http://dx.doi.org/10.14400/JDC.2014.12.5.231

# 유니버설 디자인에 기반을 둔 새로운 그래픽 패스워드 기법

양기철, 김황용*
목포대학교, 멀티미디어공학과
광주대학교, 작업치료학과*

# A New Graphical Password Scheme Based on Universal Design

**Gi-Chul Yang & Hwangyong Kim***
**Department of Multimedia Engineering, Mokpo National University**
**Department of Occupational Therapy, Gwangju University***

**요 약** 텍스트 기반 패스워드 인증의 문제점을 해결하기 위해서 이미지를 사용하는 그래픽 패스워드가 발전 하였다. 기본적으로 그래픽 패스워드는 화면에 보이는 이미지 위의 정확한 점의 위치를 순서대로 선택(클릭)하여 인증을 처리하는 방식이다. 이러한 기존의 그래픽 패스워드 방식은 화면상의 정확한 지점을 선택하여 클릭하지 못하면 인식에 실패한다. 본 논문에서는 이러한 단점을 개선한 신 개념의 그래픽 패스워드 방식인 PassPositions를 소개한다. PassPositions는 지금까지의 그래픽 패스워드 방식에서 사용하지 않았던 상대위치를 패스워드 생성에 사용한 신개념의 그래픽 패스워드 기법이다. PassPositions는 유니버설 디자인에 기반을 둔 그래픽 패스워드 기법으로 사용자의 신체적 조건에 관계없이 모두가 편리하게 사용할 수 있다.

**주제어** : 그래픽 패스워드, 유니버설 디자인, 정보보호, 개인 식별 시스템

**Abstract** Graphical passwords using images have been developed to solve problems in text based password recognition. The basic recognition process scheme of graphical passwords is clicking certain points on the screen image in correct order. In this pre-developed method of graphical passwords the recognition will fail if the precise positions are not clicked. A new graphical password system called PassPositions is introduced in this paper. PassPositions is a new graphical password scheme which is using relative positions never used earlier graphical password schemes. PassPositions is a graphical password scheme based on universal design that everybody can use conveniently without regarding their physical conditions.

**Key Words :** Graphical Passwords, Universal Design, Information Security, Personal Identification System

## 1. 서론

현대와 같은 정보사회에서는 정보보호의 중요성이 날로 커지고 있다. 정보보호를 위해 필요한 것 중 하나가 정보기기의 보안이며, 정보기기의 보안을 위해서 오늘날 가장 일반적으로 사용되는 것이 비밀번호이다. 비밀번호

Received 17 February 2014, Revised 15 April 2014
Accepted 20 May 2014
Corresponding Author: Hwangyong Kim(Gwangju University)
Email: hkim97@hanmail.net

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

는 숫자만을 사용하거나 숫자와 문자의 조합을 이용하기도 한다. 이러한 인증 기법을 텍스트 기반 인증이라 한다. 텍스트 기반 인증에는 문제점이 있는데, 사용자는 비밀번호를 쉽게 기억할 수 있어야 하지만 다른 사람들은 쉽게 예측할 수 없어야 하는 것이다. 하지만 비밀번호를 쉽게 기억하기 위해서는 비밀번호의 길이가 짧아야하고 그 조합의 의미가 있으면 좋지만 짧고 의미 있는 조합의 비밀번호는 쉽게 도용될 수 있는 것이다. 더욱이 사람들은 비밀번호 입력 시 빠르게 입력하기를 원하고 길이가 긴 비밀번호는 기억하기 어려워 여러 곳(account)의 비밀번호를 같은 것으로 사용하는 경우가 많다[1,2]. 따라서 하나의 비밀번호가 노출되면 다른 여러 곳(account)의 보안도 유지되기 어려워진다.

이러한 텍스트 기반 인증의 문제점을 해결하기 위해서 다양한 방법 들이 개발 되었다. 그 중에는 지문이나 홍채를 인식하는 생체인식 기법[3], 텍스트를 대신하여 이미지를 사용하는 그래픽 패스워드 (Graphical Passwords) 등이 있다. 생체인식 기법은 특수 장치들이 필요하여 시스템 구축비용이 많이 들고 불편하다. 또한 개인의 신체 정보 유출과 같은 문제점이 있다. 반면 그래픽 패스워드[4]는 생체인식 기법에 존재하는 문제점 없이 사용자가 텍스트보다는 쉽게 기억할 수 있는 이미지를 사용하는 인증 기법이다.

