韓國컴퓨터情報學會 論文誌
第16卷 第6號, 2011. 6.

2011-16-6-3-4

스마트폰 사용자 인증을 위한 카메라 영상 프레임 비교에 관한 연구

장 은 겸*, 남 석 우**

Study on the Camera Image Frame's Comparison for Authenticating Smart Phone Users

Eun-Gyeom Jang*, Seok-Woo Nam**

요 약

스마트폰을 기반으로 한 앱은 병원의 의료 서비스, 은행 및 카드사의 금융서비스, 기업 및 가정의 유비쿼터스 기술 등 다양한 영역에 활용되고 있다. 이러한 서비스 환경에서 외부인에 의한 스마트폰의 불법적인 노출은 공·사적 정보의 유출을 포함한 자산의 손실이 발생한다. 이를 위한 보호 기법으로 비밀키 및 패턴 인식 기술, 정적인 단일 영상 인증 기법이 적용되고 있으나 정적인 키 값의 유출 또는 사진과 같은 영상을 활용하여 접근이 가능하다는 문제를 가지고 있다.

본 논문에서는 이러한 위험요소 및 문제로부터 스마트폰을 보호하기 위한 기술로 사용자 얼굴 인증 기술을 제안한다. 제안 기술은 사용자의 얼굴 동영상의 키 프레임을 실시간으로 추출하여 사용자를 인증하고 스마트폰의 접근을 제어한다. 인증 정보는 다수의 키 프레임으로 구성되며, 영상의 화소 및 휘도의 DC 값을 활용한 유사도 판별 알고리즘으로 사용자의 접근을 통제한다.

▸ Keyword : 스마트폰, 얼굴인식, 영상, 비교, 인증

Abstract

APP based on the smart phone is being utilized to various scopes such as medical services in hospitals, financing services at banks and credit card companies, and ubiquitous technologies in companies and homes etc. In this service environment, exposures of smart phones cause loss of assets including leaks of official/private information by outsiders. Though secret keys, pattern recognition technologies, and single image authentication techniques are being applied as protective methods, but they have problems in that accesses are possible by utilizing static key

• 제1저자 : 장은겸 • 교신저자 : 남석우
• 투고일 : 2011. 02. 01, 심사일 : 2011. 02. 24, 게재확정일 : 2011. 03. 17
* 대전대학교 컴퓨터공학과(Dept. of Computer Science, Daejeon University)
** 혜천대학 컴퓨터정보학과(Dept. of Computer Information, Hyechon College)

values or images like pictures.

Therefore, this study proposes a face authentication technology for protecting smart phones from these dangerous factors and problems. The proposed technology authenticates users by extracting key frames of user's facial images by real time, and also controls accesses to the smart phone. Authentication information is composed of multiple key frames, and the user's access is controlled by distinction algorism of similarity utilizing DC values of image's pixel and luminance.

▸ Keyword : Smart Phone, Face cognition, Image Compare, Authentication

I. 서 론

스마트폰 시장의 주축을 이루는 아이폰은 블루투스와 GPS 모듈을 탑재한 이동형 단말기이다. 기술적인 측면에서 기존의 WinCE를 탑재한 HP의 단말장치, 블랙베리, 심비안에 비해 뛰어난 스펙이 아니었음에도 불구하고 스마트폰 시장에 각광을 받고 있다. 이것은 폰 단말의 기술 보다는 아이폰과 결합된 어플리케이션의 집합인 앱스토어가 중요한 방점을 가진다는 것이다. 특히 국내에서 가장 많이 사용하던 윈도우 모바일의 계열과 가장 큰 차이였다. 구글의 안드로이드 플랫폼, Bada 플랫폼, Windows Phone의 환경에서 다양한 앱이 제공되어 현재의 스마트폰 시장을 구축하고 있다[1,2].

스마트폰은 '내 손안의 인터넷', '내손안의 PC', '내손안의 휴대폰'의 기능을 포함한 통합 기술 매체이다. 또한 다양한 병원의 의료 서비스, 은행 및 카드사의 금융서비스, 기업 및 가정의 유비쿼터스 기술이 적용되어 유용하게 활용되고 있다. 이렇게 집중된 기능을 갖고 있는 스마트폰은 개인 및 기업, 가정 등에 필요한 기능 및 정보를 포함하고 있다.

그러나 역기능으로 악성코드를 포함한 불법적인 매체 및 콘텐츠 접근에 의해 피해 사례가 발생하고 있다. 또한 다양한 앱 서비스와 사용자 인증서 등의 예민한 정보가 스마트폰에 탑재되어 있어, 타인에 의한 불법적인 스마트폰 접근은 자산 및 산재가 발생할 수 있다. 그러므로 이러한 위험요소로부터 스마트폰을 보호하기 위한 기술이 필요하다[2,3].

현재, 스마트폰 접근 제어 기술은 비밀키 및 패턴 인식에 의한 접근 방식을 활용하고 있고, 사용자의 얼굴을 인식하는 방식을 제공하기도 한다. 그러나 비밀키 및 패턴 인식 방식은 정적인 키 값을 활용하고 있어 키 값의 유출로 스마트폰의 안전성은 보장하지 못한다. 또한 현재 얼굴 인식 기술은 사용자의 얼굴 영상을 캡쳐하여 정지 영상 프레임을 사용자의 인증 정보와 비교하는 기법으로 사진과 같은 영상을 활용한 스마트폰 접근의 문제를 가지고 있다.

