual abstraction

접수일(2010년05월01일), 심사의뢰일(2010년05월02일), 심사완료일(1차:2010년05월16일, 2차:2010년05월31일)

게재일(2010년08월31일)

[1]110-791 서울시 종로구 동숭동 169, 한국방송통신대학교 평생대학원 정보과학과.
email: whitegoldruby@hanmail.net

[2]110-791 서울시 종로구 동숭동 169, 한국방송통신대학교 평생대학원 정보과학과.
email: point289@nate.com

[3](교신저자)110-791 서울시 종로구 동숭동 169, 한국방송통신대학교 컴퓨터과학부 교수.
email: jgshon@knou.ac.kr

1. 서론

정보통신의 발달과 인터넷 서비스의 보편화로 각종 웹서비스를 통한 전자상거래가 보편화되고 있는 추세이다. 이러한 대부분의 상용화된 웹서비스들을 이용하기 위해서는 각 사이트에서 구축한 사용자 인증시스템을 통하여 개인인증을 필요로 한다. 아이디나 비밀번호, 주민등록번호 등의 개인인증을 위한 정보들이 웹서버로 전송되는 네트워크 구간에서는 공개키기반구조(PKI; Public Key Infrastructure)나 보안소켓레이어(SSL; Secure Sockets Layer)를 통해 암호화하기 때문에 그 구간에서 시도되는 각종 해킹 시도를 무력화할 수 있다. 하지만 정보가 전송되기 직전 구간에서의 사용자의 PC 내에 이미 설치된 키로거와 같은 해킹 툴에 대해서는 사용자의 프라이버시와 정보들이 무방비로 노출될 위험이 있다[1]. 사용자가 키보드를 누를 때마다 키 입력값을 받아 특정파일에 저장해 놓는 기능을 하고 있는 키로거는 획득한 정보를 네트워크를 통한 실시간 전송, FTP 전송, 메일 발송, 메신저 전송 등의 방법을 통하여 해커에게 개인 정보를 전달한다[2]. 그 결과 개인 정보와 자산의 유출, 범죄행위에 도용될 수 있다. 이러한 위험성에 대처하고자 각종 백신과 보안 솔루션이 등장하고 있으나 신종 키로거와 같은 해킹 툴에 대해서는 원천적인 방지책이 되지 못한다.

이에 키보드로 입력되는 각종 키로거 공격에 대비하여 우회적인 방법으로 키보드 입력값 탈취를 원천적으로 방지하고자 하는 다양한 방법들이 제안되었다[3]. 이러한 노력들 중의 하나가 가상키보드를 이용하여 마우스만으로 정보를 입력하는 기술이다. 기존의 가상키보드에 의한 입력방식은 무작위로 배열된 숫자나 문자를 마우스로 입력하기 때문에 사용자의 가독성이 떨어져 입력시간이 지연된다는 단점이 있다. 따라서 본 논문에서는 숫자나 문자를 순차적으로 배열하여 사용자가 쉽게 인식할 수 있는 시각적 추상화 방법을 기반으로 하는 가상키보드를 제안하고, 이를 구현한다.

2. 관련연구

2.1 기존의 가상키보드시스템

가상키보드로 입력되는 정보에는 사용자 아이디나 비밀번호, 주민등록번호, 공인인증서 비밀번호, 계좌번호, 계좌 비밀번호 등이 있고, 본 논문에서는 비밀번호 입력을 위주로 하여 설명하고자 한다. [그림 1]의 (a)는 사용자가 비밀번호 생성과정에서 제공되는 사람 얼굴 이미지 중에서 자신의 비밀번호에 해당하는 얼굴 이미지를 기억하고 있다가 비밀번호를 조합 구성한다[4]. [그림 1]의 (b)는 1차 로그인을 한 상태에서 추가 인증을 위한 2차 비밀번호 입력 폼이다[5]. [그림 1]의 (c)는 우측 상단에 위치한 옵션의 선택에 따라 '무작위 배열' 또는 현재 보편적으로 쓰이고 있는 쿼티(QWERTY) 자판 배열과 유사한 '기본 배열' 간의 선택을 전환할 수 있다. 따라서 '무작위 배열'로 배열 변경을 했을 경우 무작위로 변환된 키 배열을 제공받는다[6]. [그림 1]의 (d)는 비밀번호 입력 시 마우스로 상단의 키보드를 누르면 아래 텍스트박스 부분에 아스트리크(*)로 비밀번호가 표시된다. 이것을 마우스로 드래그하여 복사한 후 원래의 비밀번호 입력 박스에 붙여 넣어 사용한다[7].

(a) 국외 P사 (b) 국내 N사

(c) 국내 E사

(d) 국외 A사

[그림 1] 가상키보드의 예

[Fig. 1] Examples of virtual keyboards

이미지 기반 가상키보드는 무차별 대입 공격(brute force attack)이나 사전 공격(dictionary attack)에 대하여 강인하지만[8], [그림 1]의 (a)는 얼굴인식불능증(prosopagnosia)의 경우를 고려하지 못하였다. 또한 텍스트 기반에서는 비밀번호를 특수문자로 감출 수 있지만, 이미지 비밀번호는 입력이 완료된 시점에서 훔쳐보기(shoulder surfing)나 자동 캡쳐 프로그램 등으로부터 안전하지 않다. 또한 문자로 비밀번호를 입력하는 전통적인 시스템과의 호환이나 이식 용이성이 떨어진다. 그 외 일반적으로 쓰이는 텍스트 기반 가상키보드 방식의 순차배열은 사용자에게 익숙하지만 비밀번호가 노출될 수 있는 위험성이 커지는 단점이 있고, 무작위 배열은 보안성은 높아지나 사용이 불편하여 입력시간이 지연된다는 단점이 있다. 본 논문에서는 이러한 단점을 보완하여 보안 단계를 높이면서도 사용자 편의성을 고려한 시각적 추상화 기반의 회전형 가상키보드시스템인 R-VKS를 제안한다.