현재는 그래픽 패스워드도 여러 가지 방식으로 발전하였으나 기본적으로 화면에 보이는 이미지의 정확한 위치를 순서대로 선택(클릭)하여야 인증이 되는 그래픽 패스워드 방식은 장애인들에게는 또 다른 문제를 야기하였다. 즉 화면상의 정확한 지점을 선택하여 클릭하기가 어려운 사람들이 있는 것이다. 이러한 특정 사람들의 편의를 위한 디자인으로 무장애 디자인(Barrier Free Design)이 있다. 무장애 디자인은 사회적 약자인 고령자나 장애인들의 주거환경 개선을 위한 물리적 장애를 제거한다는 의미로 사용되다가 최근에는 제도적 장애까지 포함한 모든 분야에 걸쳐 적용되고 있다. 유니버설 디자인은 여기서 한발 더 나아가 장애는 물론이고 성별, 연령, 문화 국가 등에 관계없이 누구나 쉽게 사용할 수 있는 제품과 환경을 만들기 위한 디자인 이다. 따라서 유니버설 디자인은 특정 범주의 사람들만을 위한 것이 아니라 어느 누가 사용하여도 편리한 디자인을 창조하는데 목적이 있다. 유니버설 디자인은 1985년 로널드 메이스(Ronald Mace)가 제안한 것으로 공평성, 유연성(사용상의 융통성), 단순성 및 직감성, 쉬운 인지성, 안전성(오류에 대한 포용력), 이용의 효율성(적은 물리적 노력), 그리고 이용이 용이한 크기 및 접근 가능한 공간 등의 7가지 디자인 원칙을 가지고 있다[5]. 따라서 본 논문에서는 기존 그래픽 패스워드의 장점을 살리고 도용가능성도 낮추면서 일반인이나 장애인 모두 쉽게 사용할 수 있는 유니버설 디자인에 기반을 둔 신개념의 그래픽 패스워드인 PassPositions를 소개한다.

이를 위하여 다음 장에서는 그래픽 패스워드 발전과정에서 몇 가지 중요한 그래픽 패스워드 시스템을 알아보고, 3장에서 PassPositions를 자세히 설명한다. PassPositions는 상대적 위치(Relative Position)를 이용하는 일종의 그래픽 패스워드 시스템이다. 그리고 4장에서 결론과 함께 앞으로의 발전 방향에 대하여 논한다.

## 2. 그래픽 패스워드 관련 연구

본 장에서는 그래픽 패스워드에 대한 아이디어가 나오고부터 지금까지 어떤 연구들이 있었고, 어떤 시스템들이 개발 되었는지 알아본다. 기존의 시스템들을 알아봄으로서 본 논문에서 제안하고자 하는 신개념의 인증 시스템 PassPositions가 기존의 시스템들과 어떤 차이점이 있는지를 이해하는데 도움이 될 것이다.

그래픽 패스워드는 사용자들이 쉽게 기억하고, 인증 코드도 텍스트 기반 인증 기법에 비하여 다른 사람들이 알아내기 어려운 인증 기법이다[6]. 그래픽 패스워드는 Blonder의 아이디어[4]가 나온 이후 텍스트 기반 인증 기법을 대체할 수 있는 인증 기법으로 빠른 발전을 보여 왔다. 그래픽 패스워드는 크게 인식 기반 (Recognition-Based) 그래픽 패스워드와 재현 기반(Recall-Based) 그래픽 패스워드로 나눌 수 있다. 먼저 인식 기반 그래픽 패스워드부터 설명하기로 한다.

인식 기반 그래픽 패스워드는 Blonder 방식으로부터 발전 하였다. Blonder 방식의 그래픽 패스워드[4]는 시스템 개발자가 사용될 이미지를 미리 정하고 그 이미지를 특정 구역으로 나누어 놓는다. 이미지에 따라 여러 모양으로 나누어진 이미지의 구역들은 선택 점으로 사용될 수 있다. 사용자는 패스워드를 만들 때 화면상 이미지의

구역들을 순서대로 선택하고, 인증을 위해서는 같은 순서로 같은 구역을 선택하면 된다.

