적응적으로 방향 데이터의 범위를 생성하여 패턴을 인식하는 보안시스템

한주찬, 전민성, 김정영, 최경주
충북대학교 소프트웨어학과
e-mail : npqr11@naver.com

A Security System that Flexibly Generates a Range of Direction Data and Recognizes the Pattern

Juchan Han, Minseong Jeon, Jeongyeong Kim, Kyungjoo Cheoi
Dept of Computer Science, Chungbuk National University

요약

본 논문에서는 손의 움직임 패턴으로 암호를 구성하고, 이를 인식하는 보안 시스템에서 기존의 고정된 공간에서 방향 데이터 범위를 생성하여 입력되는 패턴마다 적응적으로 방향 데이터를 뽑아낼 수 없었던 단점을 극복하고자 입력되는 움직임 패턴의 방향 데이터를 입력 패턴마다 적응적으로 생성하는 방법을 제안한다. 기존의 고정된 공간에서의 방향 데이터 생성 방식 기법과 비교 실험한 결과 정인식률 94.2%로 기존방식의 91.4%보다 높은 인식률로 만족할 만한 성능을 보여줌을 확인할 수 있었다.

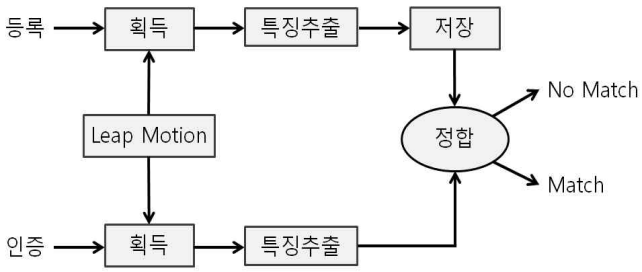
1. 서론

기존의 키패드로 동작하는 일반 디지털 도어락과 달리 보안을 높이기 위해 인가된 사용자만이 알고 있는 간단하고도 독특한 움직임의 패턴으로 암호를 구성하는 보안시스템이 대두되고 있다[1]. [1]의 시스템에서 제안된 보안 시스템은 암호를 등록하기 위해 손가락의 좌표를 입력받아 이에 대한 패턴 이미지와 방향 데이터를 저장하여 사용자가 등록한 암호와 일치하는지 인증하는 시스템이다. 이 시스템은 립모션 컨트롤러(Leap Motion Controller)를 통해 실시간으로 제공되는 손의 좌표를 입력받고, OpenGL(Open Graphic Library)과 OpenCV(Open Computer Vision) 라이브러리를 사용하여 구현되었으며 사용자가 등록한 암호는 패턴 이미지와 방향 데이터로 구성되어 저장한다. 여기서 방향 데이터를 구할 때 고정된 공간에서 방향 데이터의 범위를 생성하였는데 본 논문에서는 이를 개선하여 적응적으로 방향 데이터의 범위를 생성하는 보안 시스템으로 제안하고자 한다.

2. 제안하는 시스템

제안하는 시스템에 대한 전체적인 동작과정은 다음 (그림 1)과 같다. '등록' 모듈에서 사용자가 손의 움직임으로 입력하는 암호를 Leap Motion을 이용하여 값을 획득한 뒤에 이에 대한 특징을 추출하여 저장한다. 사용자가 등록한 암호의 특징 추출은 손의 움직임으로 그려진 패턴 이미지와 이에 대한 방향 데이터이다. '인증' 모듈에서는 사용자가 등록한 암호와 같은 암호를 Leap Motion을 이용하여 값을 획득한 뒤에 등록한 정보와 일치하는지 확인하여 인가된 사용자를 인증한다.

제안하는 시스템은 전체적인 동작과정 중에서 더 높은 인식률을 위해 특징 추출할 때 적응적으로 방향 데이터의 범위를 생성하는 방법을 적용하였다. [1]의 시스템에서의 경우 고정된 공간에서 방향 데이터의 범위를 생성하여 사용자가 범위의 경계선을 알 수 없기 때문에 이에 대한 오류율이 존재하였다.



