(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0065821
(43) 공개일자 2012년06월21일

(51) 국제특허분류(Int. Cl.)
G06F 21/22 (2006.01) *G06F 21/04* (2006.01)
(21) 출원번호 10-2010-0127134
(22) 출원일자 2010년12월13일
심사청구일자 없음

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
정용화
대전광역시 유성구 은구비로 31, 열매마을아파트 505동 402호 (지족동)
이성주
서울특별시 마포구 월드컵북로22길 20 (성산동)
김학재
서울특별시 중구 신당6동 44-13 15통 1반
(74) 대리인
특허법인충현

전체 청구항 수 : 총 5 항

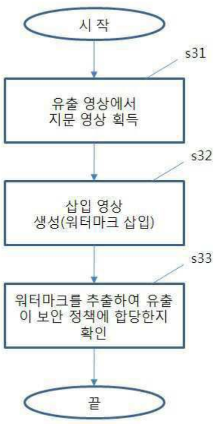
(54) 발명의 명칭 **지문 정보 보호 방법**

(57) 요 약

본 발명은 지문 영상을 보유하고 있는 특정 기관에서 외부로 유출되는 영상으로부터 지문을 검출하고 검출된 지문에 소정의 정보를 삽입하여 지문 정보를 보호할 수 있는 방법에 관한 것이다.

본 명세서에서 개시하는 지문 정보 보호 방법은 (a)하나의 네트워크를 통해 연결된 특정 집단으로부터 외부로 유출되는 영상에 포함된 지문(fingerprint)을 검출하여 지문 영상을 생성하는 단계; 및 (b)상기 지문 영상에 소정의 보호 정보를 삽입하여, 상기 보호 정보가 삽입된 영상을 생성하는 단계를 포함하여 본 발명의 과제를 해결한다.

대 표 도 - 도2a



특허청구의 범위

청구항 1

(a)하나의 네트워크를 통해 연결된 특정 집단으로부터 외부로 유출되는 영상에 포함된 지문(fingerprint)을 검출하여 지문 영상을 생성하는 단계; 및

(b)상기 지문 영상에 소정의 보호 정보를 삽입하여, 상기 보호 정보가 삽입된 영상을 생성하는 단계를 포함하는 지문 정보 보호 방법.

청구항 2

제 1 항에 있어서, 상기 (a)단계는

(a1)상기 특정 집단이 보유하는 지문을 학습하는 단계;

(a2)상기 학습된 결과를 이용하여 상기 보유 지문에 대한 분류자(classifier)를 생성하는 단계; 및

(a3)상기 분류자를 이용하여, 상기 유출 영상에 상기 특정 집단이 보유하는 지문이 포함되는지 판단하고 검출하는 단계를 포함하는 것을 특징으로 하는 지문 정보 보호 방법.

청구항 3

제 2 항에 있어서, 상기 학습 및 분류자의 생성은

SVM(Support Vector Machine)를 이용하여 이루어지는 것을 특징으로 하는 지문 정보 보호 방법.

청구항 4

제 1 항 내지 제 3 항 중 어느 한 항에 있어서, 상기 소정의 보호 정보의 삽입은

상기 (a)단계에 의해 생성된 지문 영상에 워터마크(watermark)를 삽입하여 이루어지는 것을 특징으로 하는 지문 정보 보호 방법.

청구항 5

제 4 항에 있어서,

(c)상기 소정의 보호 정보가 삽입된 지문 영상이 상기 특정 집단의 외부로 유출되는 경우, 상기 유출의 발생 즉시 상기 보호 정보를 추출하여 상기 특정 집단의 정보 보안 정책에 합당하게 유출되었는지를 확인하는 단계를 더 포함하는 것을 특징으로 하는 지문 정보 보호 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 지문 정보의 보호 방법에 관한 것으로, 보다 상세하게는 지문 영상을 보유하고 있는 특정 기관에서 외부로 유출되는 영상으로부터 지문을 검출하고 검출된 지문에 소정의 정보를 삽입하여 지문 정보를 보호할 수 있는 방법에 관한 것이다.

배 경 기 술

[0002] 급속한 정보화 및 인터넷의 발달로 인해 네트워크를 통한 정보의 교류가 활발해지고 온라인 뱅킹 등 전자상거래와 관련된 산업의 규모가 커지면서 개인 인증(personal authentication)의 정확성과 아울러 보안성 확보에 대한 요구가 점증하고 있다. 가장 일반적인 개인 인증 수단으로 PIN(Personal Identification Number) 또는 패스워드가 사용되지만, 유출 및 망각의 위험이 상존하므로 이에 따른 보안상의 문제가 최근 들어 크게 부각되고 있다. 이러한 문제점을 해결할 수 있는 개인 인증 방안으로서 개인 생체정보 대표적으로 사용자 지문을 통한 인증 방안의 도입이 확산되고 있다.