이러한 Blonder 방식의 그래픽 패스워드[4]는 이미지 내의 미리 정해진 구역만을 선택 점으로 사용하여야 되므로 사용자가 개인적인 이미지를 사용할 수 없고 선택점도 임의로 정할 수 없다는 불편한 점이 있다. 즉, 사용자가 선택하고자하는 선택 점이 미리 나누어진 구역과 구역의 경계에 있다면 Blonder 방식의 그래픽 패스워드에서는 이를 선택 점으로 사용할 수 없는 것이다. 이러한 초기의 Blonder 방식의 그래픽 패스워드의 단점을 개선하기 위하여 Wiedenbeck과 그녀의 동료들은 미리 정해진 구역도 없고, 임의의 이미지나 사진을 사용할 수 있는 패스워드 시스템인 PassPoints를 개발 하였다[6,7]. 따라서 PassPoints를 사용하는 사용자는 패스워드를 만들 때 화면상의 그림의 내용과 관계없이 아무 픽셀이나 선택점으로 선택할 수 있고 선택된 픽셀을 중심으로 일정거리에 있는 주변의 픽셀들은 모두 같은 선택 점으로 인정된다. 예를 들어 하나의 선택된 픽셀 주위로 반경 2mm 이내 또는 3mm 이내의 모든 픽셀을 선택 점으로 본다는 것이다. 이때 반경을 크게 잡으면 패스워드가 도용되기 쉽고 작게 잡으면 사용하기 불편할 수 있다. 또한 이미지 내의 구역이 아니라 픽셀을 선택 점으로 사용하기 때문에 화면상의 이미지는 선택 점들을 기억하는데 도움을 주는 역할만 한다. 따라서 미리 정해진 이미지를 사용하지 않아도 되고 자신이 좋아하는 사진이나 그림을 사용할 수 있다. 또한 서로 다른 시스템에서 서로 다른 그림을 사용하여 패스워드의 도용을 방지하는데 도움이 될 수 도 있다. 그럼에도 불구하고 그래픽 패스워드에는 주어진 그림에서 패스워드로 자주 사용될만한 특정 부위가 있기 마련이다. [Fig. 1]은 PassPoints 시스템에서 사용한 하나의 이미지와 선택 점들이다. Dirik과 그의 동료들은 PassPoints 시스템에서의 도용 가능성에 대해 연구하였다[8]. 즉 어떤 배경화면이 사용되었을 때 그 그림에서 선택점이 될 만한 것들을 미리 예측하는 방법에 대한 연구이다.

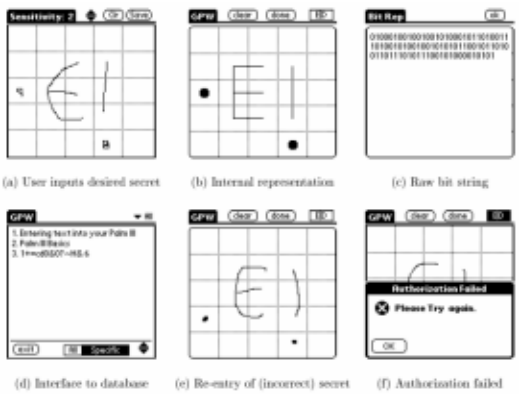

[Fig. 1] An Image and Chosen Points in PassPoints[9]

또한 그래픽 패스워드를 도용 하거나 훔쳐보기 어렵게 만들기 위한 노력도 있었다[10,11]. [Fig. 2]는 그래픽 패스워드를 등 뒤에서 훔쳐보더라도 인식 코드를 알기 어렵게 만들기 위해 여러 가지 객체를 많이 사용한 예이다[11].

[Fig. 2] A Shoulder-Surfing Resistant Graphic Password Scheme[10]

Thorpe과 Oorschot는 이처럼 복잡한 여러 가지 그래픽 패스워드를 알아내는 방법을 연구 하였고 'Graphical Dictionaries'라는 개념을 소개하였다[14]. 다음은 재현 기반(Recall- Based) 그래픽 패스워드에 대하여 알아본다.

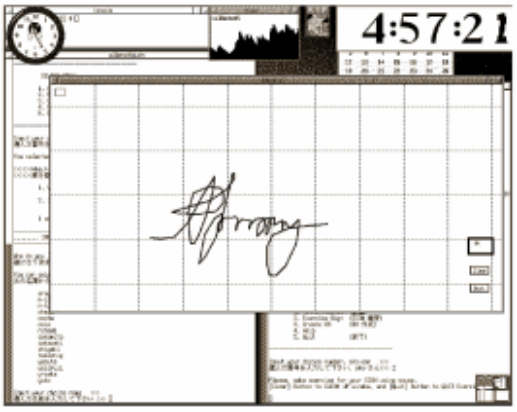
재현 기반 그래픽 패스워드로 Jermyn과 그의 동료들은 DAS(Draw-A-Secret)로 알려진 시스템을 소개 하였다[12]. 이 시스템은 [Fig. 3]과 같이 패턴을 그릴 수 있는 시스템이다.