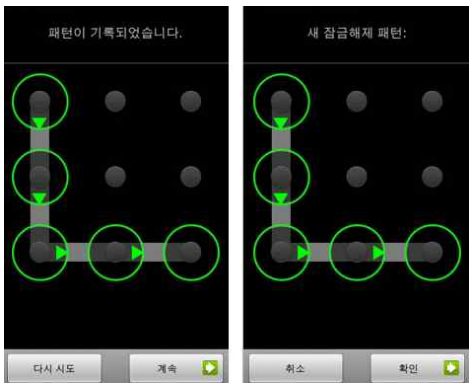
이러한 기존 기술의 문제로부터 스마트폰의 불법적인 접근을 방지하기 위해 본 논문에서는 사용자의 얼굴 영상을 동영상으로 실시간 인증하는 기법을 제안한다.

II. 스마트폰 및 영상 관리 기술 분석

1. 기존 스마트폰 기술의 문제점

현재 스마트폰의 사용자 인증을 위한 인터페이스 기술 영역은 터치 인터페이스와 시각인식 기술이다. 터치 인터페이스는 키패드의 비밀키 입력(그림 1)에 따른 스마트폰 접근을 통제하고 있다. 최근 변형된 인터페이스로 패턴을 인식하는 접근 방식이 있다. 패턴 인식 기술(그림 2)은 터치 패드에 이미지가 형성되어 순서적인 이미지 터치에 의해 접근하는 방식이다.

<그림 1> 비밀번호 인식
<Fig.1> Password recognition



<그림 2> 스마트폰 패턴인식
<Fig. 2> Smartphone pattern recognition

시각인식 기술은 스마트폰의 카메라를 활용하여 스캐너처럼 데이터를 인식하는 기술과 바코드 및 QR 코드를 인식하는 기술이 있다. 또한 최근 스마트폰 얼굴 인증 솔루션을 (주)그린정보기술[4]에서 출시하였다.

<그림 3> GFR-S V1.0 테스트
<Fig. 3> GFR-S V1.0 test

(주)그린정보통신에서 출시한 스마트폰 얼굴 인증 솔루션(그림 3)은 스마트폰에 내장된 카메라를 이용하여 얼굴을 인증하고 별도의 추가 장비가 불필요하다. 강화된 보안 기능으로 사용자 본인의 얼굴특징 분석을 통한 인증으로 타인의 대리인증 불가능, ID, P/W, 공인인증서 등의 분실 및 도용 등에 대한 보완적 보안성 강화, 본인 인증 로그인 시도에 대한 얼굴이미지 이력 기록(얼굴이미지 확인을 통한 보안 관리 강화)의 특징을 갖는다. GFR-S V1.0[4]은 사용자의 얼굴을 인식하여 하나의 이미지로 저장한다. 저장된 이미지는 사용자의 얼굴을 실시간으로 인증하기 위한 인증 정보로 활용된다. 사용자가 인증을 요청하면 인증 요청 이미지와 인증 정보 이미지를 비교하여 사용자를 인증하는 기법이다.

이와 같이 현재 연구 개발된 기술은 스마트폰의 다양한 서비스에 비해 많은 보안의 허점을 갖는다. 비밀키 입력 방식은 정적인 키 값을 갖는다. 정적인 키 값은 타인에게 유출되어 오용될 수 있다는 문제점을 갖는다. 또한 이러한 방식의 변형된 모델로 패턴을 인식하여 스마트폰 접근을 통제하는 기술이 나왔다. 패턴 값은 다양한 변화를 줄 수 있으나 그 변화된 입력 패턴은 정적인 키 값의 특징을 벗어 날 수는 없었다. 즉, 기존의 비밀키 입력 방식의 인터페이스만 다르다는 것이다. 비밀키 입력 방식은 텍스트 기반으로 운영되고 패턴인식 기술은 GUI 환경의 인터페이스 차이인 것이다. 또한 기존 연구된 스마트폰 얼굴 인식 기술은 사용자의 생체인식 기술로서 얼굴 이미지를 활용하여 인식률이 높은 실험 결과를 얻었다. 그러나 정지 영상을 활용한 이미지 인증 기법으로 사진과 같은 매체로 인한 접근 문제를 갖는다는 것이다[5].

이러한 문제를 보완하기 위해 생체인식 기술의 하나의 영역인 얼굴 인증 기술을 본 논문에서는 제안한다. 본 제안 기술은 사용자의 인증 정보 및 실시간 인증 데이터를 동영상으로 여러 개의 키 프레임을 추출하여 비교하는 기법을 제시하고 각 키 프레임의 영상 정보를 비교하여 인증하기 위한 영상 비교 알고리즘을 제안한다.

2. 영상 검출 기술

2.1 화소단위 비교법과 히스토그램 비교법

화소단위 비교 방법[6]은 동일한 샷 내에서는 화소 값의 변화가 적다는 성질을 이용하는 것으로 식 1에서 $F_i(x,y)$는 i 번째 프레임에서 (x,y)의 화소 값이고, 이때 인접하는 프레임의 대응하는 화소 값의 차가 임계값 t를 초과하는 경우 1로 된다.

$$DP_i(x,y) = \begin{matrix} 1 & \text{if}\,|F_i(x,y) - F_{i+1}(x,y)| > t \\ 0 & otherwise \end{matrix} \qquad (1)$$

식 2에서 전체 화소에 대한 1로 된 화소의 비율이 특정 임계값 Tp를 넘으면, 컷으로 간주한다. X, Y는 이미지의 최대 높이와 넓이를 표시한다.

$$\frac{\sum_{x,y=1}^{X,Y} DP_i(x,y)}{X * Y} * 100 > T_p \qquad (2)$$

이러한 화소 단위 비교 방법은 카메라의 움직임과 물체의 움직임에 따라 잘못된 장면전환을 많이 검출한다. Fade와 Zoom in/out과 같은 카메라 이동, 그리고 물체의 이동은 많은 화소의 변화를 가지고 오고, 결국 잘못된 장면전환을 검출하는 결과를 보이게 된다.

