(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년03월26일
(11) 등록번호 10-2231409
(24) 등록일자 2021년03월18일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 21/60* (2013.01)
(52) CPC특허분류
G06F 21/62 (2013.01)
G06F 21/602 (2013.01)
(21) 출원번호 10-2018-7030946
(22) 출원일자(국제) 2017년03월20일
심사청구일자 2019년04월18일
(85) 번역문제출일자 2018년10월25일
(65) 공개번호 10-2019-0002487
(43) 공개일자 2019년01월08일
(86) 국제출원번호 PCT/CN2017/077279
(87) 국제공개번호 WO 2017/167052
국제공개일자 2017년10월05일
(30) 우선권주장
201610188604.2 2016년03월29일 중국(CN)
(56) 선행기술조사문헌
CN101114256 A
KR1020020084216 A
KR1020070096014 A
KR1020090126333 A

(73) 특허권자
어드밴스드 뉴 테크놀로지스 씨오., 엘티디.
케이만 군도, 그랜드 케이만 케이와이1-9008, 조지 타운, 27 하스피탈 로드, 케이만 코포레이트 센터
(72) 발명자
엘브이 첸첸
중국 저지앙 311121 항저우 유 항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
관 웨이강
중국 저지앙 311121 항저우 유 항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
(74) 대리인
김태홍, 김진희

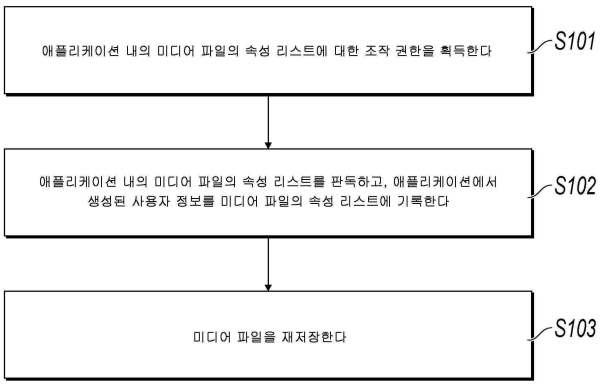
전체 청구항 수 : 총 14 항 심사관 : 구대성

(54) 발명의 명칭 **애플리케이션에 포함된 사용자 정보를 은닉하기 위한 방법 및 디바이스**

(57) 요 약

본 출원은 애플리케이션에 포함된 사용자 정보를 은닉하는 방법 및 디바이스를 개시한다. 이 방법은 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득하는 것과; 애플리케이션 내의 미디어 파일의 속성 리스트를 판독하고, 애플리케이션에서 생성된 사용자 정보를 미디어 파일의 속성 리스트에 기록하는 것과; 이 미디어 파일을 재저장하는 것을 포함한다. 애플리케이션에서 생성된 사용자 정보는 애플리케이션 내의 미디어 파일의 속성 리스트에 기록된다. 이와 같이, 사용자 정보는 은닉되어 모바일 디바이스의 로컬 폴더에서 거의 발견 및 획득될 수 없고, 애플리케이션에서 생성된 사용자 정보는 공개되지 않게 된다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

컴퓨터 구현 방법(computer-implemented method)으로서,

소프트웨어 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득하는 단계 - 상기 조작 권한을 획득하는 단계는, 상기 미디어 파일의 파일 핸들(file handle)을 획득하는 단계 및 상기 미디어 파일의 속성 리스트에 대한 판독 또는 기록 허가를 획득하는 단계를 포함함 - ;

상기 미디어 파일의 속성 리스트를 식별하는 단계 - 상기 속성 리스트는 상기 미디어 파일을 설명하는 속성 정보를 포함함 - ;

상기 소프트웨어 애플리케이션의 실행 동안 생성된 사용자 정보를 키-값의 쌍의 형태(key-vale pair format)로 상기 미디어 파일의 속성 리스트에 기록하는 단계; 및

상기 소프트웨어 애플리케이션의 설치 경로에 상기 미디어 파일을 저장하는 단계

를 포함하는, 컴퓨터 구현 방법.

청구항 2

제1항에 있어서,

상기 사용자 정보는 민감 정보 및 기밀 정보를 포함하고, 상기 사용자 정보는 암호화되며, 상기 민감 정보는 로그인 계정, ID 카드 번호, 모바일 번호 및 은행 카드 번호 중 적어도 하나를 포함하는 것인, 컴퓨터 구현 방법.

청구항 3

제1항에 있어서,

상기 미디어 파일은 사진 파일, 오디오 파일, 또는 비디오 파일을 포함하는 것인, 컴퓨터 구현 방법.

청구항 4

제1항에 있어서,

상기 소프트웨어 애플리케이션에 의해 로직 처리가 수행된 사용자 정보를 상기 속성 리스트에 기록하는 단계를 더 포함하는, 컴퓨터 구현 방법.