2.2 시각적 추상화

시각적 추상화(Visual Abstraction)란 실제의 사물과 현상에서 핵심적이며 중요한 것을 추출하고 기억하며 활용하는 인간 고유의 능력을 말한다. 인간은 반복된 경험과 학습을 통해 사물이나 이미지에 대한 정보가 기억 속에 추상화된 어떤 형식으로 잠재되어 있다. 즉, 시각적으로 나타나는 구체적인 현상들이 인간의 지적인 능력과 결합하여 보다 간단하고 유용하고 보편적이면서 구분이 가능한 어떤 시각적 추상 형태로 다시 표현되는 것이다[9]. 시각적 추상 형태는 즉시성이 있고 직관적으로 수용되기 때문에 내용과 형식을 동시에 잘 알 수 있게 한다. 또, 시각적 추상 형태는 유사성에 기반을 둔 아날로그적인 경향이 있고, 범위를 형성하여 연속적인 의사소통이 가능하게 된다. 따라서 시각적 체계는 디지털보다는 아날로그적인 경향이 있고 여러 가지의 메시지를 동시적・직

관적으로 전달할 수 있으므로 사고 없이 행해지는 '자동반응'을 불러일으킬 수 있는 구조적 속성을 가진다[10]. 이러한 이론적 배경은 무작위한 문자 배열에 비해 반복된 경험과 학습으로 추상화된 순차적인 문자 배열이 동시적·직관적으로 파악하기 쉽다는 것을 의미한다. 게슈탈트 시지각 이론과 메타포는 이러한 시각적 추상화의 일환으로서 R-VKS의 순차배열 구조, 그룹별 분할 구조, 회전형 타원 구조의 설계에 적용이 되었다.

2.2.1 게슈탈트 시지각 이론

인간은 환경의 자극에 대해 감각 기관을 통해 반응하며, 특히 시각이 전체의 80% 이상을 차지한다. 인간은 어떤 형태를 마주하게 될 때 우선적으로 형태의 1차적인 특성을 관찰하고 그 형태나 모양에 기초하여 선형인지 도형인지의 구별, 각의 유무와 각의 정도 등 기초적인 기하학적 정보를 받아들인다. 그 후에는 이전에 경험한 적이 있거나 유사한 형태, 혹은 이미 인지하고 있는 사물들과 연관하여 그 형태를 판단하기 시작한다[11]. 이러한 지각이론에 기초한 형태 심리학은 일반 대중을 상대로 하는 기호나 빠른 판단을 요구하는 아이콘, 웹 사이트의 레이아웃, 출판디자인과 교육심리학, 도로 표지판이나 기업의 심벌, 빠른 시간 안에 정확히 주제와 정보를 전달해야 하는 포스터 등에 응용되고 있다.

특히 게슈탈트 시지각 이론의 그룹핑 원리는 사람들이 형태를 지각할 때 개개 단위가 공통적인 특성을 가지고 있으면 이들 중 유사한 시각요소들을 가지고 있는 것끼리 그룹을 짓거나, 좀 더 가까이에 있는 두 개 이상의 시각 요소들을 하나의 그룹으로 인식하려는 경향을 갖는다는 것이다. 이는 인터페이스 설계에 있어서 주목성과 가독성을 높일 수 있는 근거가 된다. 나아가 사용자에게 정보를 전달하고자 할 때 명백하고 일관성 있는 개념적 구조를 제공하게 되어 무질서와 혼란을 방지할 수 있다[12]. 그룹핑의 원리에는 근접성의 법칙, 유사성의 법칙, 연속성의 법칙 등이 있다.

2.2.2 메타포

메타포의 사전적 의미는 은유라는 희랍어 ‘metaphor'에서 왔다. 이 말은 '넘기다'라는 의미의 'meta'와 '가져가다'라는 의미의 'pherein'에서 유래 되었다. 한 사물의 양상이 다른 하나의 사물로 '넘겨 가져가'지거나 옮겨져서 두 번째의 사물이 마치 첫 번째의 사물을 표현하는 것처럼 의미 상징으로 이해한다. 이와 같이 메타포란 다른 대상의 특징을 통해 특정 대상을 이해하거나 경험하는 행위라고 정의할 수 있다[13]. 메타포는 이와 같이 원천 영역과 목표 영역이라는 두 개의 영역을 연결시키는 행위라고 할 수 있다. 원천 영역이란 이미 사람들이 잘 알고 있고 익숙한 영역이다. 예를 들어 책상이라는 영역이나 책이라는 영역은 우리가 실생활에서 이미 오랜 기간 동안 사용해 왔기 때문에 일반적으로 크기는 얼마나 되고 어떻게 사용하는지와 같은 특성에 대하여 잘 알고 있다. 한편 목표 영역이란 사람들이 아직 잘 알고 있지 못하고 익숙하지 않은 영역이다. 따라서 목표 영역은 새로운 시스템이나 콘텐츠처럼 사람들에게 익숙하지 않은 개념이다. 메타포라는 것은 이와 같이 하나의 익숙한 개념을 이용하여 또 다른 새로운 개념을 이해하기 위하여 서로 다른 영역을 연결하는 것이라고 할 수 있다[14].

3. R-VKS의 설계와 구현

3.1 R-VKS의 설계

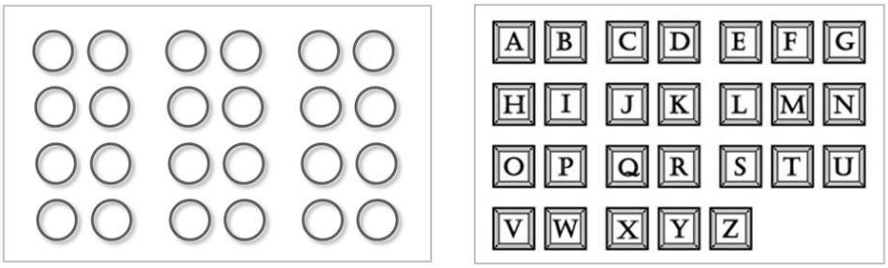
3.1.1 게슈탈트 시지각 이론의 적용

본 논문에서 제안한 R-VKS는 형태 심리학의 대표적 이론인 게슈탈트의 시지각 이론 중 그룹핑의 원리를 중점적으로 응용한다. 그룹핑의 원리란 사람들이 형태를 지각할 때 개개 단위가 공통적인 특성을 가지고 있으면, 이들 중 유사한 시각 요소들을 가지고 있는 것끼리 그룹을 지어 보려고 하는 경향이다. R-VKS는 다양한 그룹핑의 원리 중 근접성의 법칙, 유사성의 법칙, 연속성의 법칙을 적용하여 설계하였다.

