

손동작 인식을 이용한 출입 보안 시스템

최경주[†], 한주찬^{**}

A Novel Door Security System using Hand Gesture Recognition

Kyungjoo Cheoi[†], Juchan Han^{**}

ABSTRACT

In this paper, we propose a novel security system using hand gesture recognition. Proposed system does not create a password as numbers, but instead, it creates unique yet simple pattern created by user's hand movement. Because of the fact that individuals have different range of hand movement, speed, direction, and size while drawing a pattern with their hands, the system will be able to accurately recognize only the authorized user. To evaluate the performance of our system, various patterns were tested and the test showed a satisfying result.

Key words: Security Door, Hand Gesture Recognition

1. 서 론

기존의 키패드로만 동작하는 일반적인 출입문 보안 시스템은 비밀번호의 분실, 도난 가능성이 높다. 이러한 이유 때문에 보다 보안을 높이기 위하여 사용자의 암호를 번호로 구성하지 않고 9개의 점을 지나는 일정한 패턴으로 구성한다거나, 지문인식이나, 얼굴인식 등과 같은 사람의 생체정보를 사용하는 시스템[1,2]이 개발되고 있다. 또한 결제 시스템에 있어서도 카드 번호를 입력하는 대신 사용자의 생체정보 특히 지문정보를 인식하여 결제하는 기술도 적용하고 있다. 이러한 사용자 인증에 관련된 보안 시스템에 대한 연구는 패턴이나 생체정보 등, 번호를 대신할 수 있는 새로운 방식의 보안 시스템 뿐 아니라 기존 방식에서의 문제점을 보완하는 방식으로도 이루어지고 있다.

기존의 상용화된 보안 시스템 중 지문인식이나, 숫자키패드, 패턴 그리기 등의 보안 시스템은 사용

자를 인증하기 위해 패드에 손으로 직접 입력해야하기 때문에 패드에 지문(흔적)이 남는다는 단점이 있다. 본 논문에서는 이러한 문제점을 보완하면서 기존 방식과 달리 새로운 방식의 보안 시스템으로써 사용자의 암호를 번호로 구성하지 않고, 사용자만이 알고 있는 간단하면서도 독특한 손동작으로 생성한 움직임 패턴을 허공에 그리면 그것이 암호로 구성하는 새로운 방식의 보안 시스템을 제안하고자 한다. 손동작으로 생성해내는 암호 패턴의 경우, 사용자가 패턴을 그릴 때 손의 움직임 범위가 개인별로 다르고, 특정 모양을 그릴 때 나타나는 움직임 방향과 크기, 속도 등이 다르기 때문에 이를 통해 인가된 사용자만을 정확히 걸러낼 수 있다. 또한 어떤 부분에 있어서는 숫자를 암기하는 것보다 자신만의 규칙적인 행동을 암호로 사용하는 것이 어르신 분들에게는 조금 더 나은 편리함을 제공할 수도 있다. 단순하면서도 충분한 개인차를 가지는 이러한 특징이 보안에 더 효율적이다.

* Corresponding Author: Kyungjoo Cheoi, Address: (361-768) ChungDae-ro 1, Seowon-gu, Cheongju-si, Chungbuk, Korea, TEL: +82-53-261-3487, FAX: +82-53-273-2265, E-mail: kjcheoi@chungbuk.ac.kr
Receipt date: Jul. 28, 2016, Approval date: Aug. 6, 2016
[†] Dept. of Computer Science, Chungbuk National University

^{**} Dept. of Computer Science, Chungbuk National University (E-mail: npqr11@naver.com)

* This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(NRF-2011-0023674)

카메라를 이용하여 손동작을 인식하는 연구는 여러 가지 방법으로 진행되어졌다[3-9]. 손동작 인식을 통해 보다 자연스러운 인터페이스를 구현하기 위한 연구가 주로 많이 진행되었다[5-7]. Park[5]은 손동작을 활용하여 미래 자동차와 탑승자 간의 자연스런 상호작용에 대한 연구를 수행하였는데, 이 연구에서는 손동작으로 통해 0~9까지의 숫자 형태의 제스처(gesture) 경로를 추출하고, 은닉 마르코프 모델을 이용하여 해당 손동작이 어떤 숫자를 표현하는지 인식하는 시스템을 개발하였다. 이 시스템에서는 인식을 위해 학습의 단계를 거쳐야 했으며, 총 70.37%의 인식률을 가지고 있다. Kim[6]은 손동작을 이용한 마우스의 포인터 이동과 이벤트 처리방법을 제안하였는데, 사용자가 원하는 모든 위치에 커서를 위치시킬 수 있지만, 컬러 정보만을 이용하기 때문에 살색 계통의 물체가 손과 함께 갑자기 나타날 경우 손을 잘 인식하지 못하고, 노란색 불빛인 경우, 마우스 움직임과 동작 인식률이 낮아지는 단점이 있다. Hwang[7]은 가상공간에서의 객체 조작을 위한 비전 기반의 손 검출 및 추적 시스템에 대해 연구하였는데, 이 연구에서는 기하학적 구조에 의하여 손 외형을 인식하여 검출하는 통계적 방법을 사용하였으며, 카메라의 각도에 의해 손이 겹쳐 보이는 문제를 줄이기 위하여 다중 카메라를 사용하였다. 또한 손동작을 기본 형태와 6가지 형태로 규정하고 기본 형태를 인식하였고, 동작인식에 있어 동적 학습 알고리즘을 사용하여 한정된 수의 학습 집단으로 학습이 가능하도록 하였고, 검출된 불완전한 동작을 정정 가능하도록 하였다.