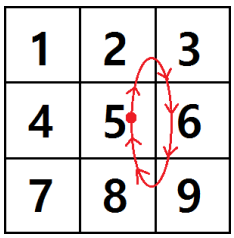
(그림 1) 시스템의 전체적인 동작과정

이 오류율을 줄이기 위한 방법으로 적응적으로 방향 데이터를 생성하여 사용자가 방향 데이터의 경계선을 알지 못하더라도 등록한 패턴 이미지의 모양을 맞게 그린다면 인증할 수 있도록 알고리즘을 개선하였다. 다음 2.1절에서는 등록 및 인증 시 방향 데이터의 추출방법에 대해 설명하고, 이어 2.2절에서는 인증 시 사용되는 패턴 이미지 처리 방법을 기술한다.

2.1 등록 및 인증 시 방향 데이터 추출방법

1) 기존의 방향 데이터 특징 추출

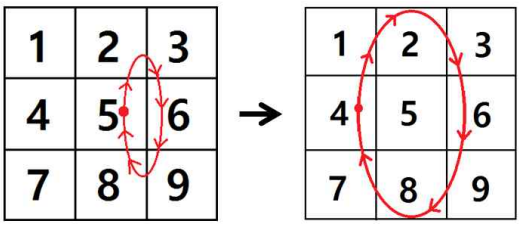
(그림 2)는 고정된 공간에서 방향 데이터를 생성하는 [1]의 시스템이 적용한 방법으로 사용자가 보안 패턴을 등록하였을 때의 방향 데이터를 저장하는 과정을 나타낸 것이다. 사용자가 암호를 입력할 때 사용되는 전체 범위의 3X3 매트릭스를 그려서 생성된 암호가 해당 매트릭스의 각각의 위치를 지났는지 판별하여 방향 데이터를 설정한다. 예를 들어 사용자가 매트릭스 5번에 위치한 점에서부터 시작하여 시계방향으로 반원을 그려 보안 패턴을 만들었을 때 이때의 방향 데이터의 값은 5 2 3 6 9 8 5가 된다. 이 정보는 등록과정에서 저장되고, 사용자가 후에 인증할 때에는 등록된 방향 데이터와 비교하여 인가된 사용자를 인증한다.



(그림 2) 고정된 공간에서 방향 데이터 생성

2) 개선된 방식의 방향 데이터 특징 추출

(그림 3)의 오른쪽 영상은 제안하는 시스템에서 적용한 방법으로써 만일 (그림 3) 왼쪽 영상과 같이 [1]의 시스템의 방식처럼 방향 데이터가 입력되었다면 그려진 패턴 이미지의 크기를 정사각형으로 자르고 정규화하여 적응적으로 방향 데이터 3X3 매트릭스를 생성한다. [1]의 시스템에서의 방식과 차이점은 암호를 입력할 때 [1]의 시스템의 경우에는 공간의 경계선에 의존적인 매트릭스이지만, 개선된 방식은 입력하는 패턴 이미지에 의존적임을 알 수 있다. 그렇기 때문에 사용자가 허공에서 매트릭스의 경계선을 알지 못하더라도 등록한 패턴 이미지를 알고 있다면 쉽고, 정확하게 인증할 수 있다. 개선된 방식에서의 방향데이터 값은 4 1 2 3 6 9 8 7 4가 되며 마찬가지로 이 정보는 등록과정에서 저장하고, 사용자가 인증할 때의 방향 데이터와 비교하여 인가된 사용자를 인증한다.