청구항 5

제4항에 있어서,

상기 소프트웨어 애플리케이션에 의해 생성된 사용자 정보에 대하여 로직 처리를 수행하는 것은,

상기 사용자 정보에 대하여 가역 로직 처리(reversible logic processing)를 수행하는 것; 및

대칭 암호화 알고리즘을 사용하여 상기 사용자 정보에 대하여 대칭 암호화 처리를 수행하는 것

을 포함하는 것인, 컴퓨터 구현 방법.

청구항 6

동작들을 수행하도록 컴퓨터 시스템에 의해 실행 가능한 하나 이상의 명령어가 저장된 비일시적 컴퓨터 판독 가능 저장 매체로서, 상기 동작들은,

소프트웨어 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득하는 동작 - 상기 조작 권한을 획득하는 동작은, 상기 미디어 파일의 파일 핸들을 획득하는 동작 및 상기 미디어 파일의 속성 리스트에 대한 판독 또는 기록 허가를 획득하는 동작을 포함함 - ;

상기 미디어 파일의 속성 리스트를 식별하는 동작 - 상기 속성 리스트는 상기 미디어 파일을 설명하는 속성 정보를 포함함 - ;

상기 소프트웨어 애플리케이션의 실행 동안 생성된 사용자 정보를 키-값의 쌍의 형태로 상기 미디어 파일의 속성 리스트에 기록하는 동작; 및

상기 소프트웨어 애플리케이션의 설치 경로에 상기 미디어 파일을 저장하는 동작

을 포함하는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 7

제6항에 있어서,

상기 사용자 정보는 민감 정보 및 기밀 정보를 포함하고, 상기 사용자 정보는 암호화되며, 상기 민감 정보는 로그인 계정, ID 카드 번호, 모바일 번호 및 은행 카드 번호 중 적어도 하나를 포함하는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 8

제6항에 있어서,

상기 미디어 파일은 사진 파일, 오디오 파일, 또는 비디오 파일을 포함하는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 9

제6항에 있어서,

상기 동작들은, 상기 소프트웨어 애플리케이션에 의해 로직 처리가 수행된 사용자 정보를 상기 속성 리스트에 기록하는 동작을 더 포함하는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 10

제9항에 있어서,

상기 소프트웨어 애플리케이션에 의해 생성된 사용자 정보에 대하여 로직 처리를 수행하는 것은,

상기 사용자 정보에 대하여 가역 로직 처리를 수행하는 것; 및

대칭 암호화 알고리즘을 사용하여 상기 사용자 정보에 대하여 대칭 암호화 처리를 수행하는 것

을 포함하는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 11

컴퓨터 구현 시스템(computer-implemented system)으로서,

하나 이상의 컴퓨터; 및

상기 하나 이상의 컴퓨터에 상호 동작 가능하게 연결되고, 상기 하나 이상의 컴퓨터에 의한 실행 시 하나 이상의 동작을 수행하는 하나 이상의 명령어가 저장된 유형의(tangible) 비일시적 머신 판독 가능 매체를 구비한, 하나 이상의 컴퓨터 메모리 디바이스

를 포함하고, 상기 하나 이상의 동작은,

소프트웨어 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득하는 동작 - 상기 조작 권한을 획득하는 동작은, 상기 미디어 파일의 파일 핸들을 획득하는 동작 및 상기 미디어 파일의 속성 리스트에 대한 판독 또는 기록 허가를 획득하는 동작을 포함함 - ;

상기 미디어 파일의 속성 리스트를 식별하는 동작 - 상기 속성 리스트는 상기 미디어 파일을 설명하는 속성 정보를 포함함 - ;

상기 소프트웨어 애플리케이션의 실행 동안 생성된 사용자 정보를 키-값의 쌍의 형태로 상기 미디어 파일의 속

성 리스트에 기록하는 동작; 및

상기 소프트웨어 애플리케이션의 설치 경로에 상기 미디어 파일을 저장하는 동작

을 포함하는 것인, 컴퓨터 구현 시스템.

청구항 12

제11항에 있어서,

상기 사용자 정보는 민감 정보 및 기밀 정보를 포함하고, 상기 사용자 정보는 암호화되며, 상기 민감 정보는 로그인 계정, ID 카드 번호, 모바일 번호 및 은행 카드 번호 중 적어도 하나를 포함하는 것인, 컴퓨터 구현 시스템.

청구항 13

제11항에 있어서,

상기 미디어 파일은 사진 파일, 오디오 파일, 또는 비디오 파일을 포함하는 것인, 컴퓨터 구현 시스템.

청구항 14

제11항에 있어서,

상기 하나 이상의 동작은, 상기 소프트웨어 애플리케이션에 의해 로직 처리가 수행된 사용자 정보를 상기 속성 리스트에 기록하는 동작을 더 포함하고,

상기 소프트웨어 애플리케이션에 의해 생성된 사용자 정보에 대하여 로직 처리를 수행하는 것은,

상기 사용자 정보에 대하여 가역 로직 처리를 수행하는 것; 및

대칭 암호화 알고리즘을 사용하여 상기 사용자 정보에 대하여 대칭 암호화 처리를 수행하는 것

을 포함하는 것인, 컴퓨터 구현 시스템.