손동작 인식을 위하여 깊이정보를 사용하는 연구도 진행되었다[8, 9]. Kim[8]은 손 추적과 동작 인식 시스템 개발 연구에서 손을 이용하는 사용자 손의 3차원 기하학적 정보를 취득하기 위해 깊이 정보를 획득하는 별도의 깊이 정보 획득 장비를 사용하였으며, 사용자의 손 위치와 동작 정보는 깊이 정보로부터 추정하였다. 또한 Park[9]은 키넥트로 얻은 깊이 영상에서 손끝점을 찾고 통계적 특징 기반의 인공신경망(ANN)을 이용하여 공중에 그린 서명을 인식하는 알고리즘을 제안하였는데, 3차원 공간상의 x, y, z좌표에 관한 통계적 특징을 사용하였는데, 주성분분석(PCA) 기법을 통해 통계적 특징의 차원을 10으로 축소하고, 인공신경망(ANN)을 통해 학습한 후

15가지의 서명을 분류하였다.

위와 같은 관련 연구에서도 보았듯이 손동작을 인식하기 위해서는 기본적으로 손 검출과 손 검출 후에 손을 이용한 제스처 인식의 2단계로 이루어진다[3]. 손 검출이 먼저 진행되므로 손 검출이 제대로 되지 않으면 손동작 인식률이 떨어질 수 밖에 없다. 기존의 손동작 인식에 관련된 많은 연구들은 인간과 기계간의 보다 편한 인터페이스 구축에 초점을 두고 진행된 경우가 많았으며, 이를 보안 시스템에 적용한 사례는 없었다. 따라서 본 논문에서는 손동작 인식을 통해 보안을 한층 강화시킨 보안 시스템을 제안하고자 한다. 특히 제안하는 시스템은 어두운 곳에서도 안정적으로 손의 좌표값을 입력받을 수 있도록 림모션 컨트롤러(Leap Motion Controller)를 사용하였으며, OpenGL(Open Graphic Library)과 OpenCV(Open Computer Vision) 라이브러리를 사용하여 구현되었다. 다음 2장에서 제안하는 보안 시스템에 대하여 자세히 설명하고, 3장에서 실험 및 결과를, 그리고 마지막으로 4장에서 결론을 맺는다.

2. 제안하는 시스템

제안하는 시스템의 전체적인 동작과정은 다음 Fig. 1과 같다. 제안하는 시스템의 사용은 사용자가 먼저 자신이 암호로 사용할 패턴을 시스템에 등록시키고, 암호 등록 후에 인증 받는 일반적인 보안 시스템과 동일한 처리과정을 가진다.

Fig. 1의 왼쪽에 보이는 부분은 사용자의 암호를 등록시키는 절차를 나타낸 것으로, 손동작을 통해 생성되는 독특한 움직임 패턴의 특징을 시스템에 등

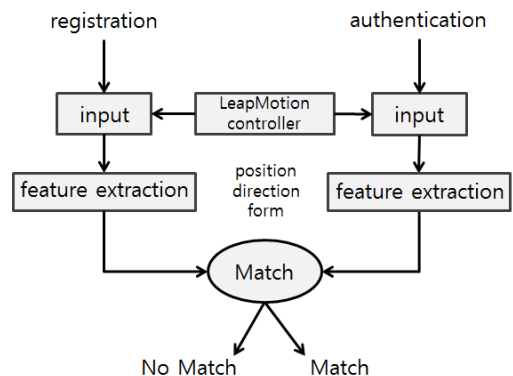


Fig. 1. Overall Process of the System.