히스토그램 비교 방법[6]은 동일한 샷 내의 프레임들은 서로 유사한 색상분포를 가진다는 특성을 이용한 가장 보편적인 검출방법으로 식 3과 같이 동영상에서 인접한 프레임들의 히스토그램 차이를 계산하여 주어진 임계값 T_h와 비교함으로서 장면전환을 검출하게 된다. 여기서 i 는 프레임 번호를 나타내고, j 는 히스토그램 상의 색상 값을 나타낸다. 또한, H는 주어진 색상 값에 대한 빈도수를 나타낸다.

$$D_i = \sum_{j=1}^{N} | H_i(j) - H_{i+1}(j) | T_h \quad (3)$$

히스토그램 비교 방법은 빠르게 물체가 움직여도 전체의 히스토그램의 변화는 크게 변하지 않기 때문에 화소단위 비교 방법보다 움직임에는 정확한 장면전환을 검출할 수 있다. 그러나 히스토그램 비교 방법은 밝기 변화에 잘못된 장면전환을 검출할 수 있다. 즉, 갑작스런 조명변화나, 섬광, 비슷한 배영이나 분위기에는 잘못된 장면 전환을 검출할 수 있다[7,8].

2.2 엔트로피를 이용한 비교방법

영상 정보의 복잡도를 확률에기반한 엔트로피로 나타내면 식 4와 같다. 이 엔트로피를 이용하면 영상의 복잡도를 측정할 수 있다.

$$E=-\sum_{j=0}^{K} P(a_j)\log P(a_j) \quad (4)$$

여기서 a_j는 j번째 화소 값의 개수이며, $P(a_j)$는 a_j의 확률이다. 동영상에서는 연속하는 두 프레임간의 엔트로피 차이를 측정하여 프레임 차이를 판별한다. 급격한 조명변화가 생겼을 때, 컬러 히스토그램의 분포는 크게 차이가 난다. 그러나 물체나 배경, 혹은 영상 전체의 밝기 변화가 생기더라도 그 영상의 복잡도는 크게 변하지 않기 때문에 엔트로피 값이 크게 변하지 않는다. 따라서 연속되는 두 프레임간의 엔트로피 차이를 사용하면 조명 변화로 인한 잘못된 장면검출을 막을 수 있다. 그래서 컬러 히스토그램과 엔트로피 비교 방법을 함께 사용하여 두 프레임간의 컬러 히스토그램과 엔트로피의 차이를 구하여 D_{total} 이 임계값을 넘을 때에 장면전환으로 간주한다.

식 5는 연속되는 두 프레임간의 엔트로피 차이를 나타내며 식 6은 컬러 히스토그램 차이를 D_h라 했을 때 식 5의 엔트로피 차이를 D_e를 결합한 전체 차이를 나타낸다. 이는 두 프레임간의 차이가 컬러 히스토그램의 차이와 엔트로피 차이의 합으로 나타낼 수 있음을 뜻한다.

$$D_e = E_m - E_{m+1} \quad (5)$$

$$D_{total} = D_h + wD_e \quad (6)$$

$$D_{total} > T_e \quad (7)$$

여기서 w는 가중치이며, 두 프레임간의 차이가 식 7과 같이 어느 임계값을 넘으면 장면전환으로 간주한다. 엔트로피 방법은 갑작스런 조명변화에 잘못된 장면전환을 검출하지 않지만 fade처럼 점점 어두워지거나 밝아지면 장면전환을 판별하게 된다[7,9].

2.3 압축 영역에서 에지 영상을 이용한 비교 방법

식 8과 같이 AC 계수들 중 저주파에 해당하는 5개의 계수를 이용해 저주파 에지 강도, P_L를 계산하고 이를 임계값과 비교해 에지 블록을 구함으로서 에지 영상을 얻어내었으며 식 9에서와 같이 움직임이 보상된 참조 프레임의 수평, 수직방향의 에지 히스토그램, P_H', P_v'와 현재 프레임의 수평, 수직방향의 에지 히스토그램, P_H, P_V를 비교하여 장면전환검출을 시행하였다.

$$P_L = F_{01}^2 + F_{10}^2 + F_{02}^2 + F_{20}^2 + F_{11}^2 \quad (8)$$

$where, F_{i,j}$: (i,j) 위치의 DCT 계수

$$d(k, k+1) = \sum_{x=0}^{M-1} |P_H(x+u) - P_H(x)| + \sum_{y=0}^{N-1} | P_V(y+v) - P_v(y) | \quad (9)$$

$where, M, N$: 에지 영상의 가로, 세로 크기
u, v : 수평, 수직 방향의 움직임 벡터

DCT 계수의 특성상 AC 계수를 이용하여 복원하는 경우보다 더 정확한 에지 영상을 얻을 수 있고 따라서 장면전환검출 결과가 좋은 장점이 있다.

밝기 값이 변하는 블록에서는 DC 계수의 코드길이(MPEG 신택스에 포함되어 있는 dct_dc_size)가 길어진다

는 특징을 이용해 dct_dc_size의 크기를 디코딩하여 에지 블록을 구한 후 에지 영상을 복원하고 이를 장면전환검출에 적용하였다. 이 방법은 알고리즘에 사용되는 데이터를 얻기 위한 디코딩 과정이 줄어드는 장점이 있다.