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

발명의 설명

기 술 분 야

[0001] 본 출원은 단말기 기술 분야에 관한 것으로, 특히 애플리케이션에 포함된 사용자 정보를 은닉하는 방법 및 디바이스에 관한 것이다.

배 경 기 술

[0002] 다양한 무선 모바일 디바이스 및 모바일 인터넷의 급속한 발전에 따라, 점점 더 많은 무선 모바일 디바이스가 사람들의 일상 생활에서 사용되며, 많은 무선 모바일 디바이스가 삶의 일부가 되었다. 현재, iOS, Android 또는 Windows 시스템과 상관없이, 데이터 전파의 속도, 편의성, 안정성 및 보안은 무선 모바일 디바이스를 측정하는 데 중요한 지표가 된다. 특히, 그것이 중요한 개인 사용자 정보와 관련된 경우 보안 지표는 더욱 중요해진다.

[0003] 무선 모바일 디바이스에 사용되는 애플리케이션은 쇼핑, 채팅, 친구 사귀기, 여행 등과 같은 다양한 생활 및 업무 기능을 구현할 수 있다. 그것은 사용자에게 큰 도움이 된다. 애플리케이션을 사용할 때, 애플리케이션은

애플리케이션에 대한 로그인 계정 및 로그인 암호와, 민감한 기밀 사용자 정보와 관련된 이력 채팅 기록, 쇼핑 주문 정보, 지불 정보 등과 같은 다양한 데이터를 생성한다. 사용자 정보는 일반적으로 모바일 디바이스의 로컬 폴더에 텍스트 파일 및 데이터베이스 파일의 형태로 저장된다. 따라서, 위에서 언급한 텍스트 파일과 데이터베이스 파일은 쉽게 발견되고, 결과적으로 사용자 정보가 공개될 가능성이 높다. 사용자 정보의 공개 가능성을 회피하기 위해, 실행중인 애플리케이션에서 생성된 민감한 기밀 사용자 정보는 모바일 디바이스의 로컬 폴더에 저장되기 전에 암호화된다. 그러나, 정보가 암호화되었더라도, 그 암호화된 정보의 암호문은 여전히 완전히 노출되어 있다. 예를 들어, 텍스트 파일과 데이터베이스 파일(예를 들어, .txt, .db 또는 .plist 파일)은 암호화된 정보를 획득하기 위한 비교적 일반적인 제3자 툴(iTools 및 Peapod와 같은 데이터베이스 도구)를 사용하여 찾을 수 있다. 이와 같이, 민감한 기밀 사용자 정보를 획득하기 위해 암호화된 정보를 무력화(cracking)할 가능성이 증가하고, 민감한 기밀 사용자 정보는 이후 공개되며, 보안 수준은 상대적으로 낮아지게 된다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0004] 본 발명의 구현예는, 애플리케이션 실행 프로세스에서 생성된 사용자 정보가 쉽게 발견되어 획득되고, 결과적으로 사용자 정보가 공개되는 기존 기술의 문제점을 해결하기 위해, 애플리케이션에 포함된 사용자 정보를 은닉하는 방법 및 디바이스를 제공한다.

[0005] 본 발명의 구현예는 애플리케이션에 포함된 사용자 정보를 은닉하는 방법을 제공하며, 이 방법은 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득하는 것과; 애플리케이션 내의 미디어 파일의 속성 리스트를 판독하고, 애플리케이션에서 생성된 사용자 정보를 미디어 파일의 속성 리스트에 기록하는 것과; 이 미디어 파일을 재저장하는 것을 포함한다.

[0006] 또한, 사용자 정보는 민감 정보 또는 기밀 정보를 포함한다.

[0007] 또한, 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득하는 것은, 애플리케이션 내의 미디어 파일의 파일 핸들(file handle)을 획득하는 것과; 미디어 파일의 파일 핸들을 사용하여 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 판독/기록 허가를 획득하는 것을 포함한다.

[0008] 또한, 애플리케이션에서 생성된 사용자 정보를 미디어 파일의 속성 리스트에 기록하는 것은, 애플리케이션에서 생성된 사용자 정보를 키-값의 쌍의 형태로 미디어 파일의 속성 리스트에 기록하는 것을 포함한다.

[0009] 또한, 미디어 파일은 그림 파일, 오디오 파일, 및 비디오 파일을 포함한다.

[0010] 또한, 사용자 정보는 암호화된 사용자 정보이다.

[0011] 본 발명의 구현예는 애플리케이션에 포함된 사용자 정보를 은닉하는 방법을 더 제공하며, 이 방법은 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득하는 것과; 애플리케이션에서 생성된 사용자 정보에 대한 로직 처리(logic processing)를 수행하는 것과; 애플리케이션 내의 미디어 파일의 속성 리스트를 판독하고, 애플리케이션에서 로직 처리를 거친 사용자 정보를 미디어 파일의 속성 리스트에 기록하는 것과; 이 미디어 파일을 재저장하는 것을 포함한다.

[0012] 또한, 사용자 정보는 민감 정보 또는 기밀 정보를 포함한다.