록시킨다. Fig. 1의 오른쪽에 보이는 부분은 인가된 사용자를 인증하는 절차를 나타낸 것으로, 새로 입력되는 누군가의 움직임 패턴의 특징을 추출하여 시스템에 등록된 움직임 패턴의 특징과 비교하여 인가된 사용자를 인증한다. 이 때 등록과 인증에 사용되는 특징은 움직임 패턴의 움직임 순서를 나타내는 방향 데이터와, 최종으로 그려진 패턴의 형태 이미지, 그리고 전체 입력범위에서 움직임 패턴이 그려진 위치상의 정보이다.

손동작을 통해 실시간으로 입력되는 움직임 좌표값은 Fig. 2와 같은 립모션 컨트롤러를 통해 입력받는다. 사용자는 립모션 컨트롤러 위해 손을 움직이면 된다. 립모션은 적외선광과 전하결합소자 카메라를 이용해 그 반사파로 손동작을 인식하기 때문에 빛이 없는 어두운 곳에서도 손의 좌표값을 잘 입력받을 수 있고, 1/100 밀리미터 단위의 움직임까지 인식하며, 150° 반경에서 손가락 10개의 움직임을 초당 200프레임 속도로 감지한다. 이는 비교적 낮은 가격이며, 조명에 따른 인식을 변화를 최소화하여 손의 좌표값을 입력받기 매우 용이하다. 제안하는 시스템에서는 립모션 SDK를 설치하여 손바닥의 좌표값을 그대로 출력하도록 설정하였다.

다음 2.1절과 2.2절에서 암호를 등록시키는 절차와 인증하는 절차에 대해 자세히 설명한다.

2.1 손동작으로 생성되는 움직임 패턴 등록

인가된 사용자의 암호 패턴을 등록시키는 구체적인 절차는 Fig. 3과 같다. 사용자가 립모션 위에서 허공에 손을 움직여 패턴을 만들어내면 립모션으로부터 실시간으로 손의 좌표값을 입력받게 된다. 좌표값을 실시간으로 입력받을 때에는 입력 범위를 설정하여 입력받는 좌표값 순서에 맞게 방향 데이터를 생성하고, 최종 생성된 형태 이미지와 함께 등록한다. 또한 립모션이 인식할 수 있는 전체 범위에서 움



Fig. 2. LeapMotion Controller.

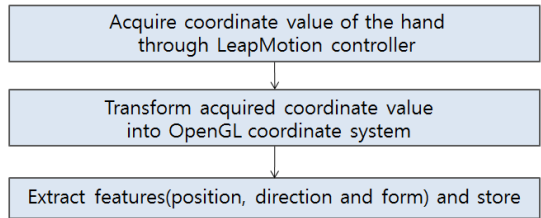


Fig. 3. Registration Process.

직임 패턴이 어느 위치에 속하는지에 대한 위치 정보도 특징으로 저장한다. 이렇게 암호로 사용되는 움직임 패턴은 여러 번 등록을 시도하는데, 총 3번의 패턴들이 모두 일치해야 일치하는 패턴이 등록되도록 하였다.

2.1.1 움직임 패턴의 방향 데이터 특징

같은 형태의 이미지라도 그려진 방향(순서)가 다르면 다른 패턴으로 구별하기 위하여 사용자가 암호로 사용할 움직임 패턴을 그릴 때 생기는 움직임의 방향 데이터 특징을 생성한다. 제안하는 시스템에서는 Fig. 4(b)에 보이는 3×3 방향 매트릭스를 사용하였다. 이 때 방향 매트릭스는 사용자가 패턴을 입력시킬 때 적용받는 전체 입력 범위(화면)에서 사용자가 그린 움직임 패턴만을 대상으로 정사각형 형태로 자르고(Fig. 4(a)), 100×100 사이즈로 정규화한 후, 이를 9등분하여 순서를 표시(Fig. 4(b))한 것이다. 따라서 방향 매트릭스는 정사각형의 형태이지만 크기는 입력된 움직임 패턴에 따라 적응적으로 변화한다. 현재는 3×3 매트릭스를 사용하였는데 이는 보안 수준에 따라 유동적으로 변경될 수 있다.

이와 같은 방향 매트릭스를 기반으로 한 방향 데

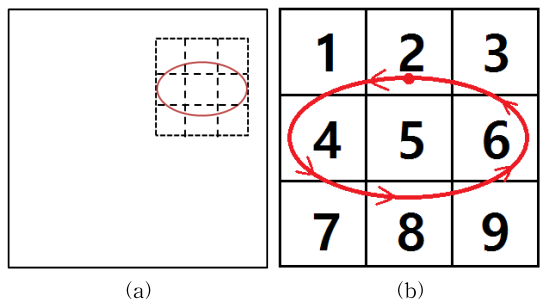


Fig. 4. Extraction process of the direction feature. (a) original whole region acquired from LeapMotion controller (b) dynamically regularized region used as direction matrix.