(1) 근접성의 법칙(law of proximity)과 적용

근접성의 법칙은 [그림 2]의 (a)에서 보는 바와 같이 보다 더 가까이에 있는 두 개 또는 그 이상의 시각 요소들을 패턴이나 그룹으로 보려고 한다는 법칙으로서 유사한 대상들이 물리적 세계에서 가까이 있으면, 이들을 지각적으로 함께 묶으려는 경향이다. 이것은 여러 가지의 시각 개체를 제시했을 때 어떤 연관성을 이해하여 정리되고 이해되는 상태로 정보를 수용하려는 효율적 정보 수용의 형태를 말한다. [그림 2]의 (a) 경우는 구분선도 없고, 도형의 색상과 모양이 동일한데도 위치상 간격을 기준으로 하여 근접한 요소들끼리 자연스럽게 그룹이 지어진다. R-VKS에서는 이를 응용하여 기존의 가상키보드와 같은 무작위 배열이 아닌 순차적 배열 구조로 설계되었다.

이는 무작위 배열의 경우 각 문자는 앞 뒤 요소에 대한 아무런 정보도 가지고 있지 않은데 비해 순차적 배열에서의 모든 개별적인 문자들은 기준 문자의 좌우에 오름차순 또는 내림차순에 따른 '앞' 또는 '뒤'라는 정보를 갖고 있다는 것을 의미한다. 따라서 R-VKS는 기준이 되는 문자와 좌우에 인접한 문자들과의 의미적인 근접성을 통해 다른 의미 그룹들과의 차별성을 가지게 된다.



(a) 근접성의 법칙 (b) 순차적 배열 구조

[그림 2] 근접성의 법칙과 적용

[Fig. 2] The law of proximity and its application

또한 [그림 2]의 (b)는 일반적으로 많이 알려진 영어권 국가의 동요인 'alphabet song'에 근거하여 운율에 맞게 한 행 내에서 2열, 2열, 3열씩의 위치 구분을 하였다. 이는 기존의 경험과 학습에 의하여 무의식적으로 익숙해져 있었던 운율이 인간의 시각 지능, 공간 감각과 융합하여 위치 탐색을 직관적으로 할 수 있게 하는 효과가 있다.

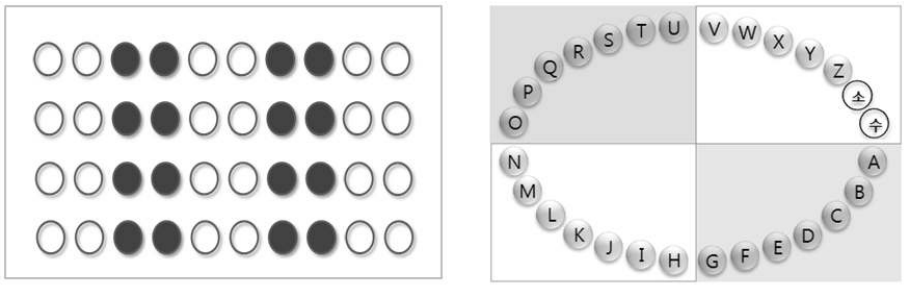
만일 [그림 2]의 (b)가 무작위로 배열되었고 서로가 같은 간격을 유지하였다면 일반적으로 순차적인 탐색을 하게 되고, 선택하는 문자를 찾을 때까지 인간의 기본적인 시각적 흐름성에 준하여 상단 좌측으로부터 우측 방향으로 문자를 읽다가 행의 끝을 만나면 다시 행을 바꿔 다음 행의 좌측 시작점에서부터 다시 우측 방향으로 판독을 하게 된다. 따라서 시각적인 탐색과 판독의 과정을 거치는 단계가 많아질수록 소요되는 시간도 누적되어 인지적 부담(cognitive load)을 가중시킨다는 것을 알 수 있다. 이에 반해 순차적인 배열 구조에서의 각 문자는 근접한 요소에 대한 정보를 포함하고 있으므로 선택하고자 하는 문자의 위치 추정이 가능하게 되어 순차 탐색이 아닌 이진 탐색이나 직접 탐색을 하게 되므로, 탐색에 따른 시간이 무작위 배열일 경우보다 적게 소요된다.

이에 근거하여 R-VKS는 기존의 가상키보드가 가졌던 무작위 배열과는 다르게 순차적 배열을 유지하도록 설계되었다. R-VKS는 기존의 가상키보드에서의 무작위 배열보다 사용자의 탐색 소요 시간을 줄여 주면서도 악성 코드로부터의 안전성을 확보할 수 있다. 이러한 R-VKS의 순차 배열 구조의 각 숫자나 문자는 순차 배열로 인한 오름차순이나 내림차순의 일정한 방향성을 내포하고 있다. 각 숫자나 문자가 가진 인접한 좌우문자에 대한 정보는 사용자로 하여금 직관적으로 선택하고자 하는 숫자나 문자를 찾아갈 수 있도록 한다.

(2) 유사성의 법칙(law of similarity)과 적용

유사성의 법칙은 [그림 3]의 (a)에서와 같이 모양, 크기, 색상, 의미에 있어서 유사한 시각 요소들끼리 연관 짓고 그룹핑 하여 패턴으로 보려는 경향이다. 즉, 유사한 자극들을 하나로 집단화 하려는 경향을 유사성으로 설명할 수 있다. 형태, 색, 방향의 연관성을 이해한다는 것은 기존의 조형 이해도와 관련이 있는 것이다. 기존의 4×3 배열이나 키보드 타입의 가상키보드는 무작위 배열이기 때문에 특정한 통일성을 기한다는 것이 기능적 개선의 관점에서는 의미가 없었다. 하지만 R-VKS에 적용된 유사성은 숫자와 영문 대문자, 영문 소문자를 분리하여 배열하였고, 기능버튼 두 개를 포함한 28개의 버튼을 4개의 그룹으로 분리하여 각각의 색상을 다르게 구분하였다. 이러한 구분은 3.1.1절에서 설명한 'alphabet song'의 운율로 인해 잠재된 학습효과가 인간의 시지각과 협응하여 공간적 메타포를 형성하게 한다.