[0013] 또한, 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득하는 것은, 애플리케이션 내의 미디어 파일의 파일 핸들을 획득하는 것과; 미디어 파일의 파일 핸들을 사용하여 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 판독/기록 허가를 획득하는 것을 포함한다.

[0014] 또한, 애플리케이션에서 생성된 사용자 정보를 미디어 파일의 속성 리스트에 기록하는 것은, 애플리케이션에서 생성된 사용자 정보를 키-값의 쌍의 형태로 미디어 파일의 속성 리스트에 기록하는 것을 포함한다.

[0015] 또한, 미디어 파일은 그림 파일, 오디오 파일, 및 비디오 파일을 포함한다.

[0016] 또한, 사용자 정보는 암호화된 사용자 정보이다.

[0017] 또한, 애플리케이션에서 생성된 사용자 정보에 대한 로직 처리를 수행하는 것은, 애플리케이션에서 생성된 사용자 정보에 대해 가역 로직 처리(reversible logic processing)를 수행하는 것을 포함한다.

[0018] 또한, 애플리케이션에서 생성된 사용자 정보에 대한 로직 처리를 수행하는 것은 대칭 암호화 알고리즘을 사용하여 애플리케이션에서 생성된 사용자 정보에 대한 대칭 암호화 처리를 수행하는 것을 포함한다.

[0019] 본 발명의 구현예는 애플리케이션에 포함된 사용자 정보를 은닉하는 디바이스를 더 제공하며, 이 디바이스는 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득하도록 구성된 획득 모듈과; 애플리케이션 내의 미디어 파일의 속성 리스트를 판독하고, 애플리케이션에서 생성된 사용자 정보를 미디어 파일의 속성 리스트에 기록하도록 구성된 판독/기록 모듈과; 이 미디어 파일을 재저장하도록 구성된 저장 모듈(saving module)을 포함한다.

[0020] 또한, 디바이스는, 애플리케이션에서 생성된 사용자 정보에 대한 로직 처리를 수행하도록 구성된 로직 처리 모듈을 더 포함한다.

[0021] 기존의 기술과 비교하여, 본 출원의 구현예에 제공된 애플리케이션에 포함된 사용자 정보를 은닉하는 방법 및 디바이스에 따르면, 애플리케이션에서 생성된 사용자 정보는 애플리케이션 내의 미디어 파일의 속성 리스트에 기록된다. 이와 같이, 사용자 정보는 은닉되어 모바일 디바이스의 로컬 폴더에서 거의 발견 및 획득될 수 없고, 애플리케이션에서 생성된 사용자 정보는 공개되지 않게 된다.

도면의 간단한 설명

[0022] 본 명세서에 기술되는 첨부된 도면은 본 출원의 보다 나은 이해를 제공하고자 하는 것이며, 본 출원의 일부를 구성한다. 본 출원의 예시적인 구현예 및 구현예의 기술은 본원을 설명하기 위한 것이며, 본원에 대한 제한을 구성하지 않는다. 첨부된 도면에서:

도 1은 본 출원의 구현예 1에 따라 애플리케이션에 포함된 사용자 정보를 은닉하는 방법을 도시하는 개략적인 흐름도이다.

도 2는 본 출원의 구현예 2에 따라 애플리케이션에 포함된 사용자 정보를 은닉하는 방법을 도시하는 개략적인 흐름도이다.

도 3은 본 출원의 구현예 3에 따라 애플리케이션에 포함된 사용자 정보를 은닉하는 디바이스를 도시하는 개략적인 구조도이다.

발명을 실시하기 위한 구체적인 내용

[0023] 본 출원의 목적, 기술적 해결책 및 장점을 보다 명확하게 하기 위해, 본 출원의 특정 구현예 및 대응하는 첨부 도면을 참조하여 본원의 기술적 해결책을 설명한다. 명백하게, 설명된 구현예는 본 출원의 모든 구현예라기보다는 오히려 일부에 불과하다. 창의적인 노력없이 본원의 구현예에 기초하여 당업자에 의해 획득되는 다른 구현예는 본 출원의 보호 범위 내에 있다.

[0024] 도 1은 본 출원의 구현예에 따라 애플리케이션에 포함된 사용자 정보를 은닉하는 방법을 도시하는 개략적인 흐름도이다. 다음은 도 1을 참조하여 본원의 구현예에 제공되는 애플리케이션에 포함된 사용자 정보를 은닉하는 방법을 상세하게 설명한다. 도 1에 도시된 바와 같이, 본원의 구현예에 제공되는 애플리케이션에 포함된 사용자 정보를 은닉하는 방법은 다음과 같은 단계를 포함한다.

[0025] 단계(S101): 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득한다.