이터 특징 생성 방법은 다음과 같다. 먼저 립모션을 통해 좌표값이 실시간으로 입력되면 입력받은 좌표값을 OpenGL의 좌표계로 변환하고, 전체 화면을 대상으로 그려진 움직임 패턴에서 배경을 잘라낸 실제 움직임만을 따로 추출한다. 패턴의 가로와 세로 길이를 비교하여 더 큰 값을 한 변의 크기로 설정하여 정사각형으로 이미지를 자르는데 중간점은 패턴의 중심을 기준으로 한다. 이렇게 자른 이미지의 크기를 일정한 크기의 정사각형으로 변환하기 위하여 정규화 과정을 진행한다. 해상도 100×100으로 정규화된 정사각형 영역을 9등분하여 입력된 좌표값이 방향 매트릭스의 어떤 칸이 속하는지 체크하고 속한 칸의 번호를 순서대로 텍스트 파일에 저장한다.

사용자가 움직임 패턴을 등록할 때 암호의 난이도에 따라 ‘상’ 또는 ‘중’에서 하나를 선택하여 등록하게 되는데, 이 난이도에 따라 방향 데이터 특징을 생성하는 방식이 다르다. Fig. 4에 보이는 움직임 패턴이 난이도를 ‘상’으로 하여 입력시켰을 때 방향 데이터의 값은 2 1 4 7 8 9 6 3 2로 만들어져 저장된다. 하지만 난이도를 ‘중’으로 설정하여 입력시키면 방향 데이터가 홀수 영역과 짝수 영역 값으로 나뉘어 만들어지는데, 이 예에서는 홀수 영역은 1 7 9 3 으로, 짝수 영역은 2 4 8 6 2로 만들어져 저장된다.

2.1.2 움직임 패턴의 형태 이미지 특징

립모션을 통해 입력받은 움직임 패턴에 대한 좌표값을 OpenGL의 좌표계로 변환하여 이를 형태 이미지로 저장하는데 움직임 패턴의 방향 데이터 특징 생성할 때와 마찬가지로 움직임 패턴을 패턴의 가로와 세로 길이를 비교하여 더 큰 값을 한 변의 크기로 설정하여 정사각형으로 이미지를 자르고 정규화하여 저장한다. Fig. 5의 왼쪽 그림은 립모션이 인식할 수 있는 전체 범위(화면)에서 그려진 형태 이미지이며, 오른쪽 그림은 그려진 형태 이미지는 움직임 패턴만을 정사각형 형태로 자르고 정규화한 그림이다.

2.1.3 움직임 패턴의 위치 특징

형태 이미지를 저장할 때 형태 이미지의 위치에 대한 정보도 특징으로 저장한다. 위치는 립모션이 인식할 수 있는 전체 범위를 4등분 하여 사용자가 입력하는 움직임 패턴이 4개의 영역 중 어디에 속하는지 정하였다. Fig. 6은 사용자가 입력된 움직임 패

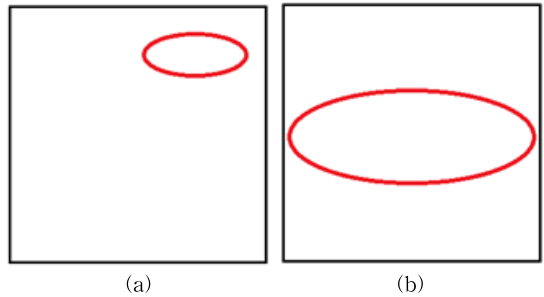


Fig. 5. Extraction process of the form feature. (a) original form image (b) regularized form image

턴의 형태가 원이었을 경우 4등분한 각 범위를 두고 전체 좌표에서 각 범위에 해당하는 좌표의 수만큼을 비율로 나타낸 것으로, 이 예에서는 각 범위 중에서 ②의 범위에 가장 많은 좌표값들이 있었기 때문에 위치 특징을 ②로 저장한다. Fig. 6의 예의 경우와 같이 나뉘어진 각 영역 중 40% 이상의 값이 있을 경우에만 위치 특징이 저장되며, 만약 두 영역이 40% 이상의 값이면 해당 영역을 모두 저장한다.