2.4 압축된 비디오에 대한 장면전환 추출

압축된 비디오 데이터는 압축 정보로 DCT계수와 움직임 벡터를 가지고 있다. DCT 계수는 복원된 영상의 화소의 세기와 색차에 해당하는 정보로 압축된 데이터에서 장면전환을 추출하는데 쉽게 사용할 수 있고, 그 정확성도 신뢰할 수 있으므로 필수 정보로 사용된다. MPEG 스트림으로부터 해당 화면정보만으로 부호화한 I 프레임을 포착하여 이웃하는 프레임 간의 차는 각 DCT블록의 차에 대한 합으로 식 10을 이용하여 구한다.

$$D_k = \sum_{x=0}^{44}\sum_{y=0}^{30}(B_{k+1}[x][y] - B_k[x][y]) \quad (10)$$

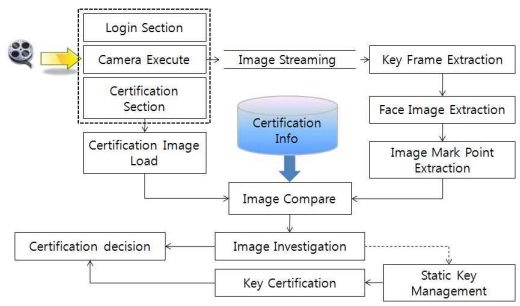
이때, 장면전환 프레임을 추출하기 위한 임계값을 전체 영상의 통계적 특성을 이용하여 평균(M)과 표준편차(STV) 또는 분산값(V)에 가중치 a를 적용한 식 11에 의해 구한다.

$$\text{임계값} = M + a \times [STV \text{ or } V] \quad (11)$$

III. 스마트폰 사용자 인증 기술

1. 시스템 구성

사용자 인증을 위해 로그인 모듈이 작동하여 사용자의 영상을 입력 받는다. 영상은 스마트폰의 카메라에 의해 입력되어 스트리밍 방식으로 동영상의 키 프레임을 추출한다. 사용자 인증 모듈의 구성은 그림 4와 같다.



<그림 4> 사용자 인증 모듈 구성
<Fig. 4> User authentication module configuration

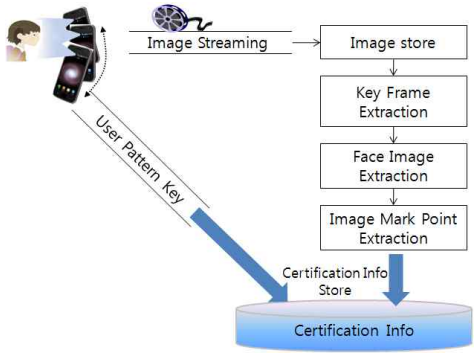
모듈은 로그인 세션을 관리, 카메라 영상 처리, 영상 추출 및 검증 영역으로 구분할 수 있다. 세부 모듈의 기능은 다음과 같다.

- Login Section: 시스템의 로그인 인터페이스를 관리하고 기능 모듈을 관리한다. 그리고 최종 인증 정책 및 로그인 검증을 결정한다.
- Camera Execute: 사용자의 인증 영상(얼굴 영상)을 입력 받는 기능을 수행한다.
- Certification Section: 등록된 인증 영상 및 정정 키 관리를 수행하며 인증 정보와 입력 정보를 비교하는 기능을 수행한다. Certification Info Database에 등록된 인증 영상을 로드하고 영상을 비교하는 기능을 수행한다.
- Key Frame Extraction: 인증을 요하는 입력 동영상의 키 프레임을 추출한다.
- Face Image Extraction: 추출한 키 프레임 영상의 얼굴 영역을 추출한다.
- Image Mark Point Extraction: 얼굴 영상의 특징점을 추출한다.
- Image Compare: 추출한 얼굴 영상의 특징점을 Certification Info Database에 등록된 인증 정보와 비교한다.
- Image Investigation: 비교 영상에 대한 검증 결과를 추출한다.
- Static Key Management, Key Certification: 정적인 비밀키(키 패턴)를 적용하여 사용자를 인증한다.
- Certification decision: 검증 결과 값과 정적 비밀키 확인 정보를 이용하여 사용자 인증을 결정한다.

사용자 인증을 위한 비밀키 및 영상은 인증 정보로 사전에 Certification Info Database에 등록되어야 한다. 인증 정보를 저장 모듈 구성은 그림 5와 같다. 사용자 인증 영상은 동영상으로 스트리밍 방식으로 스마트폰의 임시 메모리에 저장된다. 저장된 영상은 영상의 키 프레임을 추출한다. 추출된 키 프레임은 얼굴 영상을 추출하고, 추출된 얼굴 영상 영역에서 특징점을 찾아 사용자의 패턴 비밀키와 함께 Certification Info Database에 저장한다.

특징점은 얼굴의 눈, 코, 입의 위치 정보를 가지며 각 특징점간의 위치 비율 정보를 갖는다. 입력된 동영상은 정적인 영상에 약점을 보완하여 좌에서 우로 스캔하는 방식을 적용하여 스트리밍에 의해 입력된 영상의 키 프레임을 추출한다. 키 프레임은 영상 변화에 의한 방식과 시간 단위 키 프레임 생성

방식을 적용한다.