[Fig. 3] DAS(Draw-A-Secret) Scheme[12]

DAS 시스템에서는 화면에 나눠진 구역이 있고 그 구역들을 지나가면서 패턴이 그려진다. 패턴이 그려지면서 지나가는 구역의 순서가 기억되고 이것이 맞아야 인증이 된다. 따라서 사용자는 패스워드를 만들 때 그렸던 패턴과 어느 구역에 어떤 순서로 패턴을 그려야 하는 지를 기억하였다가 인증 시 재현하여야한다.

다음 [Fig. 4]는 Syukri와 동료들이 제안한 시스템으로 마우스로 서명을 그려서 인증하는 방식이다[14]. 온라인 서명 인식은 또 다른 주제이므로 여기서는 더 깊이 논하지 않기로 한다.




[Fig. 4] A Signature Recognition System[14]

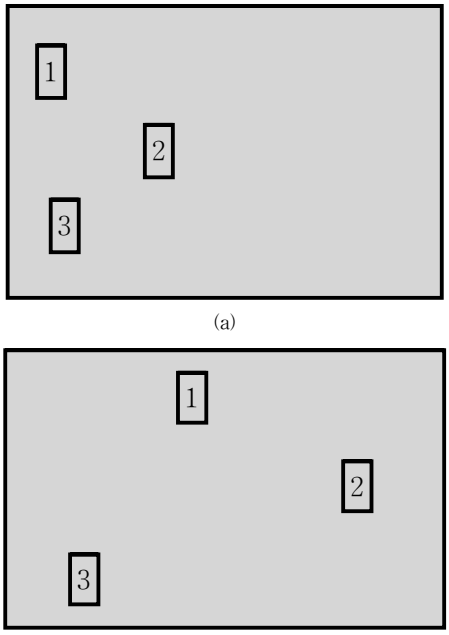
Syukri와 동료들의 시스템은 사용자가 자신의 서명을 그대로 사용하기 때문에 기억하기 쉽고 가른 사람이 도용하기 어렵다는 장점이 있지만, 마우스를 이용하여 서명하기가 어렵고 인식의 절차도 복잡하다는 단점이 있다. 최근에는 그래픽 패스워드와 텍스트 기반 패스워드를 함께 사용하는 기법도 소개 되었다[15]. 다음 3장에서는 신개념의 그래픽 패스워드 PassPositions를 소개한다.

## 3. 상대적 위치를 이용한 새로운 그래픽 패스워드

2장에서 살펴본 바와 같이 그래픽 패스워드는 텍스트 기반 패스워드보다 사용하기 편리하고 도용되기 어려운 장점이 있다. 하지만 장애인들에게는 불편한 점이 있다. 즉 그래픽 패스워드가 요구하는 이미지 상의 정확한 위치선택이 장애인들에게는 쉽지 않은 것이다. 마우스 - 심지어는 손가락 - 를 이용하여 정확한 선택 점의 지정이 어려운 장애인들도 있다. 이를 개선하기 위해서는 선택 점의 크기를 크게 하여야 하는데 그러면 패스워드의 도용 가능성이 커진다. 따라서 선택 점의 크기와 관계없이 보안성을 유지할 수 있고 장애인도 쉽게 사용할 수 있는 그래픽 패스워드 기법의 개발이 요구된다. 본 장에서는 그래픽 패스워드의 장점을 지니면서 장애인도 쉽게 사용할 수 있는 신개념의 그래픽 패스워드 PassPositions를 소개한다.