2.2 사용자 인증

사용자를 인증하는 절차는 Fig. 7과 같이 나타낼 수 있다. 사용자 인증 시 입력된 움직임 패턴의 특징과 움직임 패턴 등록 시 저장된 특징을 비교함으로써 인증을 수행한다. 인증 과정에서도 암호로 사용될 움직임 패턴을 등록할 때와 마찬가지로 방향 데이터, 형태 이미지, 위치 특징을 추출하는 과정은 동일하다. 사용자 인증 시 입력된 움직임 패턴의 위치 범위가 일치하면 방향 데이터를 비교하고, 방향 데이터가 일치할 경우 형태 이미지를 템플릿 매칭 (Template Matching)을 사용하여 정합하게 되는데,

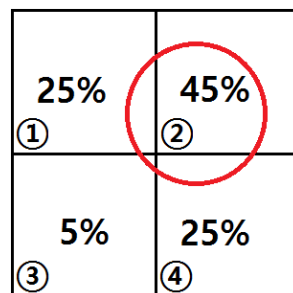


Fig. 6. Example of extracting process of the position feature.

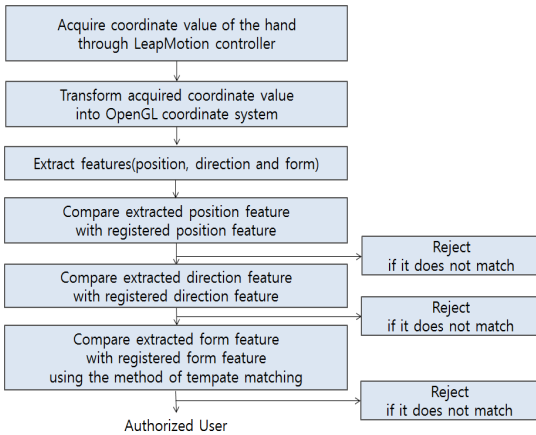


Fig. 7. Authentication Process.

매칭 계수가 설정한 값 이상의 값으로 출력되면 같은 형태의 이미지라고 판단하며 최종적으로 인가된 사용자로 인증한다.

2.2.1 위치 및 방향 데이터 비교

등록 시 저장된 위치 특징과 인증 시 입력된 패턴의 위치 특징을 비교하여 일치하면 방향 데이터를 비교한다. 움직임 패턴의 난이도가 ‘상’으로 설정되었을 경우에는 방향 데이터의 값이 방향 매트릭스의 각 위치 범위를 지날 때마다 모두 저장되기 때문에 등록 시 저장된 방향 데이터 값과 그대로 비교한다. 난이도가 ‘중’으로 설정되었을 경우에는 등록 시 저장된 방향 데이터 값이 홀수 영역과 짝수 영역을 나누어 저장되어 있으므로 인증 시 홀수 영역과 짝수 영역의 방향데이터 중 하나라도 일치하면 인증하도록 하였다.

2.2.2 형태 이미지 비교

형태 이미지를 비교하기 위해서 템플릿 매칭(Template Matching) 기법을 사용하였는데 이는 참조영상에서 템플릿 영상과 매칭되는 위치를 탐색하는 기법이다. 템플릿 매칭을 하려면 비교하고자 하는 2개의 이미지의 크기가 같아야 픽셀 값을 비교할 수 있으며, 템플릿 매칭을 통해 얻게 되는 매칭 계수 값은 2개의 이미지의 템플릿 매칭 정도를 나타낸 것으로 이 값이 높을수록 더 일치한다는 의미이다. 템플릿 매칭은 일반적으로 형태는 같지만 서로 다른 위치(Fig. 8)에 있다가, 위치와 형태가 같지만 크기가 다른 경우(Fig. 9) 템플릿 매칭 계수는 굉장히 낮은

값이 나와 서로 다른 이미지로 인식된다. 따라서 이러한 문제를 해결하기 위해 제안하는 시스템에서는 등록할 때와 인증할 때, 전체 화면을 대상으로 그려진 움직임 패턴에서 배경을 잘라낸 실제 형태 이미지를 따로 추출하고, 추출된 형태 이미지를 정규화 이미지로 변환하였다. 자세한 과정은 2.1절에 설명되어 있으니 이를 참조하길 바란다.

또한 선의 굵기가 얇으면 똑같이 그린 그림도 미세한 차이로 인해 템플릿 매칭 계수가 다르게 나올 수 있다. 그렇기 때문에 제안하는 시스템에서는 침식 연산을 이용하여 선의 굵기를 굵게 만든 후 정합하도록 하였다. 침식 연산은 수학적 모폴로지 연산 중 하나로 물체의 크기를 그 배경과 관련하여 일정하게 줄여준다. 배경의 경우 검정색이기 때문에 결국 패턴이 짙어지게 된다. 침식연산을 7번 수행하면 Fig 10(c)와 같은 결과가 나온다. 이렇게 침식 연산을 수행한 후 2개의 이미지를 정합하면 같은 모양에서의 미세한 차이로 인한 오류율을 줄일 수 있다.