[0026] 본원의 본 구현예에서, 실행중인 프로세스에서, 모바일 디바이스의 애플리케이션은 사용자 조작에 대응하는 사용자 정보를 생성한다. 사용자 정보는 민감한 기밀 사용자 정보를 포함하며 사용자 정보는 모바일 디바이스에 자동으로 저장된다. 이전 애플리케이션은 모바일 디바이스에 설치된 다양한 애플리케이션, 예를 들어, 지불을 위한 애플리케이션 또는 친구를 만들기 위한 애플리케이션일 수 있다. 지불 애플리케이션이 일 예로서 사용된다. 사용자가 지불 애플리케이션을 사용할 때, 애플리케이션은 로그인 계정, 로그인 암호, ID 카드 번호, 모바일 번호, 은행 카드 번호 및 지불 암호와 같은 민감한 기밀 사용자 정보를 생성한다. 이러한 사용자 정보에서, 로그인 암호 및 지불 암호는 기밀 사용자 정보이고, 로그인 계정, ID 카드 번호, 모바일 번호 및 은행 카드 번호는 민감 정보이다.

[0027] 또한, 애플리케이션 실행 프로세스에서, 상이한 서비스 타입 또는 애플리케이션 시나리오는 상이한 사용자 정보

에 대응한다. 지불 애플리케이션의 예를 계속하면, 지불 애플리케이션 시나리오에서 지불과 관련된 민감한 기밀 사용자 정보가 생성된다. 또한, 채팅 정보와 관련된 사용자 정보는 채팅 애플리케이션 시나리오에서 생성된다.

[0028] 현 단계에서, 애플리케이션 내의 미디어 파일은 애플리케이션의 설치 디렉토리에 위치할 수 있으며, 이전 사용자 정보를 저장하는 캐리어로서 사용될 수 있다. 서로 상이한 타입의 사용자 정보는 상이한 미디어 파일에 저장될 수 있다. 또한, 이전 사용자 정보는 미디어 파일의 속성 리스트에 저장될 수 있고, 속성 리스트는 미디어 파일을 기술하는 데 사용되는 속성 정보를 포함한다. 이전 미디어 파일은 그림 파일, 오디오 파일, 및 비디오 파일 중 임의의 하나일 수 있다. 바람직하게, 이전 미디어 파일은 그림 파일일 수 있다. 이전 미디어 파일은 애플리케이션 아이콘의 일부로서 애플리케이션 설치 패키지 내에 사전 패키징될 수 있으며, 애플리케이션이 설치된 후, 이전 미디어 파일은 애플리케이션의 설치 디렉토리 내에 위치한다.

[0029] 사용자는 마우스 포인터를 미디어 파일로 이동하고, 마우스 오른쪽 버튼을 클릭하고, 미디어 파일 속성 옵션을 클릭하고, 다음 자세한 정보를 클릭하여, 속성 식별자 및 대응하는 속성 값을 포함하는, 미디어 파일의 속성 리스트를 볼 수 있다. 예를 들어, 사진의 속성 리스트는 속성 식별자 및 속성 식별자에 대응하는, 이름, 프로젝트 타입, 생성 날짜 및 수정 날짜와 같은 속성 값을 포함한다.

[0030] 또한, 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득하는 것은, 애플리케이션 내의 미디어 파일의 파일 핸들을 획득하는 것과; 미디어 파일의 파일 핸들을 사용하여 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 판독/기록 허가를 획득하는 것을 포함한다.

[0031] 미디어 파일의 파일 핸들은 미디어 파일의 객체 포인터라고 지칭될 수도 있다. 파일 핸들은 고유 정수 값, 즉, 애플리케이션 내의 상이한 객체 및 동일한 타입의 객체의 상이한 인스턴스를 식별하는 데 사용되는 4-바이트 값(64-비트 프로그램 내의 8-바이트 값)이다. 미디어 파일의 파일 핸들이 획득되며, 애플리케이션은 파일 핸들을 사용하여, 미디어 파일로부터, 즉 미디어 파일의 속성 리스트로부터 정보를 판독하거나 미디어 파일 내에, 즉 미디어 파일의 속성 리스트 내에 정보를 기록할 수 있다.

[0032] 단계(S102): 애플리케이션 내의 미디어 파일의 속성 리스트를 판독하고 애플리케이션에서 생성된 사용자 정보를 미디어 파일의 속성 리스트에 기록한다.

[0033] 본 구현예에서, 미디어 파일의 파일 핸들이 획득되기 때문에, 미디어 파일의 속성 리스트는 판독 또는 기록될 수 있는 객체로서 사용될 수 있다. 미디어 파일의 속성 리스트는 미디어 파일을 기술하는 데 사용되는 속성 정보를 포함한다.

[0034] 미디어 파일의 속성 리스트는 모바일 디바이스의 메모리 내로 판독되고, 이전 사용자 정보는 모바일 디바이스의 메모리에서 미디어 파일의 속성 리스트에 기록된다.

[0035] 또한, 애플리케이션에서 생성된 사용자 정보를 미디어 파일의 속성 리스트에 기록하는 것은, 애플리케이션에서 생성된 사용자 정보를 키-값의 쌍의 형태로 미디어 파일의 속성 리스트에 기록하는 것을 포함한다.

