한국컴퓨터정보학회 하계학술대회 논문집 제23권 제2호 (2015. 7)

비인가 접근 사용자 확인을 위한 앱

용승림*, 조혜민*, 이민철°
*°인하공업전문대학 컴퓨터시스템과
e-mail : slyong@inhatc.ac.kr*, jhinnin@nate.com*, mc92lee@naver.com°

An Application for Checking Unauthorized Access User

SeungLim Yong*, Hye-Min Jo*, Min-Cheol Lee°
*°Dept. of Computer Systems and Engineering, Inha Technical College

● Abstract ●

본 논문에서는 스마트폰 인증기법 중 연산기반 패스워드 기법을 통하여 사용자의 접근을 제어하고 비인가 접근자에 대해 얼굴을 촬영하여 비인가 접근 시도를 소유자가 확인할 수 있도록 한다. 우선적으로 사용자 접근 제어를 위해 연산기반 패스워드 기법을 이용하고, 비인가 접근이 확인되는 경우 잠금 기능과 함께 비인가자의 얼굴을 촬영하여 소유자가 비인가자를 확인할 수 있는 카메라 액션을 추가한다. 스마트폰 소유자는 사용자의 접근을 제어하고 비인가자의 접근에 대한 확인을 할 수 있으므로 안전성에 대한 향상을 기대할 수 있다.

키워드: 스마트폰 인증(SmartPhone Authentication), 카메라 액션(Camera Action), 접근제어(Access Control)

I. Introduction

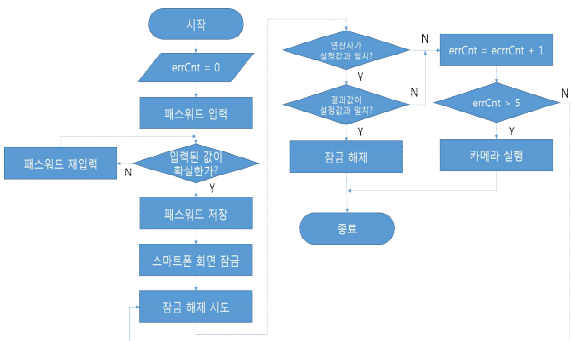
스마트폰의 발전과 함께 PC뿐만이 아닌 스마트폰의 보안에 대해 많은 관심이 비춰지고 있다. 스마트폰 인증은 인가된 사용자만이 접근하고 비인가자의 접근을 제한하는 기능을 한다. 스마트폰 인증의 종류에는 '패턴', 'PIN 혹은 비밀번호', '제스처' 등이 있다[1].

본 논문에서는 사용자에 대한 접근제어 기능에 더불어 비인가자의 인증 시도를 확인하는 기능을 추가하여 안전성이 높은 인증기법을 구현하고자 한다. 연산기반 패스워드 기법을 통하여 사용자 접근을 제어하고 얼굴 촬영기능을 통하여 비인가 시도를 확인한다. 구현하는 인증기법은 일정 횟수 연산자 혹은 입력한 수의 연산 결과 값이 설정한 값과 다를 때 전면 카메라를 이용하여 비인가자의 얼굴을 촬영하여 설정한 자신의 스마트폰에 저장하고 추후 소유자가 확인할 수 있는 기능을 구현한다.

II. Proposed Application

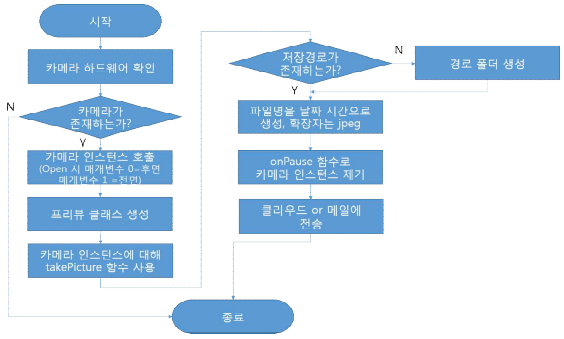
1) 개념 및 기능 설명

사용자 접근 제어를 위하여 연산기반 패스워드 기법을 이용한다. 연산기반 패스워드는 연산자와 연산 값을 설정하여 잠금을 해제할 때 연산자와 입력한 수의 연산 결과 값이 일치하는지 확인하는 방법으로 사용자를 인증하는 패스워드 기법이다[2]. 이 기법에서는 인증이 통과되지 않으면 사용자의 스마트폰을 일정 시간 잠그는 기능을 수행한다. 제안하는 구현에서는 비인가 접근이 확인 되는 경우 잠금 기능에 비인가자의 얼굴을 촬영하여 소유자가 비인가자를 확인할 수 있는 카메라 액션을 추가한다. 설정과 해제. 그리고 카메라 액션에 대한 전체적인 흐름도는 [그림1]과 같다.