제안하는 시스템에서는 템플릿 매칭 계수를 20으로 설정하여 설정한 값보다 큰 값이 출력되면 같은 형태 이미지로 판단하였다.

3. 실험 및 결과

시스템의 성능을 평가하기 위해 다양한 보안 패턴들을 대상으로 2가지 실험을 수행하였다. 첫 번째



Fig. 8. Same images with different position.

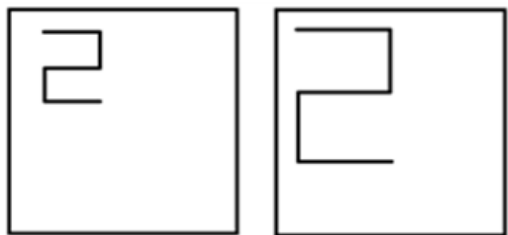


Fig. 9. Same images with different size.

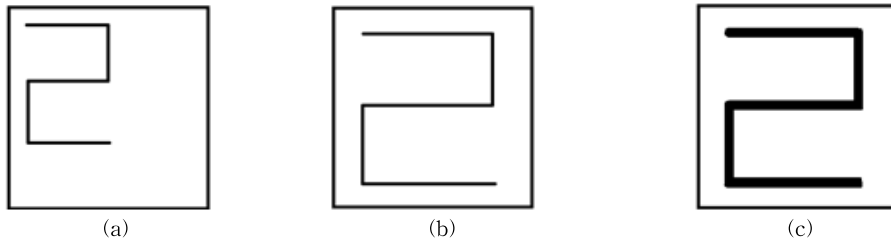


Fig. 10. Preprocess before applying template matching. (a) original pattern (b) regularized Pattern (c) erosion processed pattern.

실험은 제안하는 시스템과 유사한 [11]의 시스템보다 개선되었는가를 확인하는 실험이고, 두 번째 실험은 실제 사람들이 암호로 사용할 만한 보안 패턴을 획득하여 이를 대상으로 자체적인 성능평가를 하는 것이다.

성능평가 척도로는 올바른 패턴을 제대로 인식하는 참긍정률(TPR : True Positive Rate), 올바른 패턴을 잘못 인식하는 참부정율(TNR : True Negative Rate), 틀린 패턴을 올바르게 잘못 인식하는 거짓긍정율(FPR : False Positive Rate), 틀린 패턴을 틀리다고 제대로 인식하는 거짓부정율(FNR : False Negative Rate)을 사용하였다.

첫 번째 실험의 비교 대상인 [11]의 시스템은 제안하는 시스템과 유사하나, 방향 특징을 추출하는 방법에 있어 차이가 난다. 방향 특징을 추출할 때 [11]의 시스템의 경우에는 립모션이 인식할 수 있는 전체 입력 범위를 대상으로 고정된 공간에서 방향 데이터의 범위를 생성하기 때문에 사용자가 방향 매트릭스의 경계선을 제대로 상태로 패턴을 입력시키기에 따른 오류가 상당히 존재하였다. 다시 말하면 사용자는 자신의 보안 패턴을 제대로 입력하였다고 생각되지만 방향 매트릭스에서 조금의 오류도 허용하지 않아 거부해버리는 참부정율이 발생하는 확률이 높았다. 하지만 제안하는 시스템은 허공에서 보이지 않는 고정적인 방향 매트릭스의 경계선에 맞게 인증할 필요없이 사용자가 등록한 패턴과 모양을 같게 그려도 괜찮도록 적응적으로 방향 데이터의 범위

를 생성하는 방법을 적용하여 더 높은 인식률을 참긍정율을 높이고, 참부정율은 낮게 되도록 시스템을 개선하였다.

첫 번째 실험에 사용된 영상은 [11]의 실험에서 사용된 영상과 동일한 영상을 대상으로 실험하고 평가하였다. 실험에 사용한 보안 패턴은 난이도(복잡성)를 기준으로 상, 중, 하로 나누었고, 각각 2개의 패턴이 포함되어 있다. ‘상’에 속하는 보안패턴은 별(star)과 영문자 ‘S’이며, ‘중’에 속하는 보안패턴은 삼각형과 사각형, ‘하’에 속하는 보안패턴은 원과 직각삼각형이다. 난이도는 ‘상’, ‘중’, ‘하’로 구분하였지만 대체로 별 모양을 제외하고는 대체로 평이한 패턴이다. 이러한 6개의 보안 패턴을 등록하고, 각각의 패턴에 대해 등록된 패턴과 일치하는 패턴인지 인증하는 실험을 30회씩 총 180회 수행하였으며, 등록된 패턴과 불일치하는 패턴으로 인증하는 실험을 30회씩 총 180회 수행하였다. 여기서 말하는 등록패턴과의 불일치 패턴이란 패턴이 그려지는 위치, 방향, 형태를 각각 변화시킨 패턴이다. 같은 모양이라도 위치가 다르거나, 방향(그려지는 순서)이 다르면 불일치 패턴이라 칭한다.