따라서 [그림 3]의 (b)에서 보는 바와 같이 유사성을 가지는 요소들끼리 그룹을 지어 색상 구분을 하여 배열함으로서 타 그룹과의 신속한 구별력을 제공해 준다. 영어 소문자 배열일 경우에도 [그림 3]의 (b)와 동일한 형태를 가지고 있으며, 숫자 배열일 경우에는 영문자 배열과의 버튼 위치와 간격을 동일하게 유지하고자 숫자 두 벌을 반복하여 배치하였고, 특수문자를 포함하여 28개의 버튼을 사용하였다. 이와 같이 R-VKS는 유사성의 법칙을 적용하여 인간의 시지각에 의한 공간 분할 능력을 최대한 활용할 수 있게 설계되었다.



(a) 유사성의 법칙 (b) 그룹별 분할 구조

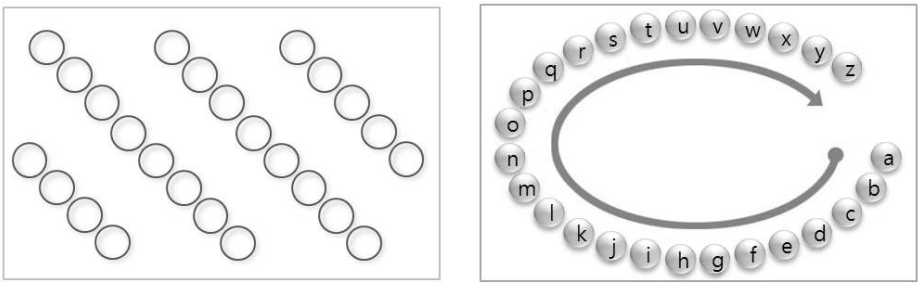
[그림 3] 유사성의 법칙과 적용

[Fig. 3] The law of similarity and its Application

(3) 연속성의 법칙(law of continuation)과 적용

연속성의 법칙은 [그림 4]의 (a)에서 보는 바와 같이 시각적 요소들이 일정한 방향으로 연속적이거나 곡선을 형성하기 위해 집단화 하려는 경향을 말한다. 인간은 대상을 인지할 때 그 안에서 일관된 반복을 찾아내고 일정한 체계를 추출하여 단절과 공백까지 전체적인 구조의 일부로 파악하게 함으로써 이를 하나의 연속적인 대상으로 지각하게 된다. R-VKS는 [그림 4]의 (b)와 같이 타원구조의 순차 배열이므로 시선의 흐름에 있어서 단절이나 공백이 없으며, 인간의 자연스러운 시각적인 경로에 일관된 흐름을 제시하며 회전이 되더라도 연속적인 흐름에 흐트러짐이 없다.

기존의 4×3 배열이나 키보드 타입의 가상키보드는 행렬구조이므로 행의 시작과 끝에서의 개방형 구조로 인해 시선 경로가 다음 행으로 이어지기 위해서는 공백의 구간이 형성될 수밖에 없었다. 그러나 R-VKS는 [그림 4]의 (b)와 같이 배열 전환을 위한 기능 버튼 2개를 포함하여 연속적인 하나의 곡선으로 이루어져 있고, 한 문자가 입력될 때마다 랜덤 함수에 의해 버튼들이 곡선 경로를 따라 회전이 되므로 시선 경로의 단절이 생기지 않는다. 또한 기존의 4×3 배열이나 키보드 타입의 가상키보드는 무작위 배열이므로 순차 탐색을 하기 위해 연속적인 시각 경로가 형성되더라도 [그림 4]의 (b)와 같이 각 문자의 그룹과 좌우 문자에 대한 근접 정보를 가지면서 연속적인 시각 경로를 형성하는 것은 아니다.



(a) 연속성의 법칙 (b) 회전형 타원 구조

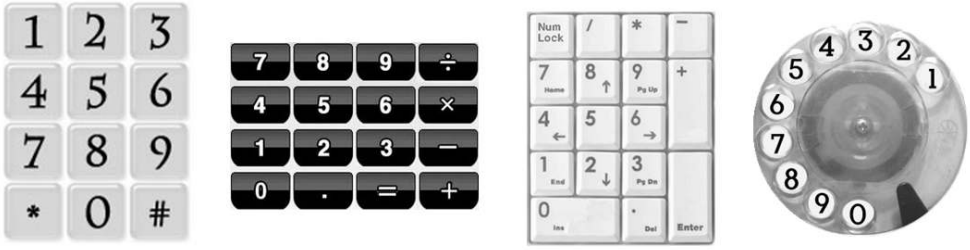
[그림 4] 연속성의 법칙과 적용

[Fig. 4] The law of continuation and its Application

3.1.2 메타포의 적용

문서 작성이나 필기, 독서 등 텍스트에 대한 정보를 습득할 때 일부 경우를 제외하고는 보통 인간의 시각적 흐름은 기본적으로 좌측에서부터 우측으로, 또는 상단에서부터 하단으로 향하며 이는 시각적 우선순위와 밀접한 관련이 있다[15]. 시각적 흐름에 영향을 주는 요소에는 색상의 강도, 레이아웃 형태로 다양화 될 수 있으나, 텍스트만 있는 단조로운 페이지를 접했을 때는 보편적으로 본능적인 시각적 흐름에 따르게 된다. 이는 단순히 10개의 숫자를 나열하는 경우나 26개의 영문자를 나열하는 경우에도 해당되기에 되도록 1열 횡대의 형태로 배치되는 것이 자연스럽다.

그러나 실생활의 다양한 기기에 숫자나 문자가 배열되는 경우 공간적 한계에 충실하거나 기능적 면에서의 효율성을 추구하고자 다양한 공간적 분할을 적용하여 변형적으로 배치하는 경우가 있다. 하지만 이런 경우에도 탐색 소요시간과 가독성을 위하여 계산기나 키보드, 전화기 등 일반적으로 사용되는 잘 알려진 배치 방법들이 있으며 [그림 5]는 실생활에서 다양하게 접할 수 있는 숫자 배열의 구성 방법에 대한 예들이다.



(a) 버튼식 전화기 (b) 계산기 (c) 키보드 숫자패드 (d) 다이얼식 전화기

[그림 5] 숫자 배열의 구성 예

[Fig. 5] Examples of number layout structure

[그림 5]의 (a)는 행렬 구조로서 상단 좌측으로부터의 오름차순으로 구성되었고, (b)와 (c)도 역시 행렬 구조이긴 하지만 (a)와는 반대의 방향인 하단 좌측으로부터의 오름차순으로 구성되어져 있다. (d)는 원형 구조로서 반시계 방향으로의 오름차순으로 구성되어져 있다. 숫자 배열을 표현하는데 있어서 이런 다양한 배치 형태가 존재하지만 사용자는 이러한 제품을 특별한 학습과정을 거치지 않아도 순차적인 배열이라는 것과 배열의 방향성을 파악하는 순간 별 무리 없이 사용이 가능하다.