[0036] 애플리케이션 실행 프로세스에서, 민감 정보 및 기밀 정보와 같은 사용자 조작과 관련된 사용자 정보가 생성된다. 사용자 정보는 암호화되지 않은 평문일 수 있으며, 사용자 정보는 미디어 파일의 속성 리스트 내에 직접 기록될 수 있다.

[0037] 예를 들어, 애플리케이션 실행 프로세스에서, 계정 암호가 생성되고 로컬로 저장된다. 사용자의 계정 암호가 도난당하지 않도록 하기 위해서, 계정 암호는 키-값의 쌍의 형태로 미디어 파일의 속성 리스트에 기록되어 계정 암호를 은닉할 수 있다. 계정 암호에 대응하는 속성 식별자 Key는 Password로 명명될 수 있다. 계정 암호의 속성 값 Value는 암호를 나타내는 스트링(string)일 수 있으며, 이 스트링은 평문일 수 있다. 확실히, 계정 암호를 보다 잘 은닉하고 위장하기 위해 계정 암호에 대응하는 속성 식별자 Key는 식별될 가능성이 낮은 시스템 타입의 속성 식별자 Key로 설정될 수 있다.

[0038] 또한, 사용자 조작과 관련되고 애플리케이션에서 생성된 사용자 정보가 대안적으로 암호화된 암호문일 수 있다는 것에 주목할 가치가 있다. 사용자 정보의 암호화 방법은 MD5, DES, RSA, SM2 및 SM3과 같은 암호화 알고리즘을 포함한다.

[0039] 또한, 상이한 애플리케이션 시나리오에서 생성된 사용자 정보는 상이한 미디어 파일 내에 기록될 수 있다. 예를 들어, 애플리케이션 지불 시나리오에서 생성된 (지불 암호 및 주문 정보와 같은) 사용자 정보는 미디어 파일 내에, 예를 들어, 사진 a 내에 기록될 수 있으며, (채팅 정보 내의 전화 번호 및 은행 카드 번호와 같은) 채팅

애플리케이션 시나리오에서 생성된 사용자 정보는 다른 미디어 파일 내에, 예를 들어, 사진 b 내에 기록될 수 있다.

[0040] 단계(S103): 미디어 파일을 재저장한다.

[0041] 본 구현예에서, 은닉될 필요가 있는 모든 사용자 정보가 미디어 파일의 속성 리스트에 기록된 후에, 이전 미디어 파일은 재저장되어야 한다. 사용자는 마우스 포인터를 미디어 파일로 이동하고, 마우스 오른쪽 버튼을 클릭하고, 미디어 파일 속성 옵션을 클릭하고, 다음 자세한 정보를 클릭하여, 속성 리스트에 기록된 사용자 정보가 미디어 파일의 속성 리스트 내에 저장되었다는 것을 알 수 있다.

[0042] 미디어 파일이 성공적으로 저장되면, 미디어 파일은 애플리케이션의 설치 경로 내에 저장되며, 그 경우 사용자 정보는 성공적으로 위장된다.

[0043] 미디어 파일이 저장되지 않으면, 미디어 파일은 하나의 사전결정된 시간 구간의 간격(예를 들어, 3 내지 5 초)으로 자동으로 재저장될 수 있고, 사전결정된 개수의 재저장의 회수는 3일 수 있다. 3 회의 회수로 재저장하는 동안 미디어 파일이 성공적으로 저장되면, 그것은 사용자 정보가 성공적으로 위장된다는 것을 나타낸다. 3 회 초과의 회수로 재저장한 후, 미디어 파일이 저장되지 못하면, 그러한 저장 실패는 실패 대기열(failure queue) 내에 저장된다.

[0044] 사용자 정보가 미디어 파일 내에 기록되고 미디어 파일이 성공적으로 저장된 후, 민감한 기밀 정보와 관련된 사용자 정보가 애플리케이션에서 다시 생성되면, 실패 대기열이 자동으로 호출되고 미디어 파일은 미디어 파일이 성공적으로 저장될 때까지 재저장된다. 파일이 여전히 저장되지 않으면, 그 작업은 새로운 실패 대기열에 추가되고, 이전의 프로세스는 미디어 파일이 성공적으로 저장될 때까지 반복된다.

[0045] 도 2는 본 출원의 구현예 2에 따라 애플리케이션에 포함된 사용자 정보를 은닉하는 방법을 도시하는 개략적인 흐름도이다. 다음은 도 2을 참조하여 본원의 구현예 2에 제공되는 애플리케이션에 포함된 사용자 정보를 은닉하는 방법을 상세하게 설명한다. 도 2에 도시된 바와 같이, 본원의 구현예 2에 제공되는 애플리케이션에 포함된 사용자 정보를 은닉하는 방법은 다음과 같은 단계를 포함한다.

[0046] 단계(S201): 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득한다.

[0047] 본 구현예에서, 본 단계는 본원의 구현예 1에서 제공되는 애플리케이션에 포함된 사용자 정보를 은닉하는 방법의 단계(S101)와 기본적으로 동일하고, 여기서는 간략화를 위해 그 상세한 설명은 생략한다.