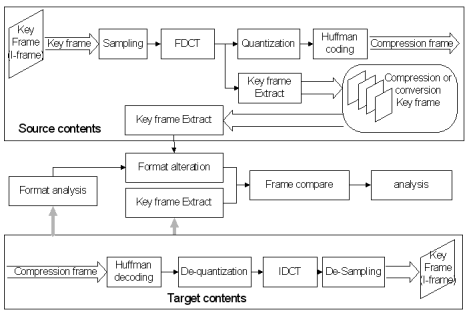


<그림 5> 인증 정보 관리
<Fig. 5> User authentication Management

2. 키 프레임 추출 및 비교 알고리즘

키 프레임은 Sampling에 의해 색상체계가 변환되고, 변환된 데이터를 코사인 함수로 변환하여 양자화 절차를 갖는다. 양자화 과정에 의해 데이터의 손실을 일으키므로 이전 데이터인 DCT 과정에 의해 얻은 결과 데이터를 추출하여 콘텐츠 인증 데이터로 추출한다. DCT 과정으로 얻은 결과 데이터를 허프만 코딩에 의해 압축을 하여 관리하면 압축효율을 발휘함으로서 허프만 코딩에 의해 압축하여 관리한다. 그림 6은 콘텐츠 키 프레임 추출 및 비교 알고리즘이다.

Source Contents는 사용자 인증 원본 콘텐츠이고 Target Contents는 실시간으로 인증을 요청하는 콘텐트이다. "format analysis"는 인증을 요청하는 콘텐츠의 포맷을 분석하고 "Key frame extract"에 의해 영상의 키 프레임이 추출된다. 추출된 키 프레임은 "format alteration"에 의해 이미지 포맷을 변경한다. 변경 크기는 24*24의 고정 크기를 갖는다. 변경된 영상은 제안한 영상 비교 알고리즘에 의해 유사도를 추출(frame compare)하여 결과를 분석(analysis)한다.



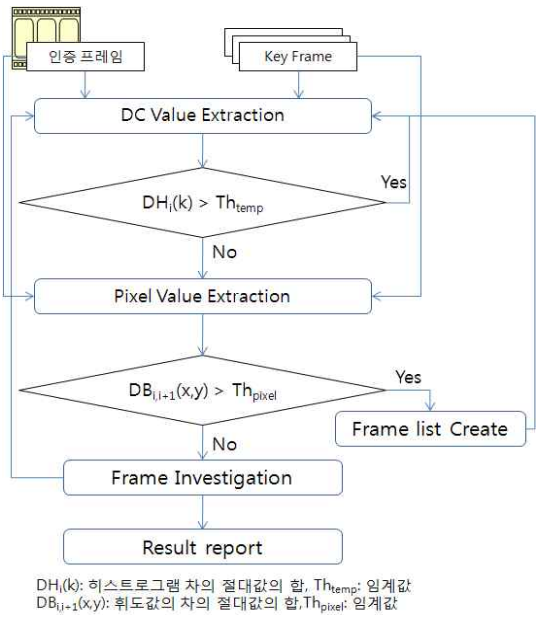
<그림 6> 콘텐츠 키 프레임 추출 및 비교 알고리즘
<Fig. 6> Content key frame extraction and comparison algorithm

3. 키 프레임 유사도 판별

프레임 비교 알고리즘(그림 7)은 색차블록의 DC 값을 이용하여 DH(Difference of Histogram) 비교 알고리즘을 적용한다. 1차 비교 알고리즘은 프레임의 색차 블록의 DC 값을 추출하여 인증 영상 키 프레임과 대상 키 프레임의 값을 비교하여 임의의 임계값과 비교한다.

값 비교에 의해 얻은 결과가 임계값 보다 작으면 유사한 프레임으로 보고, DB(Difference of Brightness) 비교 알고리즘을 적용한다. DB 비교 알고리즘은 화소값을 이용하여 인증 영상 프레임과 대상 키 프레임을 비교하여 얻은 결과를 임의의 임계값과 비교하여 작은 결과를 얻으면 프레임이 유사한 것으로 최종 결정한다. 또한, DB 비교 알고리즘에서 임의의 임계값 보다 큰 값을 얻었을 때의 경우에는 유사한 프레임으로 인지하여 정당한 사용자임을 인증한다.

키 프레임 비교는 두 가지 기법을 이용한다. 화소값 차이를 이용한 비교 방법과 색상분포의 유사성의 성질을 이용한 비교 방법을 활용한다. 프레임 비교에 두 개의 알고리즘을 활용하는 것은 화소값의 차이를 이용하는 기법은 개체의 이동이나 프레임의 잡음에 민감한 특성을 가지고 있고, 색상블록의 DC 값을 이용하는 기법은 조명 변화가 다양한 영상에는 비효율성을 갖기 때문이다.



<그림 7> 프레임 유사성 비교 알고리즘
<Fig. 7> Frame similarity comparison algorithm

3.1 색상블록의 DC 값을 이용한 프레임 유사성 비교 알고리즘

DH 프레임 비교 기법은 프레임간의 색상블록의 DC값을 이용한 프레임 유사성 비교 알고리즘은 식 12와 같다.

$$DH(k) = \sum_{k=0}^{K-1} |H(k) - T_j(k)| > Th_{temp} \quad (12)$$

K: 휘도 or 컬러 레벨의 총 개수

$H(k)$: 인증 영상 프레임의 k 휘도값을 갖는 히스토그램 함수

$|H(k) - T_j(k)|$: 원본 인증 영상 프레임과 대상 j 번째 프레임간의 k 휘도값을 갖는 히스토그램의 차의 절대값

$DH_j(k)$: 원본 인증 영상 프레임과 대상 j 프레임간의 유사성을 나타내는 히스토그램의 차의 절대값의 합

Th_{temp} : 유사성 임계값

$DH_j(k)$ 값이 작게 나타나면 유사성이 있는 프레임으로 판단하고, $DH_j(k)$ 의 값이 크면 유사성이 없는 것으로 판단한다. 유사성의 판단 기준은 임의의 임계값 Th_{temp}에 의해 결정된다.