이것은 사용자들이 익숙한 사용감에 잘 인지하지 못하고 있을지라도 사실은 텍스트 기반의 공간적 메타포(spatial metaphor)를 적용하고 있는 경우라 할 수 있겠다. 공간적 메타포란 일반적인 메타포의 의미를 확장한 것으로 인간의 공간적 감각과 상식을 그대로 디자인에 적용하여, 별다른 안내 설명이나 지침이 필요 없이 직관적으로 사용할 수 있어서 실수나 오류를 줄일 수 있는 경우를 일컫는다. 따라서 나열된 숫자들을 탐색해야 할 경우 처음 시작점에서부터 시각적으로 스캔(판독)하는 과정 없이도 직관적인 구역 분할에 의하여 효과적인 탐색을 할 수 있다.

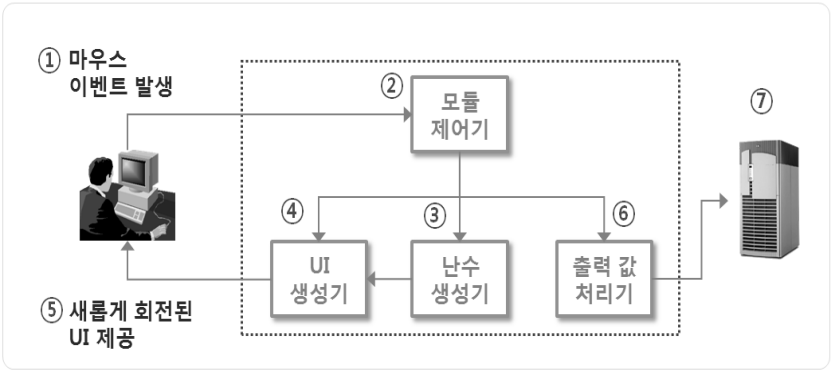
[그림 5]의 예들은 각 경우의 기능적 요구사항에 따라 숫자 배치가 모두 다른 형태로 구성되어져 있지만 시각적 추상화를 기반으로 응집되고 그룹핑 되어 있어서 사용자가 용이하게 인지할 수 있고, 즉시적이며 직관적으로 방향의 연관성을 이해할 수 있다. 즉, 정형화된 공간에서 각각의 경우에 따라 인간의 공간 지각능력과 결합하여 보다 보편적이면서 구분이 용이한 공간적 메타포를 형성하게 되는 것이다. 이로써 [그림 5]에서와 같이 방향성이 서로 다른 경우라도 사용자는 반복과 학습 과정을 통해 이미 형성된 시각적 추상화를 기반으로 각각의 경우를 별다른 거부감 없이 직관적으로 인식할 수 있다.

즉, 입력하고자 하는 숫자와 다양한 입력시스템에서의 해당 숫자를 매핑 시켜 선택하는 협응 능력은 인간이 가지고 있는 공간 감각이 물리적인 공간 배치에 대한 구조를 우선적으로 파악함으로써 가능한 것이다. 또한 탐색하고자 하는 숫자 좌우에서 정렬의 연관성이 강한 근접 숫자에 대한 응집적 단서를 동시에 획득함으로써 가능한 것이다.

이를 기초로 하여 순차적인 배열로 설계한 R-VKS는 사용자가 이미 학습과 경험을 통해 익숙해진 공간적 메타포를 기반으로 숫자나 문자에 대하여 즉각적이며 직관적인 공간 분할을 하게 한다. 그리고 탐색하고자 하는 숫자나 문자에 직접적으로 접근할 수 있게 하는 것이다. 이는 사용자의 입장에서 무작위 배열로 인한 인지적 부담을 현저히 경감시키는 효과가 있고, 그 결과 사용 편의성을 증대시킬 수 있다는 것을 의미한다.

3.2 시스템 구성과 동작 원리

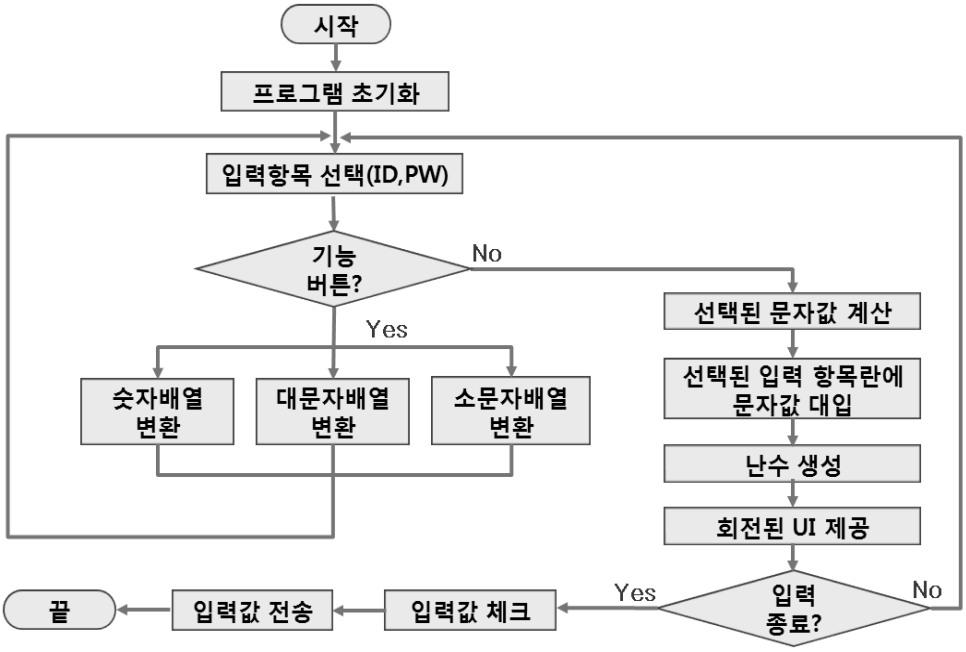
R-VKS는 [그림 6]과 같이 난수 생성, UI 생성, 출력값 처리 등 세 개의 모듈과 이 세 개의 서브 모듈을 제어, 관리하는 상위 모듈인 모듈 제어기로 구성되었으며, Windows XP 환경에서 개발도구인 Delphi 6.0 Enterprise를 사용하여 구현되었다. 테스트 환경은 UNIX(HP-UX 11.23) 기반의 Jeus 6.0 웹서버로 구성하였고, 서버와의 통신은 이더넷(TCP/IP)을 사용하였다.