[0003] 사용자 지문 인식을 통한 인증 방안은 상기한 일반적인 인증 방안의 문제는 해결할 수 있지만, 사용자 지문이

타인에게 도용된다면 패스워드나 PIN과 달리 쉽게 재변경이 불가능하거나 변경이 제한적이기 때문에 심각한 문제를 일으킨다. 따라서 암호, 워터마킹(watermarking), 스테가노그래피(steganography) 등의 기술을 이용하여 사용자의 지문 정보를 보호하기 위한 연구가 활발히 진행되고 있다.

[0004] 한편 지문 인식은 통상적으로 영상 인식(image recognition)을 통해 이루어지므로 사용자의 지문을 스캔한 지문 영상을 저장해 두어야 함이 필요한데, 사용자 인증시마다 저장된 지문 영상을 참조하여 인증이 이루어지기 때문이다. 따라서 이러한 지문 영상이 인터넷 등 네트워크를 통해 특정 기관의 내부에서 외부로 유출되는 경우 외부의 제3자에 의해 사용자 지문이 악용될 우려가 매우 높다.

발명의 내용

해결하려는 과제

[0005] 따라서 본 발명이 해결하려는 과제는 지문 영상을 보유하고 있는 특정 기관에서 외부로 유출되는 영상으로부터 지문을 검출하고 검출된 지문에 소정의 정보를 삽입하여 지문 정보를 보호할 수 있는 방법을 제공하는 것이다.

과제의 해결 수단

[0006] 상기와 같은 과제를 해결하기 위해 본 명세서에서 개시하는 지문 정보 보호 방법은

[0007] (a)하나의 네트워크를 통해 연결된 특정 집단으로부터 외부로 유출되는 영상에 포함된 지문(fingerprint)을 검출하여 지문 영상을 획득하는 단계; 및 (b)상기 획득된 지문 영상에 소정의 보호 정보를 삽입하여, 상기 보호 정보가 삽입된 영상을 생성하는 단계를 포함하여 본 발명의 과제를 해결한다.

[0008] 아울러 (c)상기 소정의 보호 정보가 삽입된 지문 영상이 상기 특정 집단의 외부로 유출되는 경우, 상기 유출의 발생 즉시 상기 보호 정보를 추출하여 상기 특정 집단의 정보 보안 정책에 합당하게 유출되었는지를 확인하는 단계를 더 포함하여서도 본 방법 발명의 과제를 해결한다.

발명의 효과

[0009] 본 발명에 의하면, SVM을 이용하여 지문의 특징을 학습하기 때문에 특정 집단에서 외부로 유출되는 영상에서 지문 영상의 정확한 추출이 가능하다. 아울러 분류된 지문 영상에 워터마크 등의 소정의 보호 정보를 삽입하여 지문 정보에 대해 보다 안전성을 추구할 수 있으며, 지문 영상의 유출 즉시 보호 정보를 추출함으로써 특정 집단이 보유하는 지문 정보에 대한 보안성 확보에도 기여할 수 있다.

도면의 간단한 설명

[0010] 도 1은 본 발명이 구현될 수 있는 환경을 제시한 도면이다.

도 2a과 도 2b는 본 발명의 바람직한 일 흐름을 제시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0011] 이하, 본 발명이 해결하고자 하는 과제의 해결 방안을 명확하게 하기 위한 발명의 구성을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다.

[0012] 도 1은 본 발명이 구현될 수 있는 환경을 제시한 도면이다.

[0013] 본 발명은 특정 집단의 내부 인트라넷에서 라우터 혹은 허브(102)에 구현되어 외부 네트워크(101)와 연결될 수 있다. 본 발명은 특정 집단의 내부 구성원(103)에 의해서 외부 네트워크(101)로 전송되는 각종 영상 정보로부터 소정의 분류자(classifier)를 통해 지문 영상을 추출(검출)할 수 있도록 하는 것이다. 여기서 특정 집단은 지문 정보를 요하거나 보유하고 있는 모든 집단을 포함하는 개념으로 대표적으로 지문 정보를 개인 인증수단으로 활용하는 집단을 들 수 있다.