임계값 보다 작은 $DH_j(k)$ 의 프레임은 2차 프레임 비교 알고리즘을 적용한다. 1차 비교 알고리즘은 색상의 밝기에 비효율적으로 검출을 하기 때문에 2차 비교 알고리즘을 적용하여 1차 비교 알고리즘의 단점을 보완한다. 또한, 임계값 보다 큰 $DH_j(k)$ 의 프레임은 유사성이 없음을 판별하고 차기 프레임을 읽어 들여서 1차 프레임 비교 기법을 적용시킨다.

3.2 화소의 차를 이용한 프레임 유사성 비교 알고리즘

DB 비교 알고리즘는 DH 비교 알고리즘의 결과로서 $DH_j(k)$ 의 값이 임계값 보다 작을 경우에 적용되는 알고리즘이다. DB 프레임 비교 알고리즘은 화소를 이용하여 유사성을 검출하는 알고리즘이다.

화소의 차를 이용하는 방법은 동일한 위치에 있는 두 프레임의 화소값들의 차의 절대값의 합이 일정한 임계값을 초과할 경우에 유사성이 없는 프레임으로 판단한다. 즉, 사용자를 인증하지 못 하는 경우이다. 화소값의 차를 이용한 유사성 검출은 식 13에 의해 얻어진다.

$$DB_j(x, y) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \Delta P_j(x, y) > Th_{pixel} \quad (13)$$

M: 수직 방향의 픽셀수

N: 수평 방향의 픽셀수

$P(x,y)$: 프레임의 (x,y) 점의 픽셀의 휘도값

$\Delta P_j(x,y)$: $|P(x,y) - P_j(x,y)|$ 으로 인증 프레임과 j 프레임의 (x,y) 점의 픽셀의 휘도값의 차의 절대값

$DB_j(x,y)$: 인증 프레임과 j 프레임간의 유사성을 나타내는 휘도값의 차의 절대값의 합

Th_{pixel} : 유사성 임계값

유사한 프레임의 경우 픽셀 차이는 매우 작은 값을 갖는다. 그러나 유사성이 없는 프레임의 경우에는 픽셀 차가 크게 발생한다. 이렇게 발생한 픽셀의 유사성은 임의의 임계값을 이용하여 유사성을 판단한다.

임계값(Th_{pixel}) 보다 $DB_j(x,y)$ 의 값이 큰 경우, 유사 프레임이 아님을 판명한다. 그러나 1차 프레임 비교 알고리즘에서 유사하다고 판별된 프레임이므로 재검토의 필요성이 있으므로 해당 프레임의 정보를 다시 확인할 수 있도록 보관하여 관리한다. 또한, 임계값 보다 Th_{pixel}의 값이 작을 경우에는 1차와 2차의 프레임 비교 기법을 통해 유사성이 판별되었으므로 정당한 사용자임을 인증 한다.

물론, DH와 DB 프레임 비교 알고리즘은 임계값에 의존한다. 임계값을 작게 설정하였을 경우에는 좀 더 정확성을 높일 수 있으나, 정당한 사용자를 판별하지 못하는 경우가 발생한다. 또한, 임계값을 크게 하였을 경우에는 정당한 사용자와 유사한 경우에 식별하지 못하는 결과를 도출한다. 이러한 임계값은 알고리즘 성능 평가에서 임계값을 조절하면서 실험 평가를 하여 최적의 임계값을 찾는다.

IV. 실험 및 평가

1. 프레임 검출 실험

사용자 인증은 사용자의 실시간 영상 프레임과 스마트폰에

저장된 인증 영상을 비교한다. 사용자 인증 정보의 영상은 안경과 모자 등의 부유물을 착용하지 않은 상황에서 인증 정보를 생성하였다. 프레임 검출 실험은 다음과 같은 시나리오를 기반으로 테스트하여 DH와 DB Extraction Value를 분석하였다.

- 상황 A: 정당한 사용자가 사용자 인증을 요청한 상황
- 상황 B: 정당한 사용자가 안경을 착용하여 인증을 요청한 상황
- 상황 C: 정당하지 않은 사용자가 접근하여 인증을 요청한 상황
- 상황 D: 정당한 사용자의 얼굴 이미지(사진)를 활용하여 인증을 요청한 상황

① 상황 A

스마트폰에 등록된 인증 정보의 동일인이 인증을 요청하는 상황으로 사용자 얼굴 스캔 기법을 그대로 적용하였을 때 실험이다. DH는 0.94~0.99의 범위 값, DB는 0.89~0.99의 범위 값을 추출하였다. 0.968과 0.953의 평균값을 각각 추출하였다.

② 상황 B

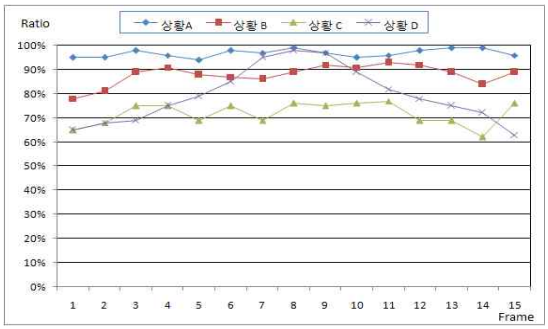
스마트폰에 등록된 인증 정보의 동일인이 모자나 안경을 착용한 후 인증을 요청한 상황으로 실험에서는 안경을 착용한 상태에서 실험하였다. DH는 0.78~0.93의 범위 값, DB는 0.75~0.94의 범위 값을 추출하였다. 0.879와 0.881의 평균값을 각각 추출하였다.