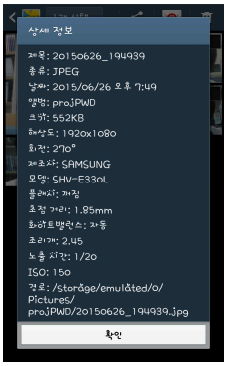


Flow chart

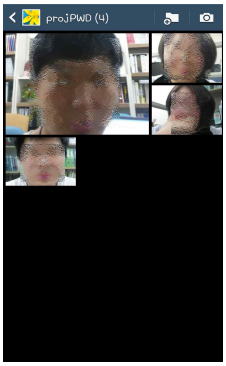
스마트폰에 있는 전면과 후면의 카메라 중 비인가자의 얼굴 촬영을 위하여 전면 카메라를 이용하여 구현한다. 카메라 실행을 위한 인스턴스를 호출하고 Open 함수를 사용할 때 매개변수를 전면 카메라에 해당하는 1을 입력받는다. 인스턴스를 호출한 뒤 프리뷰를 생성하고 촬영 함수를 호출하여 촬영하고 저장 경로에 저장한다. 이 때 저장 경로가 존재하지 않는 경우 폴더를 새로 생성한 후 사진을 저장하고 종료한다. 카메라 액션에 대한 흐름도는 [그림2]와 같다.



Flow Chart of Camera Action



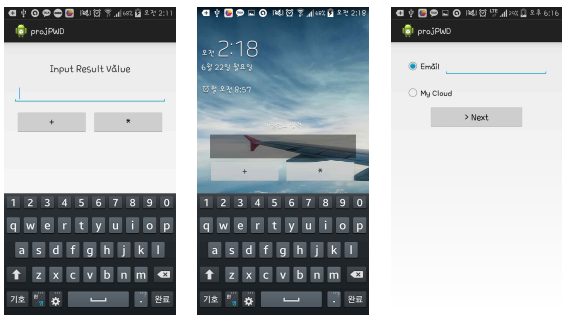
Stored Pictures



File name

2) 구 현

처음 패스워드를 설정할 때 자신이 원하는 연산 값을 입력한 후 연산자 버튼을 클릭했을 때 다이얼로그가 출력된다. 설정이 종료되면 사용자는 연산자와 숫자만의 입력으로 인증을 시도한다. 인증에 대한 구현 결과 화면은 [그림 3]과 같으며 구현 환경은 Eclipse Kepler, JDK 1.7 이고 Galaxy S4 LTE-A, Android 4.4.2 Kitkat에서 실행하였다. 자신이 잘못 설정하지 않았다면 다음을 클릭하고 입력 값이 5회 이상 틀릴 경우 사진을 받을 자주 사용하는 매체를 지정한다. 5회 틀릴 시 자동으로 전면 카메라를 실행한다. 이 때 비인가자는 프리뷰 클래스를 사용하지 않고 촬영을 하였기 때문에 자신의 얼굴이 촬영되는지 여부를 알 수 없다. 스마트폰 소유자는 기본 갤러리 앱을 통하여 비인가자의 얼굴과 촬영시간을 확인할 수 있다. 구현의 결과 화면은 [그림4], [그림5]와 같다.



a)setting password b)set storage c)unlock password
Dialog for User Authentication

III. Conclusions

본 논문에서는 비인가자에 대한 접근 제어와 더불어 비인가자를 확인할 수 있는 기능을 수행하는 어플리케이션을 구현하였다. 타인이 자신의 패스워드를 풀기 위해 시도할 때 특정 횟수 이상 잘못 입력하면 비인가자의 얼굴을 촬영하고 저장하여 스마트폰 소유주가 이를 확인할 수 있다. 추후에 스마트폰 분실 시 활용할 수 있는 기능 확장을 위하여 잠금 해제를 시도하는 비인가자의 위치정보와 사진을 클라우드 혹은 자신의 이메일로 전송하는 기능을 추가하고자 한다.

References

[1] http://samsungsimulator.com/

[2] A Password Scheme based on Calculation Resistant to Smudge and Shouder Surfing Attack, Proceedings of KSCI Conference, 2014.