[0048] 단계(S202): 애플리케이션에서 생성된 사용자 정보에 대한 로직 처리를 수행한다.

[0049] 본 구현예에서, 애플리케이션에서 생성된 (민감한 기밀 사용자 정보와 같은) 사용자 정보의 공개 가능성을 회피하기 위해, 애플리케이션 내의 사용자 정보에 대해 로직 처리가 사전에 수행될 필요가 있다. 이전 로직 처리가 가역 로직 처리임에 주목할 가치가 있다. 구체적으로, 사용자 정보를 위한 로직 처리 프로세스는 가역적이다.

[0050] 애플리케이션에서 생성된 사용자 정보에 대한 로직 처리를 수행하는 것은 대칭 암호화 알고리즘을 사용하여 애플리케이션에서 생성된 사용자 정보에 대한 대칭 암호화 처리를 수행하는 것을 포함한다.

[0051] 확실히, 로직 처리 전에, MD5, DES, RSA, SM2 또는 SM3과 같은 암호화 알고리즘을 사용하여 사용자 정보가 암호화될 수 있음에 주목할 가치가 있다.

[0052] 단계(S203): 애플리케이션 내의 미디어 파일의 속성 리스트를 판독하고, 애플리케이션에서 로직 처리를 거친 사용자 정보를 미디어 파일의 속성 리스트에 기록한다.

[0053] 본 구현예에서, 로직 처리를 거친 사용자 정보가 키-값의 쌍의 형태로 미디어 파일의 속성 리스트에 기록되어 사용자 정보를 은닉할 수 있음에 주목할 가치가 있다. 예를 들어, 사용자 정보는 계정 암호이고, 계정 암호에 대응하는 속성 식별자 Key는 Password로 명명될 수 있다. 계정 암호의 속성 값 Value는 로직 처리 후에 획득되는 스트링 또는 문자열(character string)일 수 있다.

[0054] 단계(S204): 미디어 파일을 재저장한다.

[0055] 본 구현예에서, 은닉될 필요가 있는 모든 사용자 정보가 미디어 파일의 속성 리스트에 기록된 후에, 이전 미디어 파일은 재저장되어야 한다. 본 단계는 본원의 구현예 1에서 제공되는 애플리케이션에 포함된 사용자 정보를 은닉하는 방법의 단계(S103)와 기본적으로 동일하고, 여기서는 간략화를 위해 그 상세한 설명은 생략한다.

[0056] 전술한 설명은 본원의 구현예에서 애플리케이션에 포함된 사용자 정보를 은닉하는 방법을 제공한다. 본 출원의

구현예 3은 동일한 사상에 기초하여 애플리케이션에 포함된 사용자 정보를 은닉하기 위한 디바이스를 더 제공한다. 도 3은 본 출원의 구현예 3에 따라 애플리케이션에 포함된 사용자 정보를 은닉하는 디바이스의 구조를 도시한다. 이 디바이스는: 애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득하도록 구성된 획득 모듈(301)과; 애플리케이션에서 생성된 사용자 정보에 대한 로직 처리를 수행하도록 구성된 로직 처리 모듈(302)과; 애플리케이션 내의 미디어 파일의 속성 리스트를 판독하고, 애플리케이션에서 생성된 사용자 정보 또는 로직 처리를 거친 사용자 정보를 미디어 파일의 속성 리스트에 기록하도록 구성된 판독/기록 모듈(303)과; 미디어 파일을 재저장하도록 구성된 저장 모듈(304)을 포함한다.

[0057] 이전 속성 리스트는 미디어 파일을 설명하는 데 사용된 속성 정보를 포함하는 것에 주목할 가치가 있다. 사용자 정보는 민감한 기밀 정보이며 이전 미디어 파일은 그림 파일, 오디오 파일, 및 비디오 파일을 포함한다. 또한 이전 사용자 정보는 대안으로 사전 암호화된 사용자 정보일 수 있다.

[0058] 애플리케이션에서 생성된 사용자 정보에 대한 로직 처리를 수행하는 것은 가역 로직 처리이며, 예를 들어, 로직 처리는 대칭 암호화일 수 있다.

[0059] 결론적으로, 본 출원의 구현예에 제공된 애플리케이션에 포함된 사용자 정보를 은닉하는 방법 및 디바이스에 따르면, 애플리케이션에서 생성된 사용자 정보는 애플리케이션 내의 미디어 파일의 속성 리스트에 기록된다. 이와 같이, 사용자 정보는 은닉되어 모바일 디바이스의 로컬 폴더에서 거의 발견 및 획득될 수 없고, 애플리케이션에서 생성된 사용자 정보는 공개되지 않게 된다.