[0014] 도 2a과 도 2b는 본 발명의 바람직한 일 흐름을 제시한 도면이다.

[0015] 먼저 특정 집단에서 외부로 유출되는 영상에서 지문(fingerprint)을 검출하여 지문 영상을 생성한다. 이때 특

정 집단은 도 1에서 하나의 네트워크(예를 들어 인트라넷)를 통해 상호 연결된 내부 구성원들(103)에 해당하며, 외부는 그 이외의 자들을 모두 포함한다.

[0016] 지문 영상의 생성(s31)은 바람직하게 다음과 같이 이루어질 수 있다.

[0017] 우선 특정 집단이 보유하고 있는 지문의 특징이 학습된다(s311). 다음으로 학습된 결과를 이용하여 보유 지문에 대한 분류자(classifier)를 생성한다(s312). 다음으로 생성된 분류자를 이용하여 유출 영상이 지문 영상인지를(유출 영상에 지문이 포함되어 있는지를) 판단하여(s313), 지문이 포함된 경우에는 유출 영상에서 지문만을 분리하여 지문 영상을 생성한다.

[0018] 큰 범주로 볼 때, 지문 영상의 획득(s31)은 결국 영상에서 특정 객체를 분리해내는 기술의 범주에 속한다.

[0019] 영상에서 특정 객체를 분리하는 방안으로는 차 영상과 에지 영상을 이용하여 객체를 분리하는 기법이 있다. 이는 특징 정보가 단순하여 빠른 처리는 가능하지만 복잡한 객체 및 유사한 객체를 대상으로는 분리가 어려운 단점이 있다. 영상에서 특정 객체를 분리하는 또 다른 방안으로는 영상의 색 정보를 기반으로 하여 특정 객체를 분리하는 기법이 있는데, 색이 일정한 영역을 분리한 후 이를 다시 병합하는데 상당한 처리 시간이 걸리기 때문에 대용량의 영상인 경우에는 역시 적용하기 어려운 문제가 있다.

[0020] 한편, 학습 알고리즘을 이용하여 특정 객체를 검출하는 방안이 있다. 학습 집단을 이용하여 학습 오류(empirical error)를 최소화하는 경험적 위험 최소화 원칙(Empirical Risk Minimization: ERM)을 구현하는 것과 전체 집단을 하위 집단으로 세분화한 뒤 이 집단에 대한 경험적 위험도를 최소화하는 의사결정함수를 선택하는 구조적 위험 최소화 원칙(Structural Risk Minimization: SRM) 을 구현하는 것이 있다. 그러나 이러한 학습 알고리즘은 학습 시간이 매우 오래 걸리는 단점이 있다.

[0021] 최근 들어 특정 객체의 검출에 SVM(Support Vector Machine) 이라는 기계 학습(machine learning) 방안이 많이 활용되고 있다. SVM은 통계적 학습 이론(statistical learning theory)에 기반을 두고 있으며, 이진 클래스(binary class)를 가장 최적으로 나누는 경계면(hyper plane)을 찾는 것으로 분류를 수행한다.

[0022] 본 발명에 의한 지문 특징의 학습(s311) 및 분류자의 생성(s312)는 SVM 중 SVDD(Support Vector Data Description)에 의해 이루어질 수 있다. SVDD는 학습 클래스에 속하는 객체의 존재 영역을 원형체(hyper sphere)를 설정하여 근사하는 방안으로, 원형체의 중심과 데이터의 거리를 이용하여 원형체 내부에 있는 객체만을 검출 대상 객체로 분류하고 원형체를 벗어나면 비검출 대상 객체로 분류한다. 이러한 사실을 본 발명에 적용한다면 원형체 내부에 있는 객체가 지문 영상으로 분류되는 것이며, 원형체를 벗어나는 데이터는 일반 영상으로 분류된다. SVDD는 새로운 형태의 영상이 나타날 경우 기존의 이진 분류 SVM 방식의 최적의 분리 경계면(hyper plane)을 이용한 분류 방안으로는 검출 대상 객체를 탐지하기 어려운 점을 극복 가능하게 한다.