[그림 6] R-VKS의 구성

[Fig. 6] The system structure of the R-VKS

R-VKS의 동작에 따른 처리 흐름은 [그림 7]과 같다. 즉, 사용자가 개인 인증을 필요로 하는 웹 서비스에 접속했을 때 아이디나 비밀번호를 입력하는 마우스 이벤트가 발생하고(①), 그에 따라 모듈 제어기는 난수 생성기와 UI 생성기와 출력값 처리의 구동 순서와 조합 여부를 결정한다(②). 문자나 기능 버튼을 누르면 난수 생성기는 UI 생성기에 전달할 난수를 생성하고(③), 그에 따라 UI 생성기는 회전된 새로운 UI 좌표의 기준값을 넘겨받아 사용자에게 보여주고자 하는 UI의 포맷을 결정하고(④), UI 생성기는 새롭게 회전된 UI를 사용자에게 제공하여 준다(⑤). 출력값 처리기는 마우스 이벤트의 입력값에 따라 매핑 된 사용자의 아이디나 비밀번호의 값을 외부 모듈로 넘겨주는 인터페이스를 처리한다(⑥). 확인 버튼을 누르면 입력값이 외부 서버로 전송되어 진다(⑦).



[그림 7] R-VKS의 처리 흐름도

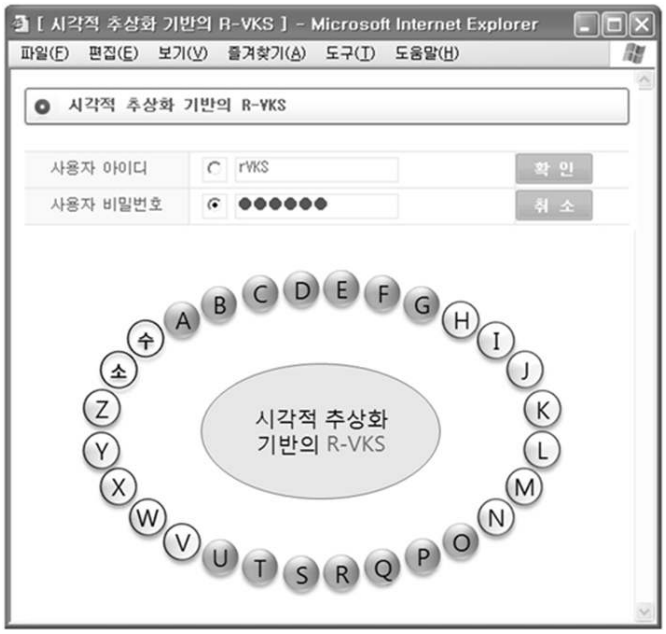
[Fig. 7] The Flowchart of the R-VKS

3.3 R-VKS의 구현

아이디와 비밀번호로 개인인증을 하는 웹 사이트 중에서 R-VKS가 적용된 웹 사이트에 접속하면 [그림 8]과 같은 화면이 R-VKS의 초기 인터페이스로서 나타난다. 키보드를 이용한 기존의 방식은 해당 텍스트 박스에 커서를 위치시켜 아이디와 비밀번호에 해당되는 키보드의 입력값을 직접 눌러 입력하는 방식이다. 반면 마우스를 이용한 입력 방식은 주로 가상키보드가 화면 위에 팝업 창 형태로 띄워진 상태에서 해당 값을 찾아서 입력하는 방식이다. 기존의 문자 배열 가상키보드 방식은

2.1절에서 설명한 것처럼 주로 숫자와 영문자가 혼합되어 배치되어 있는 키보드형의 가상키보드와 숫자와 영어 소문자, 영어 대문자를 분리하여 4×3 배열에 무작위로 배열해 놓는 방식인 4×3 배열 가상키보드 방식이 주로 쓰였다. 본 논문에서 제안하는 R-VKS는 기존의 가상키보드의 일반적인 배열과는 다르게 타원형 구조로 배열되어 있는 형태이고 숫자 배열과 영문자 배열을 분리하여 구성하였다.

[그림 8]은 구현된 R-VKS의 영문 대문자 배열의 인터페이스로서 그 외에 유사하게 구성되어진 숫자 배열, 영문 소문자 배열 중에서 무작위로 초기화면에 나타난다. R-VKS에 배열된 영어 대문자는 4그룹으로 나누어져 있으며 각 그룹마다의 차별적인 색상으로써 각 그룹을 구별할 수 있다. 각 그룹에 속한 버튼 수의 동일한 배분을 위하여 배열 전환을 위한 기능버튼을 포함한 28개의 버튼을 7개씩 구별하여 4개의 그룹을 구성하였고, 아이디와 비밀번호 입력을 위한 텍스트 박스는 기존에 사용하는 것과 동일한 형태이다. 이는 영어 소문자 배열이나 숫자 배열에도 유사한 형태로 구성되어 있으며, [그림 8]에서와 같이 "수(숫자 배열)" 버튼 또는 "소(영어 소문자 배열)" 버튼을 통하여 각 배열간의 전환을 할 수 있다.



[그림 8] R-VKS의 인터페이스

[Fig. 8] A snapshot of the R-VKS interface

실제로 아이디와 비밀번호의 구성에 필요한 숫자 버튼과 영문 대·소문자 버튼을 제외한 각각의 기능 버튼에 대한 설명은 [표 1]과 같다.