③ 상황 C

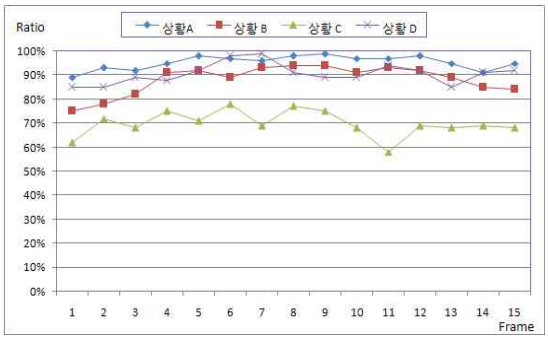
스마트폰에 등록된 인증 정보와 다른 사용자가 인증을 요청했을 때 상황 실험이다. DH는 0.62~0.77의 범위 값, DB는 0.58~0.78의 범위 값을 추출하였다. 0.717과 0.698의 평균값을 각각 추출하였다.

④ 상황 D

스마트폰에 등록된 인증 정보의 동일인의 사진을 이용하여 인증을 요청한 상황이다. DH는 0.63~0.98의 범위 값, DB는 0.85~0.99의 범위 값을 추출하였다. 0.793과 0.906의 평균값을 각각 추출하였다.



<그림 8> DH 추출 값
<Fig. 8> DH Extraction Value



<그림 9> DB 추출 값
<Fig. 9> DB Extraction Value

2. 실험 결과 분석

상황 A/B/C/D에 의한 시나리오 실험은 그림 7, 그림 8과 같은 결과를 얻었다. 위의 실험은 임계값(Thtemp)을 추출하기 위한 실험 모델이다. 실험 결과를 분석하면 다음과 같다.

- 정당한 사용자 인증: DH의 경우 94%의 유사도를 추출하고 DB는 89%이상의 유사도 추출하였다.
- 안경 착용 및 정지영상(사진)에 의한 인증: DH의 값은 98%이하의 유사도를 추출하였고, DB는 99%이하의 유사도를 추출하였다.
- 부당한 사용자 인증: DH와 DB는 78%이하의 유사도를 추출하였다.

각 상황에 따른 최대 및 최소 유사도 추출 값은 명확한 구분이 되지 못한다. 그러나 "정지영상(사진)에 의한 인증"은 곡선의 그래프 유형을 파악할 수 있고 상황 A에 대한 결과 값과는 차이가 있는 것을 볼 수 있다.

3. 성능 분석

실험 결과, 정당한 사용자 인증에 의한 유사도 추출 최소값은 DH는 94%, DB는 89%이고, 정당하지 않은 사용자 인증의 유사도 추출 최대값은 DH와 DB 모두 78%이하이다. 또한, 평균 95%의 값과 약 67%의 유사도를 추출하였다. 정당한 사용자와 정당하지 않은 사용자의 접근에 대한 인증은 실험 결과 명확하게 구분이 된다. 그러나 안경을 착용한 실험과 사진을 통한 접근의 유사도 추출은 각 프레임의 추출 값이 정상 인증 추출 값과 유사한 결과를 얻었다. 즉, 안경 착용시 약 94%의 최대 유사도를 추출하였으며 정지영상(사진)에 의한 유사도 추출 값은 최대 99%까지 유사도를 추출하였다.

실험 환경에서 안경 착용시에 대한 결과는 같은 사용자이므로 문제가 되지 않으나, 정지영상(사진)에 의한 유사도는 문제가 될 수 있다. 실제 인물의 실시간 인증이 아닌 타인의 사진에 의한 접근은 불법적인 접근이므로 문제가 된다. 그러나 유사도 추출 실험 결과, 최대값은 높은 유사도를 보이나 최소값은 63%의 유사도를 추출하였다. 또한 그래프가 일정한 형태가 아닌 곡선에 형태를 가지고 있으며, 이러한 현상은 정지영상이 정면에서 입력한 영상 정보이기 때문이다. 사용자 인증 정보는 왼쪽 측면에서 오른쪽측면으로 이동 되면서 촬영한 영상이기 때문에 이러한 결과가 추출된 것이다.

실험에서 영상의 유사도 추출의 값이 같은 사용자의 영상임에도 불구하고 100%의 유사도를 추출하지 못하는 것은 키 프레임 추출하는 시점이 각각 다르기 때문에 차이를 보이는 것이다. 또한 다른 사용자 인증 정보임에도 불구하고 유사도 추출 값이 현저한 차이를 보이지 않는 것은 사람의 얼굴의 이목구비 및 피부색상 등의 영상 구성요소의 차이가 많이 발생하지 않기 때문이다. 또한 그림 7과 8의 결과에 나와 있지는 않지만 간헐적으로 정당하지 않은 사용자임에도 일시적으로 89%의 높은 유사도를 추출하기도 하였다.

그러므로 사용자 인증을 위한 임계값은 특정한 값을 추출하여 인증하는 것도 좋으나 추출한 키 프레임의 모든 프레임의 값을 고려하여 인증해야하고 DH와 DB간의 유사도 추출 특성을 고려하여 인증 모델을 적립하여야 한다. 표 1에서 각 실험 상황에 따른 결과 분석과 적용 방안에 대해 기술하였다.