Table 1은 첫 번째 실험에 대한 실험결과를 부류에 따른 부류에 따른 참긍정(TP), 참부정(TN), 거짓긍정(NP), 거짓부정(FN)의 형태로 구분하여 보여준 것이다. Table 1의 결과에 따라 제안하는 시스템의 참긍정률(TPR)은 92.2%, 참부정률(TNR)은 7.8%, 거짓긍정률(FPR)은 0%, 거짓부정율(FNR)은 100%

Table 1. TP, FN, FP FN of the first experiment

Classification result class	w1(true)		w2(false)	
	Han's System[11]	Proposed System	Han's System[11]	Proposed System
w1(true)	149	166	31	14
w2(false)	0	0	180	180

Table 2. TPR, FNR, FPR FNR of the first experiment

evaluation criteria	Han's System[11]	Proposed System
True Positive Rate	82.2%	92.2%
False Negative Rate	17.8%	7.8%
False Positive Rate	0%	0%
False Negative Rate	100%	100%

라는 결과를 얻었다(Table 2 참조). Table. 2에 보이는 제안하는 시스템의 거짓긍정률과 거짓부정률의 결과를 보면 알 수 있듯이 제안하는 시스템은 잘못된 패턴을 인증하는 경우는 한 건도 없었으며, [11]의 시스템에 비해 참긍정률은 높아졌고 반면 참부정률은 낮아져서 [11]의 시스템보다 성능이 개선되어 있음을 확인할 수 있다.

첫 번째 실험에서 사용된 보안 패턴은 비교적 간단한 것들이었기 때문에 보다 나은 성능 평가를 위해 보다 다양한 종류의 보안 패턴을 대상으로 두 번째 실험을 수행하였다. 이 실험에서는 실제로 암호로 사용될 만한 보안 패턴을 사용하기 위하여 대학생 121명을 대상으로 설문조사를 실시하였다. 설문조사 내용은 움직임 패턴을 이용한 보안시스템에 대한 인식 정도와 본인이 사용자라면 암호를 등록할만한 보안 패턴을 그리는 것이었다. 이 조사를 통해 얻은 보안 패턴들을 실험 영상으로 만들어 두 번째 실험을 수행하였다. 설문조사를 통해 얻은 보안 패턴 중 15가지의 패턴을 추리고, 첫 번째 실험에서와 마

찬가지로 난이도를 ‘상’, ‘중’, ‘하’로 나누어 각각 5개씩 총 15개의 패턴을 대상으로 실험하였다. 두 번째 실험에서 사용한 보안패턴의 형태 이미지는 Table 3에서 확인할 수 있다. 보안 패턴의 방향과 위치는 편의상 표시하지 않았다. 이러한 15개의 패턴에 대해 등록된 패턴과 일치하는 패턴인지 인증하는 실험을 20회씩 총 300회 수행하였으며, 등록된 패턴과 불일치하는 패턴으로 인증하는 실험을 20회씩 총 300회 수행하였다.

Table 4는 두 번째 실험에 대한 실험결과를 부류에 따른 참긍정(TP), 참부정(TN), 거짓긍정(NP), 거짓부정(FN)의 형태로 구분하여 보여준 것이다. Table 3의 결과에 따라 제안하는 시스템의 참긍정률(TPR)은 90.3%, 참부정률(TNR)은 9.7%, 거짓긍정률(FPR)은 0%, 거짓부정율(FNR)은 100%라는 결과를 얻었다(Table 5 참조). 첫 번째 실험에 비해 두 번째 실험에서의 참긍정율이 낮고 참부정율이 높은 이유는 첫 번째 실험에서 사용한 보안 패턴에 비해 더 복잡한 패턴을 사용했기 때문인 것으로 파악된다. 두 번째 실험에서도 제안하는 시스템은 잘못된 패턴을 인증하는 경우는 단 한 건도 없었다.