[표 1] R-VKS의 기능 버튼 설명
[Table 1] Explanation of function buttons in the R-VKS

버튼 명	기능 버튼 설명
확인	입력된 사용자의 아이디나 비밀번호의 전송 처리
취소	기 입력된 아이디나 비밀번호의 입력 취소 처리
수	문자 배열을 숫자 배열로 전환
대	문자 배열을 영문 대문자 배열로 전환
소	문자 배열을 영문 소문자 배열로 전환

또한 R-VKS는 한 문자를 입력할 때마다 배열이 무작위로 회전을 하여 배열구조가 전환된 형태로 사용자에게 보여 진다. 그리고 사용자의 다음 입력값을 전달 받을 준비를 한다. 그리고 사용자의 아이디나 비밀번호의 입력이 끝날 때까지 이 과정은 반복된다. 회전하는 반경의 폭은 매번 무작위한 각도만큼 회전이 되므로 현재 보여 지는 배열의 이전 배열을 예측할 수도 없고, 이후의 배열에 대한 예측도 불가능하다. 하지만 숫자나 문자로의 배열 변환이 일어나거나 랜덤 함수에 의하여 회전을 하게 되더라도 순차적으로 배열되어 있는 형태는 그대로 유지하게 된다.

아이디와 비밀번호 입력을 위한 텍스트 박스는 기존에 사용하는 것과 동일한 형태로 구성되어 있다. 확인 버튼은 텍스트 박스에 입력된 아이디와 비밀번호를 사용자 인증을 위하여 서버로 전송하며, 취소 버튼은 텍스트 박스에 입력된 아이디와 비밀번호를 삭제해 주는 기능을 하고 있다.

4. 비교 분석 및 결론

데이터가 키 값의 순서에 관계없이 무순서로 연속해서 저장되어 있는 경우에 일반적으로 순차 탐색(sequential search)을 사용한다. 순차 탐색은 서로 이웃한 데이터를 차례차례로 탐색키를 비교하면서 탐색한다. 크기가 n인 리스트에서 존재하지 않는 탐색키를 찾는 시간은 n번의 탐색키 비교 연산 후에야 찾고자 하는 키가 없다는 것을 알 수 있다. 크기가 n인 선형 리스트에서 원소들의 키 값이 주어진 키 값과 같을 확률이 $1/n$로 모두 같다고 할 때 임의의 위치 k에서 탐색키를 찾는데 k번 비교 연산이 필요하며, 평균 비교 횟수는 식(1)과 같고 최악의 경우 $O(n)$의 시간복잡도를 가진다[16].

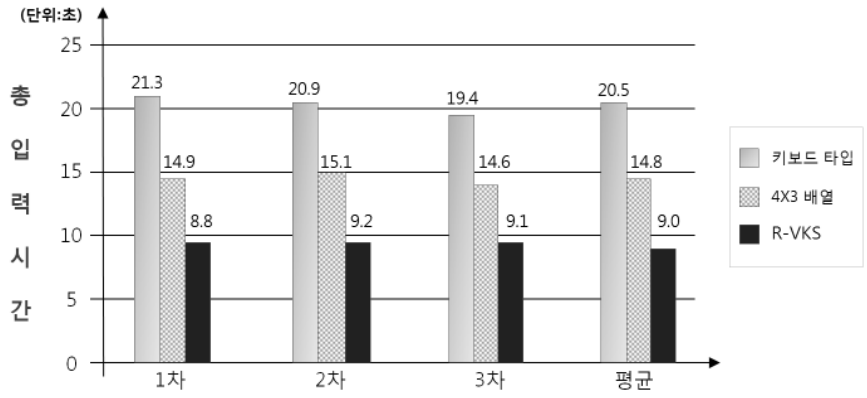
$$\sum_{k=1}^{n} k\frac{1}{n} = \frac{n+1}{2} \tag{1}$$

무작위로 배열된 데이터를 별도의 인덱스 된 정보 없이 탐색할 때에는 무조건 순차적인 탐색을 이용해야 한다. 이에 비하여 전화번호부에서처럼 모든 데이터가 순차적인 정렬이 되어 있는 경우에는 순차적인 탐색보다 효과적인 이진 탐색(binary search)을 이용하는 것이 좋다. 이진탐색은 주어진 선형 리스트가 연속 공간에 저장되어 있고, 데이터 레코드들이 키 값에 대하여 미리 정렬이 되어 있는 경우에는 탐색 성능이 순차 탐색법보다 낫다. 크기가 n인 정렬된 선형 리스트에서 이진

탐색으로 탐색키를 찾을 때 맨 처음 비교되는 원소는 선형 리스트의 가운데 원소, 즉 $n/2$ 위치에 있는 데이터 레코드의 키와 탐색키가 비교된다. 즉, 이진 검색은 레코드의 키 값에 따라 정렬된 파일의 중앙인 $n/2$번째 레코드의 키 값 Km과 탐색하기 위한 키 값 K를 비교하여, 세 가지 결과인 $K = Km$, $K > Km$, $K < Km$에 따라 해당 부분에 대해 순환적인 검색을 한다. 비교 결과 키가 일치하면 탐색을 끝내고, 만약 탐색키의 값이 데이터 레코드의 키 값보다 작으면 선형 리스트의 전반부에서 탐색하고, 그렇지 않으면 후반부에서 동일한 방법으로 탐색하는 작업을 계속한다. 이진 탐색 과정에서 탐색 대상 데이터 레코드의 수가 1/2씩 줄어들게 되고 결국은 탐색키와 동일한 키 값을 가진 데이터 레코드를 찾게 되든가, 아니면 찾고자 하는 데이터 레코드가 존재하지 않는다는 사실을 알 수 있다. 이진 탐색의 시간복잡도는 $O(\log n)$이다[16].

이 외에도 효과적인 탐색을 위한 방법으로 해싱(hashing)이 있는데, 해싱은 M보다 훨씬 작은 m개의 테이블 공간만을 써서 동적 데이터 집합을 저장하고 접근할 수 있도록 하는 방법이다. 키 값이 1부터 n사이로 n이 그리 크지 않다면, 테이블 $T[1..n]$을 두고 각 키 I의 레코드를 $T[i]$에 저장한다. 이렇게 한다면 모든 키의 레코드는 한 번에 바로 접근할 수 있다. 즉, 해싱은 하나의 문자열을 원래의 것을 상징하는 더 짧은 길이의 값이나 키로 변환하는 것이다. 짧은 해시키를 사용하여 항목을 찾으면 원래의 값을 이용하여 찾는 것보다 더 빠르기 때문에, 해싱은 데이터베이스 내의 항목들을 색인하고 검색하는 데 사용된다. 해싱으로 인덱스를 만들면 검색할 때 시간복잡도가 $O(1)$가 되는 특징을 지닌다.