[0023] 지문 영상이 생성되면, 생성된 지문 영상의 보안성을 꾀하기 위해 생성된 지문 영상에 소정의 보호 정보를 삽입하여 보호 정보가 삽입된 영상을 생성한다(s32). 이때 소정의 보호 정보는 워터마크(watermark)를 그 예로 들 수 있으며, 워터마크를 구성하는 정보의 예로는 호스트의 IP, 상기 특정 집단에서 내부 구성원이 속한 기관(해당기관)의 ID(유출 출처), 유출 시점의 시간 및 패킷 정보 등을 그 예로 들 수 있으며, 이는 상기 특정 집단의 정보 보안 정책에 따라 매우 다양하게 구성할 수 있다.

[0024] 한편 소정의 보호 정보(워터마크)가 삽입된 지문 영상이 특정 집단의 외부로 유출되는 경우, 그 보호 정보를 유출 즉시 추출하여 상기 특정 집단의 정보 보안 정책에 합당하게 유출되었는지를 확인하고(s33), 이 보안 정책에 배치되어 유출된 경우에는 지문 유출 책임자를 즉각 추적하여 책임을 추궁할 수 있게 한다. 따라서 특정 집단이 보유하는 지문의 불법 유출을 방지할 수 있다.

[0025] 본 방법발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0026] 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 유무선 네트워크를 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

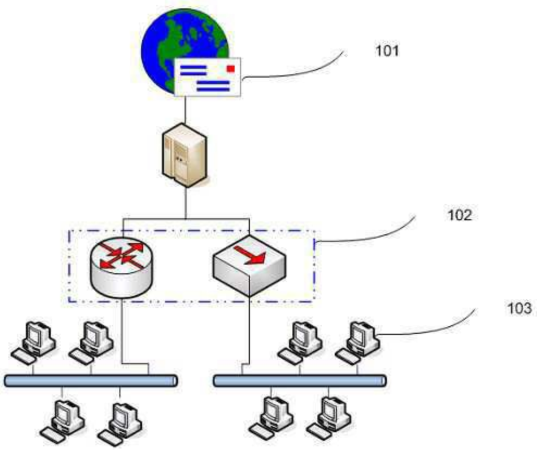
[0027] 이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현

될 수 있음을 이해할 수 있을 것이다.

[0028] 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

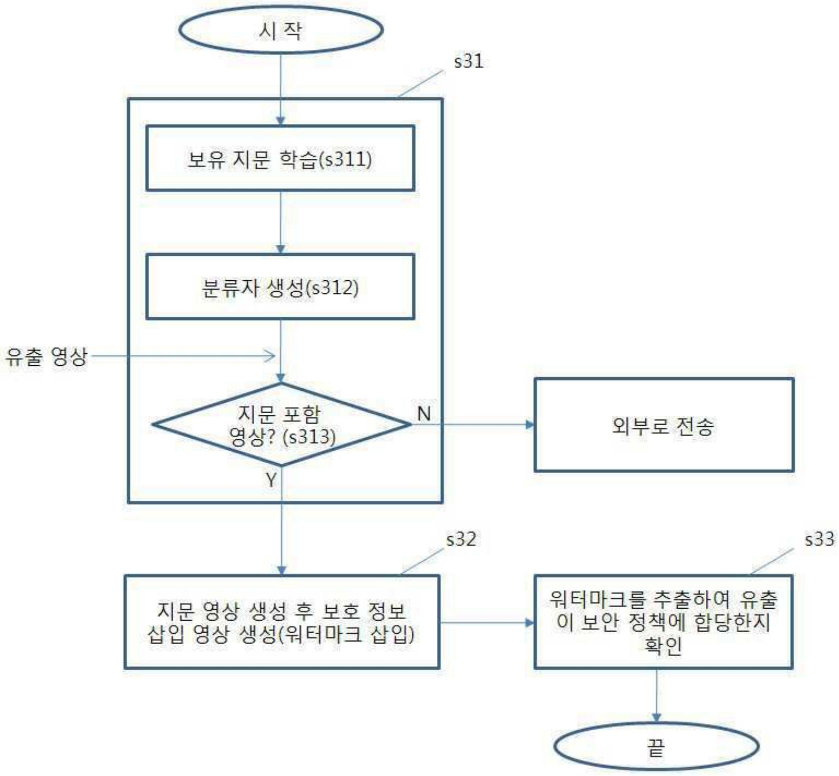
도면

도면1



도면2a

도면2b



시 작
s31
보유 지문 학습(s311)
분류자 생성(s312)
유출 영상
지문 포함 영상? (s313)
N
외부로 전송
Y
s32
s33
지문 영상 생성 후 보호 정보 삽입 영상 생성(워터마크 삽입)
워터마크를 추출하여 유출이 보안 정책에 합당한지 확인
끝