<표 1> 실험 분석 및 적용방안
<Table 1> Experimental analysis and application

상황	분석 및 적용 방안
정당한 사용자 인증	‣DB에 비해 DH가 고른 분포의 유사도 추출 ‣DH/DB 모두 약 90% 이상의 유사도 추출 ‣DH에 의한 유사도 추출 후 DB에 의해 검증
안경 착용 사용자 인증	‣DH/DB 모두 고른 분포의 유사도를 추출 ‣유사도는 낮은 값을 추출 ‣제안 메커니즘에 추가적인 인증 기법 적용
정지영상(사진) 인증	‣최대와 최소값의 차이가 심함 ‣DH/DB 모두 유사도 추출 값의 표준편차 차이 ‣추출된 유사도의 최대와 최소값의 편차 계산 판정
정당하지 않은 사용자 인증	‣DB/DH 모두 낮은 유사도 추출 ‣일정하지 못한 유사도 추출 ‣DH나 DB, 모두 평균 유사도를 추출하여 판정

정당한 사용자의 경우에는 DH가 고른 유사도를 추출하였고, DB는 약간의 추출 값들에 대한 범위가 발생하였다. 즉, 최대와 최소의 유사도 추출 값의 차이가 DH는 0.05, DB는 0.1이다. 모두 높은 유사도를 추출하였다. 또한 정당하지 않은 사용자 인증은 DH와 DB 모두 낮은 유사도를 추출하였다. 안경을 착용한 사용자의 경우에는 고른 유사도를 추출하였고 정지영상의 사진 인증은 DH은 곡선 그래프로서 추출 값들에 표준편차가 있음을 알 수 있고, DB는 약간의 차이가 있으나 DH에 비해 고른 분포를 보였다.

V. 결론

본 논문에서는 IT의 집약적인 기술 및 서비스 매체로 각광받고 있는 스마트폰의 분실이나 타인에 의한 불법적인 접근을 방지하기 위한 기술을 제안하였다.

제안 기술은 정당한 사용자와 정당하지 못한 사용자의 얼굴 영상의 유사도에 명확한 차이를 보였고 안경 착용시, 안경의 이미지 영역에 의한 차이에 의해 정당한 사용자의 유사도와는 약간의 차이를 볼 수 있었다. 또한 정적 이미지인 정당한 사용자의 사진을 활용한 접근 상황에서는 측면의 영상에 대한 인식이 부족하여 불안정한 유사도를 추출하였다.

실험을 통해 제안 기술의 유사도 판단 기준은 임계값에 의해 결정된다. 그러나 정적인 단일 임계값에 의한 사용자 인증은 문제를 갖는다. 정적 이미지(사진)의 경우 높은 유사도와 낮은 유사도를 모두 포함하기 때문에 표 1에서 제시한 각 상황에 따른 적용방안이 고려되어야 한다. 제시한 적용 방안에 의해 사용자를 인증 할 수 있도록 하여 정당하지 못한 사용자

의 스마트폰 접근을 방지할 수 있다.

제안 메커니즘은 스마트폰의 다양한 서비스 및 사적 정보 보호하기 위한 것으로 정보화 사회의 현대인에게 필수 기능이다. 스마트폰의 타인에 의한 무분별한 활용 및 접근의 문제를 사전에 방지하여 스마트폰 활용영역의 개인과 기업의 정보 및 자산을 보호하고 안전한 스마트폰 서비스 및 기능을 활용할 수 있는 환경을 지원할 것으로 기대한다.

참고문헌

[1] Seung Il, Jeong, "Android Platform and Smartphone Technology Developmental Trends", Summer Conference of Daehan Electrical Engineering Science, Vol. 33 No. 1, pp2000-2001, 2010.

[2] Jin Cheon, Lee, "Smartphone Evolution and Subsequent Challenges", Facility Journal of Daehan Facility Engineering Science, Vol. 38 No. 11, pp57-58, 2009.

[3] Yong-Seok, Kim, "Smartphone Mobile Related Articles", Special Edition II of Information Science Journal, pp88-95, 2010.

[4] "Smartphone Facial Recognition Solution", Green Information Technology, http://www.ngreenit.com/, 2010.

[5] Dong In, Kim and Chil Woo, Lee, "Smartphone User Interface Technology Trends", Special Edition of Information Science Journal, pp15-24, 2010.

[6] Eun Gyeom, Jang, "Authentication Mechanism for the Protection of Intellectual Property of Digital Contents in UCC environment", Doctoral Thesis, Daejeon University, 2007.

[7] ITU Telecom., Standardization Sector of ITU, "Video coding for low bitrate communication", Draft ITU-T Recommendation H.263. 1996.

[8] F. Pam, Z Li and K. Lim. "A Study of MPEG-4 Rate Control Sheme and its Improvements", IEEE Trans. on Circuit and Systems for Video Technology, Vol. 13, No.5, May, pp440-446, 2003.

[9] Yang, Jingyu, Dai, Qionghai, Xu, Wenli, and Ding, Rong, "A Rate Control Algorithm for MPEG-2 to H.264 Real-time Transcoding", Visual Communications and Image Processing, pp1995-2003, 2005.

저 자 소 개

장 은 겸

2007 : 대전대학교 컴퓨터공학과 공학박사.

현 재 : (주)엠투엠코리아 부설연구소장 대전대학교 컴퓨터공학과 겸임교수.

관심분야 : DRM, 컴퓨터 포렌식스, 스마트폰, 시스템 접근 제어.

Email : jangegu@nate.com

남 석 우

2004 : 숭실대학교 컴퓨터공학과 공학박사.

1988~1993 : 국방과학연구소 재직.

현 재 : 혜천대학 컴퓨터정보과 부교수.

관심분야 : 유비쿼터스, 스마트폰, 영상처리.

Email : swnam@hu.ac.kr