PassPositions는 상대적 위치(Relative Position)를 이용한 그래픽 패스워드 시스템이다. 기존의 그래픽 패스워드들은 이미지 상의 구역이나 픽셀을 이용한 절대적 위치(선택 점)를 이용 하였다. PassPositions는 사용자가 패스워드를 등록할 때 여러 개의 선택 점을 순서대로 선정하는 것은 기존의 시스템과 같다. 하지만 이들이 시스템에 등록될 때 선택 점의 절대적 위치가 시스템에 기록되는 것이 아니라 상대적 위치가 기록된다. 예를 들어 사용자가 3개의 선택 점(a, b, c)을 선택했다면, PassPositions는 픽셀 a의 절대적 위치를 계산한다. 그리고 두 번째 선택 점 b가 입력되면 b의 절대적 위치를 계산하여 b의 a에 대한 상대적 위치를 밝힌다. 즉 b가 a의 위에 위치하는지 아래에 위치하는지 또는 왼쪽이나 오른쪽에 위치하는지를 알아내는 것이다. 또 c가 입력되면 b에 대한 c에 상대적 위치를 알아내어 기록한다. 그리고 인증 시에도 같은 방법으로 선택 점들에 대한 상대적 위치를 알아내어 인증을 수행한다. 이러한 PassPositions의 기법을 사용하면 사용자는 화면상의 정확한 위치를 선택

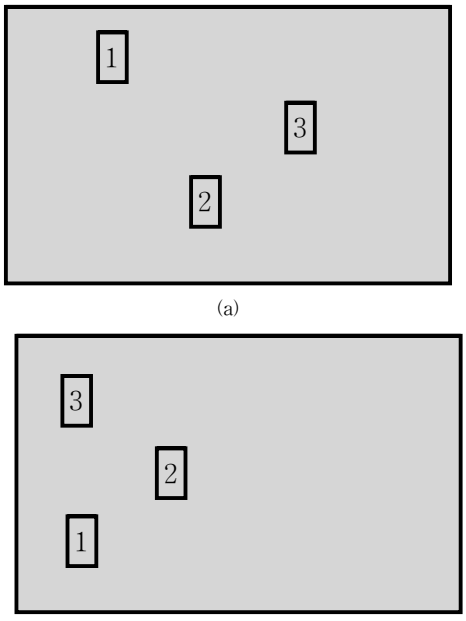
하여야하는 대신 상대적 위치만 구별하면 되는 것이다. 다음 [Fig. 5]는 PassPositions에서 선택 점의 상대적 위치가 같은 두 경우를 보인 것이다. 선택 점들에 있는 번호는 선택 순서이다.




[Fig. 5] Cases with the Same Relative Positions

선택 점들 1 2 3의순서는 [Fig. 5(a)]와 [Fig. 5(b)]가 같으나 절대적 위치는 다르다. 하지만 이들의 상대적 위치는 같다. 즉 둘 다 1의 오른쪽 아래에 2가 있고 2의 왼쪽 아래에 3이 있다. 따라서 기존의 그래픽 패스워드 시스템에서는 [Fig. 5(a)]와 [Fig. 5(b)]가 서로 다른 패스워드로 인식 되지만 PassPositions에서는 같은 패스워드로 인식된다. 하지만 [Fig. 6(a)]와 [Fig. 6(b)]는 서로 다른 패스워드로 인식되며 [Fig. 5]의 두 경우와도 상대적 위치가 모두 다른 경우이다.

이처럼 선택 점들의 절대적 위치가 아닌 상대적 위치를 이용하면 정확한 위치 선택이 어려운 사용자들에게는 매우 유용한 시스템이 된다.




[Fig. 6] Cases with Different Relative Positions

또한 PassPositions는 매번 서로 다른 위치를 선택하여도 같은 패스워드를 입력하는 효과를 볼 수 있다. 그 이유는 [Fig. 5(a)]와 [Fig. 5(b)]의 경우처럼 절대적 위치로 보면 서로 다른 위치를 선택하여도 같은 인증 코드를 생성하기 때문이다. 이러한 PassPositions의 특성은 기존의 그래픽 패스워드와 다른 점이며 훔쳐보기에 의한 패스워드 도용문제 해결에도 큰 도움이 된다.

그래픽 패스워드의 문제 중 하나는 패스워드를 다른 사람에게 알려 주기가 쉽지 않다는 것이다. 텍스트 기반 인증의 경우 간단히 문자 스트링을 보내어 다른 사람에게 패스워드를 쉽게 알려 줄 수 있으나 그래픽 패스워드의 경우에는 상대적으로 어렵다. 하지만 PassPositions의 경우 상대적 위치 스트링(RP-String)을 사용 하므로 텍스트 기반 인증의 경우와 같이 간단한 문자 스트링을 통하여 다른 사람에게 패스워드를 쉽게 알려 줄 수 있다. 다음은 PassPositions의 실행 절차이다.