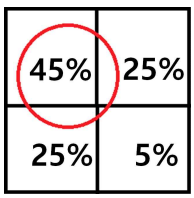


(그림 3) 적응적으로 방향 데이터 생성

2.2 인증 시 그려진 패턴 이미지 처리

1) 그려진 패턴 이미지 위치에 따른 인증

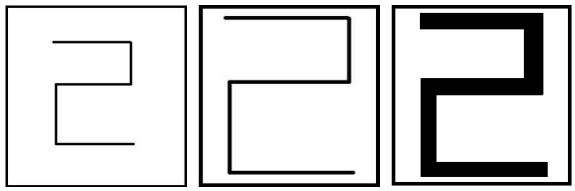
(그림 4)는 Leap Motion이 손의 움직임을 인식할 수 있는 범위에서 사용자가 어느 위치를 중심으로 패턴 이미지를 등록하였는지 판단하는 알고리즘이다. 방향 데이터를 통해 정확한 모양을 인식하더라도 등록한 암호와 다른 위치에서 인증을 할 경우를 걸러내는 것이다. 예를 들어 (그림 4)와 같이 공간을 4등분하여 가장 많이 차지하는 45%의 경우에도 오차를 20%로 설정하여 왼쪽 위에서 암호를 인증하도록 설정한 것이다.



(그림 4) 그려진 패턴 이미지 위치 판단

2) 패턴 이미지 모양의 비교에 따른 인증

등록된 이미지 모양과 같은지 먼저, 대상 패턴 이미지에 대해 전처리를 수행하는데, 전체 화면에서 그려진 패턴 이미지만큼의 크기로 잘라낸 실제 형태 이미지만을 따로 추출하고, 추출된 형태 패턴 이미지를 정규화 이미지로 변환한다. 이때 형태 이미지의 가로와 세로 길이를 비교하여 더 큰 값을 한 변의 크기로 설정하여 정사각형으로 이미지를 자른다. 시스템에 등록된 보안 패턴의 형태 이미지와 인증 모듈에 입력한 패턴의 형태 이미지를 비교하기 위하여 템플릿 매칭 (Template Matching) 기법을 사용하였다. 템플릿 매칭은 매칭 되는 점의 위치를 탐색하는 매칭기법이다. 점의 위치를 탐색하는 과정에서 선의 굵기가 얇으면 템플릿 매칭 계수가 낮게 나오기 때문에 침식연산을 통해 선의 굵기를 굵게 변환한다. 이와 같은 과정은 (그림 5)과 같다. 이렇게 전처리 과정이 끝나면, 정규화 된 패턴 이미지를 템플릿 매칭하여 템플릿 매칭 계수를 출력한다. 템플릿 매칭 계수의 값은 30을 초과하면 같은 패턴 이미지로 판단하여 인증 성공하도록 설정하였고, 그렇지 않으면 인증 실패하도록 설정하였다.



(그림 5) 패턴 이미지를 정규화하여 침식연산

3. 실험 및 결과

실험한 실험환경은 Intel Core i5-5200과 RAM 8G와 64비트 운영체제의 사양인 PC를 사용하였다. 그리고 이번 실험은 [1]의 시스템 방식의 성능과 개선된 방식의 성능 차이를 분석하기 위해 [1]의 시스템에서 실험하였던 테스트 영상을 대상으로 실험하였다.

<표 1>은 기존 방식의 실험 결과이며 제안하는 시스템의 개선된 방식에 대한 실험 결과는 <표 2>과 같다. 참긍정(True Positive; 정인식률) 88.3%, 거짓부정(False Negative) 100%, 참부정(True Negative) 0%, 거짓긍정(False Positive; 오류율) 11.7%의 결과를 얻었다. 개선된 방식도 [1]의 시스템과 마찬가지로 거짓부정은 100%로 잘못된 패턴을 인증하는 경우는 한 건도 없었다. 참부정 즉 오류율(실제 맞는 패턴을 잘못된 패턴으로 판단)의 경우 5.8%의 결과가 나왔다. 최종적으로 [1]의 시스템 방식의 정 인식률은 91.4%였으며, 개선된 방식의 정 인식률은 94.2%의 결과를 얻었다.