4. 결 론

본 논문에서는 손동작 인식을 통한 새로운 방식의 보안 시스템을 제안하였다. 제안하는 시스템은 사용자의 암호를 번호나, 지문 등으로 구성하지 않고, 사용자만이 알고 있는 간단하면서 독특한 움직

Table 3. security patterns used in second the experiments

complexity level	form image of the pattern				
High					
middle					
low					

Table 4. TP, FN, FP FN of the second experiment

Classification result class	w1(true)		w2(false)	
	Han's System[11]	Proposed System	Han's System[11]	Proposed System
w1(true)	244	271	56	29
w2(false)	0	0	300	300

Table 5. PR, FNR, FPR FNR of the second experiment

evaluation criteria	Han's System[11]	Proposed System
True Positive Rate	81.3%	90.3%
False Negative Rate	18.7%	9.7%
False Positive Rate	0%	0%
False Negative Rate	100%	100%

입 패턴으로 구성하였다. 사용자의 입장에서 손의 움직임으로 암호를 구성하는 것은 사용자의 거부감이 없으며, 버튼을 누르는 방식에서 발생할 수 있는 혼적(지문)이 남는다는 단점도 보완할 수 있다. 또한 손의 움직임을 인식하는 기술에 있어서도 립모션을 사용함으로써 빛이 없는 어두운 곳에서 제대로 인식할 수 있다는 장점이 있다. 성능에 있어서도 제안하는 시스템은 기존의 유사한 시스템에 비해 개선된 성능을 보임을 확인할 수 있었으며, 잘못된 패턴을 인증하는 경우는 한 건도 없었다. 하지만 보안 패턴의 난이도가 높아질수록 참부정율(거부율)이 생길 가능성이 높아지므로 이를 해결하기 위해서는 방향 특징을 추출하는 방법이나, 형태 이미지를 정합하는 방법에 있어 성능을 향상시킬 수 있는 방향으로 연구가 지속적으로 이루어져야 한다.

REFERENCE

[1] G. Günlü and H.Bilge, "Face Recognition with Discriminating 3D DCT Coefficients," *The Computer Journal*, Vol. 53, No. 8, pp. 1324-1337, 2010.
 [2] M. Radu and T.iberiu Letia, "Fuzzy Logic Method for Partial Fingerprint Recognition," *Proceeding of IEEE International Conference on Automation Quality and Testing Robotics*, pp. 602-607, 2012.

[3] H. Badi and S. Hussein, "Hand Posture and Gesture Recognition Technology," *Journal of Neural Computing and Applications*, Vol. 25, Issu3, pp. 871-878, 2014.
 [4] Y. Zhou, G. Jiang, and Y. LinA, "Novel Finger and Hand Pose Estimation Technique for Real-time Hand Gesture Recognition," *Journal of Pattern Recognition*, Vol. 49, pp. 102-114, 2016.
 [5] H. Park, *Hand Gesture Recognition based Smooth Passenger Interaction of the Future Vehicle*, Master's Thesis of Ulsan University, 2014.
 [6] J. Kim, "A Mouse Control Method Using Hand Movement Recognition," *Journal of Korea Multimedia Society*, Vol. 15, No. 11, pp. 1377-1383, 2012.
 [7] S. Hwang, *A Study on Hand Gesture Recognition System using Dynamic Training*, Master's Thesis of Catholic Kwandong University, 2013.
 [8] K. Kim, *A Study on Hand Gesture Recognition System Using 3D Tracking Volume*, Master's Thesis of Jungang University, 2016.
 [9] S. Park, *Using Principal Component Analysis and Artificial Neural Network*, Master's Thesis of Korea Aerospace University, 2016.
 [10] D. Kim, *C++API OpenCV Programming*, Kame Press, Goyang-si, Gyeonggi-do, 2016.
 [11] J. Han, M. Jeon, and K. Cheoi, "A Security System using a Movement Pattern Drawn with Fingers," *Proceedings of Spring Conference of the Korea Information Processing Society*, Vol. 23, No. 1, pp. 730-732, 2016.



최 경 주

1992년 3월~1997년 2월 충북대학교 컴퓨터학과 학사
1997년 3월~1999년 2월 연세대학교 컴퓨터학과 석사
1999년 3월~2002년 8월 연세대학교 컴퓨터과학·산업시스템공학과 박사

2002년 7월~2005년 2월 LG CNS 연구개발센터
2005년 3월 ~ 현재 충북대학교 전자정보대학 소프트웨어학과 교수

관심분야: 컴퓨터비전, 영상처리, 바이오컴퓨팅, 유비쿼터스컴퓨팅



한 주 찬

2012년 3월~현재 충북대학교 전자정보대학 소프트웨어학과 학사과정

관심분야: 컴퓨터비전, 영상처리