(패스워드 등록 단계)

1. 사용자가 선택 점들의 위치를 차례로 선택한다.
   - 선택 점의 개수는 텍스트기반의 패스워드와 같이 임의로 정할 수 있다.

2. PassPositions는 사용자 아이디와 함께 선택 점들의 상대적 위치 스트링(RP-String)을 데이터베이스에 기록한다.

(패스워드 검증 단계)

1. 사용자가 선택 점들의 위치를 차례로 선택한다.
2. PassPositions는 사용자 아이디와 함께 입력된 선택 점들의 상대적 위치 스트링(RP-String)을 데이터베이스에 기록되어있는 위치 스트링(RP-String)과 비교하여 인증을 수행한다.

다음은 PassPositions에서 상대적 위치 스트링 작성을 [Fig. 5]의 예를 들어 설명한다. 먼저 1이 선택 되면 1의 절대적 위치를 계산한다. 2가 입력되면 1에 대한 2의 상대적 위치를 파악하여 상대적 위치 스트링 RP-String = (RD)를 생성한다. 여기서 R = Right. L = Left, U = Up, D = Down을 나타낸다. 따라서 (RD)는 두 번째 선택 점은 첫 번째 선택 점의 오른쪽 아래에 있다는 것을 나타낸다. 다음으로 3이 입력되면 2에 대한 3의 상대적 위치를 파악하여 상대적 위치 스트링 RP-String = (RD LD)를 생성한다. 더 이상 입력되는 선택 점이 없으므로 RP-String = (RD LD)가 [그림 5]의 최종 인증 코드가 된다. 또한 [Fig. 6(a)]는 RP-String = (RD RU)가 그리고 [Fig. 6(b)]의 경우 RP-String = (RU LU)가 된다. 따라서 [Fig. 5]와 [Fig. 6(a)] 그리고 [Fig. 6(b)]는 RP-String 값이 달라 서로 다른 패스워드로 인식된다. 그리고 RP-String의 길이는 사용자가 패스워드를 만들 때(등록할 때) 몇 개의 선택 점들을 사용하느냐에 따라 결정된다.

다음은 PassPositions의 전체적인 알고리즘이다.

```
PassPositions:
(Registration Stage)
        ID = user id
        IP = the first input point position
;; Take the first input position
        BP = Abs(IP)
;; Calculate Absolute position of input point
        IP = input point
        NP = Abs(IP)
        RP = Compare (BP, NP)
             ;; Decide relative position
        RP-String = (List (ID  RP)
             ;; Build relative position string
Loop    If input = Enter then Return RP-String &
             Store in a DB ;; Return final RP-String
        IP2 = input point
        NP2 = Abs(IP2)
        RP = Compare (NP, NP2)
;; Decide relative position
        RP-String = (Append RP-String RP)
;; Expand relative position string
        NP = NP2
        Go Loop

(Verification Stage)
        ID = user id
        IP = the first input point position
;; Take the first input position
        BP = Abs(IP)
;; Calculate Absolute position of input point
        IP = input point
        NP = Abs(IP)
        RP = Compare (BP, NP)
;; Decide relative position
        RP-String = (List (ID  RP)
;; Build relative position string
Loop    If input = Enter then Find RP-String at the DB
          If RP-String is in the DB then Recognition
                                         Success
                                   else Recognition
                                         Fail
        IP2 = input point
        NP2 = Abs(IP2)
        RP = Compare (NP, NP2)
;; Decide relative position
        RP-String = (Append RP-String RP)
;; Expand relative position string
        NP = NP2
        Go Loop
```

## 4. 결론

본 논문에서는 텍스트 기반 인증기법을 대체할 수 있는 인증기법 중 그래픽 패스워드에 대하여 알아보고 신개념의 그래픽 패스워드 등록 및 인증 시스템 구현 기법인 PassPositions를 소개하였다. PassPositions는 유니버설 디자인에 기반을 둔 것으로 누구나 사용하기 좋은 그래픽 패스워드 시스템 구현 기법이다. 그 이유는 PassPositions는 선택 점들의 상대적 위치를 활용하여 인증 코드를 생성하기 때문에 정확한 절대적 위치를 선정하기 어려운 사람들도 쉽게 사용할 수 있기 때문이다.