위에서 열거한 순차 탐색, 이진 탐색, 해시 탐색의 경우의 시간복잡도를 비교해 보면 순차 탐색보다는 이진 탐색이 빠르고, 이진 탐색보다는 해시 탐색이 빠르다는 것을 알 수 있다. 본 논문에서 비교 대상으로 선정한 무작위한 숫자나 문자 배열의 경우에는 순차 탐색 방법만을 사용해서 키 값과 데이터 값을 일일이 비교해야 하는 과정을 거쳐야만 한다. 하지만 순차 배열의 경우에는 순차 탐색을 할 필요가 없으며 이진 탐색이나 해시 탐색을 하게 되더라도 순차 탐색보다 탐색시간을 단축시킬 수 있음을 간접적으로 증명할 수 있다.



[그림 9] 가상키보드 입력시간 비교

[Fig. 9] Comparisons of Input times with virtual keyboards

[그림 9]에서 보는 바와 같이 10자리 문자열에 대해 3차에 걸친 총 가상키보드 입력시간 비교 결과 키보드 타입은 평균 20.5초, 4×3 배열은 14.8초, R-VKS는 9.0초가 소요되었다. 따라서 기존의 키보드 타입 가상키보드에 비해서는 약 56.9% 정도, 4×3 배열 가상키보드에 비해 약 38.5% 정도 단축시켰음을 알 수 있다.

또한 입력해야 할 문자들에 대한 각각의 소요 시간을 구해 평균값을 비교하면 [표 2]에서와 같이 키보드 타입은 2.11초, 4×3 배열은 1.48초, R-VKS의 경우에는 0.91초가 소요되었다. 이를 토대로 최댓값과 최솟값과의 차이인 산포도를 보면 키보드 타입은 0.95초, R-VKS의 경우가 0.17초이므로 5배 이상의 차이를 보인다. 따라서 기존의 키보드 타입과 4×3 배열 가상키보드의 경우는 사용자가 입력하고자 하는 문자를 우연히 발견하는 것에 많은 영향을 받고 있음을 알 수 있고, R-VKS는 사용자의 직관에 의하여 입력하고자 하는 문자를 안정적인 속도로 입력하고 있음을 알 수 있다.

[표 2] 가상키보드 별 한 문자 당 평균 입력시간의 비교 (단위: 초)
[Table 2] Comparison of average input-time per charactor (unit:sec.)

가상키보드	최댓값	최솟값	산포도	평균값
키보드 타입	2.74	1.79	0.95	2.11
4×3 배열	1.93	1.23	0.70	1.48
R-VKS	1.01	0.84	0.17	0.91

본 연구의 향후 과제로는 영문자와 숫자 키패드를 다중 배열함으로써 키패드를 교체하는데 소요되는 시간을 단축할 수 있는 시스템으로의 확장이 가능하다. 그리고 개인정보를 입력할 때 보안 등급을 사용자가 선택할 수 있다면 입력의 신속성과 정보의 보안성 중에 사용자 개인별 선호도를 반영한 가상키보드를 제공할 수 있다.

참고문헌

[1] 이현우, 네트워크 공격기법의 패러다임 변화와 대응방안, Technical Report, p.10, 인터넷침해대응센터, 2001.

[2] 이희조, 임옥희, 김진영, 안티키로거를 이용한 개인정보 보호, Technical Report, pp.7-8, 안철수연구소, 2003.03.

[3] 김영환, 무작위 추출된 숫자 인터페이스를 지원하는 비밀번호 입력 시스템, 전남대학교 대학원 석사학위 논문, 2007.02.

[4] Passfaces Corporation, http://www.passfaces.com. (Accessed in July 2010.)

[5] (주)넥슨, http://maplestory.nexon.com. (Accessed in July 2010.)

[6] (주)이스트소프트, http://www.altools.co.kr/help/altoolbar/16/help.html. (Accessed in July 2010.)

[7] Aplin Software Corporation, http://www.aplin.com.au. (Accessed in July 2010.)

[8] 정태영, 이경률, 임강빈, "키보드해킹에 대비한 새로운 영상기반 패스워드", 정보보호학회지, 제18권 제3호, pp.41-47, 2008.06.

[9] 나일주, 교육공학관련 이론(개정판), 교육과학사, 2010.04.

[10] J. E. Burgoon, "Nonverbal Communication Research in the 1970s : An Overview“, in Communication Year Book 4, (D. Nimmo ed.)", N. J: Transaction Books, New Brunswick, 1980.

[11] 소영희, 연속적 시지각 경험을 기초로 한 경관분석과 환경디자인 적용에 관한 연구, 이화여자대학교 디자인대학원 석사학위 논문, 1999.02.

[12] 정승은, 정유정, 조진경, 장동훈, "게슈탈트 이론에 의한 웹 인터페이스 디자인에 관한 연구", HCI학회, 2001.03.

[13] G. Lakoff, M. Johnson, Metaphors We Live By, University Of Chicago Press, 1980.04.

[14] 김진우, Human Computer Interation 개론, 안그라픽스, 2005.01.

[15] J. Tidwell, 김소영 역, Designing Interfaces:인터페이스 디자인 94가지 패턴, 한빛미디어, 2007.07.

[16] 이지수, 홍영식, 조유근, Algorithm, pp.104-112, 이한출판사, 2006.01.

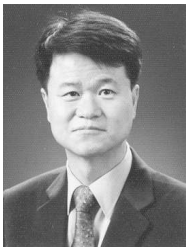
저자 소개

백금옥 (Geum Ok Baik)

2008년 한국방송통신대학교 컴퓨터과학과 이학사
2008년 ~ 현재 : 한국방송통신대학과 정보과학과 석사과정
관심분야 : 정보보호, 유비쿼터스

임철호 (Cheol Ho Lim)

2005년 전자계산학과 이학사
2009년 한국방송통신대학과 정보과학과 이학석사(정보통신)
관심분야 : 정보보호, 유비쿼터스



손진곤 (Jin Gon Shon)

1984년 고려대학교 수학과 이학사
1988년 고려대학교 이학석사(전산학)
1991년 고려대학교 이학박사(전산학)
1991년 ~ 현재 : 한국방송통신대학교 컴퓨터과학과 교수
관심분야 : 컴퓨터통신망, 분산시스템, 정보보호, 시스템모델링, 이러닝