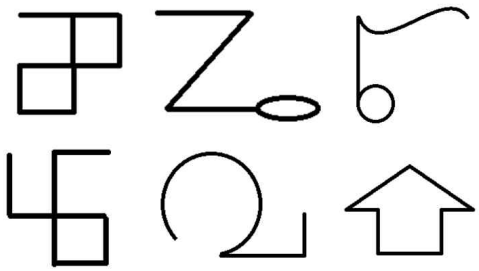
<표 1> [1]의 시스템 방식에 대한 실험 결과

부류 \ 부류결과	w1(참)	w2(거짓)
w1(참)	148	32
w2(거짓)	0	180

<표 2> 제안하는 시스템 방식의 실험 결과

부류결과 / 부류	w1(참)	w2(거짓)
w1(참)	159	21
w2(거짓)	0	180

보다나은 성능분석을 위해 더 많은 종류의 영상을 대상으로 실험하였다. 먼저, 실험 영상을 얻기 위해 대학생 121명을 대상으로 설문조사를 실시하였으며 설문조사 내용은 움직임 패턴을 이용한 보안시스템에 대한 인식 정도와 본인이 사용자라면 암호를 등록할만한 보안 패턴을 그리는 것이었다. 이를 통해 얻은 보안 패턴을 실험 영상으로 만들어 추가 실험을 수행하였다.



(그림 6) 설문조사를 통해 실험한 보안 패턴 이미지

설문조사를 통해 추출한 보안 패턴으로 실험한 실험 결과는 <표 3>과 같다. 참긍정(True Positive; 정인식률) 84.4%, 거짓부정(False Negative) 100%, 참부정(True Negative) 0%, 거짓긍정(False Positive; 오류율) 15.6%의 결과를 얻었다. 개선된 방식도 [1]의 시스템 방식과 마찬가지로 거짓부정은 100%로 잘못된 패턴을 인증하는 경우는 한 건도 없었다. 참부정 즉 오류율(실제 맞는 패턴을 잘못된 패턴으로 판단)의 경우 7.8%의 결과가 나왔다. 마지막으로 정 인식률은 92.2%의 결과를 얻었다.

<표 3> 설문조사 보안 패턴으로 실험한 결과

부류결과 / 부류	w1(참)	w2(거짓)
w1(참)	152	28
w2(거짓)	0	180

4. 결론

본 논문에서는 적응적으로 방향 데이터를 생성하는 방식을 개선한 보안 시스템으로 제안하였다. 사용자의 입장에서 손의 움직임으로 보안 패턴을 입력할 때 방향 데이터의 경계선을 알 수 없기 때문에 이로 인한 이유로 오류율이 존재하였다. 이를 개선한 방식으로는 사용자가 방향매트릭스의 경계선을 알지 못하더라도 등록한 패턴의 모양을 맞게 인증한다면 이를 구분하여 인증하는 개선된 결과를 얻을 수 있었다.

개선된 방식의 제안하는 시스템은 참 긍정 즉 정 인식률(맞는 패턴을 맞다고 판단)이 94.2%로 나와 [1]의 시스템에서의 정 인식률인 91.4%보다 높은 만족할 만한 결과를 얻을 수 있었다. [1]의 시스템과 마찬가지로 거짓부정(잘못된 패턴을 다른 패턴으로 판단)의 결과값이 100%의 결과로 나왔다. 즉, 잘못된 패턴은 인증 성공하지 못하는 것이다. [1]의 시스템에서 필요로 하는 더욱 많은 종류의 패턴을 등록하는 것도 설문조사를 통해 다양한 패턴을 추출하여 실험을 하였으며 이에 대한 정 인식률은 92.2%의 결과를 얻었다. 설문조사를 통해 추출한 보안 패턴은 <표 2>에서의 실험보다 어려운 보안 패턴으로 실험한 것이기 때문에 정 인식률이 더 낮은 결과를 얻은 것이다. 이로 인해 아직도 오류가 있는 부분이 있음을 파악하고 이를 해결하기 위해 또 다른 방식으로 개선해야한다. 향후 계획으로는 방향 데이터를 저장하는 과정에서 매트릭스를 생성하는 방식 외에 새로운 방식으로 좌표의 연결점으로 방향을 나타내고, 이들 순서의 집합을 비교하는 방식으로 연구할 계획이다.

참고 문헌

[1] 한주찬. 전민성. 최경주(2016년). 손가락으로 그린 움직임 패턴을 이용한 보안시스템. 한국정보처리학회.