PassPositions는 터치 패드와 손을 사용하여 직접 조작하는 모바일 기기에서 활용될 경우 그 실용성은 더욱

커질 수 있다. 손을 사용하는 경우에는 좁은 영역을 정확히 선택하기가 마우스나 전자 펜 같은 도구를 사용하는 경우보다 상대적으로 더 쉽지 않기 때문이다. 또한 PassPositions는 배경화면용 이미지를 PassPoints시스템에서처럼 자유롭게 선택하여 사용할 수 있다. 즉 사용자가 원하는 이미지나 사진을 배경화면으로 이용할 수 있어 사용자의 개성에 맞는 시스템 구축이 가능하다. 심지어는 아무 배경 그림이 없는 상태에서도 사용이 가능하다. 이러한 특성은 기존의 그래픽 패스워드에서 문제가 되는 Hot Spot에 의한 패스워드 스페이스 문제를 발생하지 않게 한다.

그리고 PassPositions는 매번 서로 다른 위치를 선택하여도 같은 패스워드를 입력하는 효과를 볼 수 있어서 훔쳐보기에 의한 패스워드 도용문제 해결에도 큰 도움이 된다. 그 뿐만 아니라 PassPositions의 경우 기존의 그래픽 패스워드 방식과 달리 상대적 위치 스트링(RP-String)을 사용 하므로 텍스트 기반 인증의 경우와 같이 간단한 문자 스트링을 통하여 다른 사람에게 패스워드를 쉽게 알려 줄 수도 있다. 이러한 장점을 갖은 PassPositions를 더욱 발전 시켜서 장애인을 포함한 모든 사용자들이 안심하고 보다 편리하게 사용할 수 있는 개인 인증 기법으로 개발하여 컴퓨터는 물론이고 ATM, 이동전화기 같은 다양한 IT기기에서 신뢰성 있는 개인 인증 시스템으로 활용되기를 기대한다.

## REFERENCES


[1] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[2] M. Kotadia, "Microsoft: Write down your passwords," in ZDNet Australia, May 23, 2005.

[3] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000.

[4] Blonder, G., "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[5] Ronald L. Mace, Graeme J. Hardie, Jaine P. Place, Accessible Environments: Toward Universal Design, a chapter in Design Intervention: Toward a More Humane Architecture, W.E. Preiser, JC. Vischer, E.T. White (Eds.). Van Nostrand Reinhold, New York, 1991.

[6] Xiaoyuan Suo Ying Zhu G. Scott., Graphical Passwords: A Survey, In 21st Annual Computer Security Applications Conference(ACSAC), 2005.12.

[7] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human Computer Studies, 63, pp. 102-127, 2005

[8] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Human-Computer Interaction International (HCII 2005). Las Vegas, NV, 2005

[9] A. E. Dirik, N. Memon, J.C. Birget, ``Modeling user choice in the PassPoints graphical password scheme'', Symposium on Usable Privacy and Security(SOUPS), at Carnegie-Mellon Univ., Pittsburgh, July 2007

[10] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management. Las Vegas, NV, 2004.

[11] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[12] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[13] J. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," in Proceedings of the 13th USENIX Security Symposium. San Deigo, USA: USENIX, 2004.

[14] A. F. Syukri, E. Okamoto, and M. Mambo, "A User

Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): SpringerVerlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441

[15] Ahmad Almulhem, "A Graphical Password Authentication System", World Congress on Internet Security (WorldCIS-2011), London, UK, February 21-23, 2011.

**양 기 철(Yang, Gi-Chul)**

- 1986년 8월 : University of Iowa, Department of Computer Science, MS
- 1993년 5월 : University of Missouri -Kansas City, Computer Science, Ph.D.
- 2002년 3월 : Heriot-Watt University, Visiting Scholar
- 1993년 9월 ~ 현재 : 목포대학교 멀티미디어공학과 교수
- 관심분야 : 인공지능, 휴먼-컴퓨터 상호작용, 정보검색
- E-Mail : gcyang@mokpo..ac.kr

**김 황 용(Kim, Hwangyong)**

- 1990년 6월 : University of Oregon 특수교육(M.A.)
- 1995년 6월 : University of Oregon 특수교육(Ph.D.)
- 1997년 3월 ~ 현재 : 광주대학교 작업치료학과 교수
- 관심분야 : 장애인 사회통합
- E-Mail : hkim97@gwangju.ac.kr