[0060] 1990 년대에, 기술 개선이 하드웨어 개선(예를 들어, 다이오드, 트랜지스터 또는 스위치와 같은 회로 구조 개선)인지 소프트웨어 개선(방법 절차의 개선)인지는 명백하게 구분될 수 있다. 그러나, 기술이 발전함에 따라 많은 방법 절차에 대한 현재의 개선은 하드웨어 회로 구조의 직접적인 개선으로 간주될 수 있다. 설계자는 일반적으로 하드웨어 회로에 대해 개선된 방법 절차를 프로그램하여 해당 하드웨어 회로 구조를 획득한다. 따라서, 하드웨어 개체 모듈을 사용하여 방법 절차를 향상시킬 수 있다. 예를 들어, 프로그램 가능 로직 디바이스(PLD)(예를 들어, 필드 프로그램 가능 게이트 어레이(FPGA))는 그러한 집적 회로이고, PLD의 논리적 기능은 디바이스 프로그래밍을 통해 사용자에 의해 결정된다. 설계자는 칩 제조업체에 ASIC 칩(2)을 설계하고 생산하도록 요청하지 않고도 디지털 시스템을 PLD에 "통합"하는 프로그래밍을 수행한다. 또한, 프로그래밍은 집적 회로 칩을 수동으로 제작하는 대신 "로직 컴파일러" 소프트웨어를 사용하여 주로 구현된다. 이는 프로그램 개발 및 컴파일에 사용되는 소프트웨어 컴파일러와 유사하다. 그러나, 컴파일 전의 원본 코드는 하드웨어 서술 언어(HDL)라고 지칭되는 특정 프로그래밍 언어로 기록된다. ABEL(Advanced Boolean Expression Language), AHDL(Altera Hardware Description Language), CUPL(Cornell University Programming Language), HDCal, JHDL(Java Hardware Description Language), Lava, Lola, MyHDL, PALASM 및 RHDL(Ruby Hardware Description Language)과 같은 많은 HDL이 존재한다. 현재, 초고속 집적 회로 하드웨어 서술 언어(VHDL)와 Verilog2가 가장 일반적으로 사용된다. 당업자는 또한, 설명된 몇몇 하드웨어 서술 언어를 사용하여 방법 절차가 논리적으로 프로그래밍되고 집적 회로에 프로그래밍되면, 논리적 방법 절차를 구현하는 하드웨어 회로가 쉽게 획득될 수 있음을 이해해야 한다.

[0061] 제어기는 임의의 적절한 방식으로 구현될 수 있다. 예를 들어, 제어기는 마이크로프로세서, 프로세서, 또는 프로세서(또는 마이크로프로세서)에 의해 실행될 수 있는 컴퓨터 판독 가능 프로그램 코드(예를 들어, 소프트웨어 또는 펌웨어)를 저장하는 컴퓨터 판독 가능 매체, 로직 게이트, 스위치, 주문형 집적 회로(ASIC), 프로그램 가능 로직 제어기, 또는 임베디드 마이크로제어기일 수 있다. 제어기의 예는 ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20, 또는 Silicon Labs C8051F320과 같은 마이크로제어기를 포함하지만 이에 국한되는 것은 아니다. 메모리 제어기는 또한 메모리의 제어 로직의 일부로서 구현될 수 있다. 당업자는 또한, 제어기가 순수한 컴퓨터 판독 가능 프로그램 코드를 사용하여 구현될 수 있으며, 방법의 단계는 제어기가 로직 게이트, 스위치, ASIC, 프로그램 가능 로직 제어기, 임베디드 마이크로제어기 등의 형태의 동일 기능을 구현할 수 있도록 논리적으로 프로그래밍될 수 있다는 것을 알고 있다. 따라서, 제어기는 하드웨어 구성 요소로 간주될 수 있고, 제어기 내의 다양한 기능을 구현하도록 구성된 디바이스는 하드웨어 구성 요소의 구조로 간주될 수도 있다. 대안으로, 다양한 기능을 구현하도록 구성된 디바이스는 방법 또는 하드웨어 구성 요소의 구조를 구현할 수 있는 소프트웨어 모듈로 간주될 수 있다.

[0062] 이전 구현예에 도시된 시스템, 디바이스, 모듈, 또는 유닛은 컴퓨터 칩 또는 개체를 사용하여 구현될 수 있거나, 특정 기능을 갖는 제품을 사용하여 구현될 수 있다.

[0063] 설명의 용이함을 위해, 설명된 디바이스는 기능을 다양한 유닛으로 분할함으로써 기술된다. 물론, 본 출원이

구현될 때, 각 유닛의 기능은 하나 이상의 소프트웨어 및/또는 하드웨어 부분으로 구현될 수 있다.

[0064] 당업자는 본 발명의 구현예가 방법, 시스템, 또는 컴퓨터 프로그램 제품으로서 제공될 수 있음을 이해해야 한다. 따라서, 본 발명은 하드웨어 전용 구현예, 소프트웨어 전용 구현예, 또는 소프트웨어와 하드웨어의 조합을 갖는 구현예의 형태를 사용할 수 있다. 또한, 본 발명은 컴퓨터 사용 가능 프로그램 코드를 포함하는 하나 이상의 컴퓨터 사용 가능 저장 매체(자기 디스크 메모리, CD-ROM 및 광학 메모리를 포함하지만 이에 국한되지 않음) 상에 구현되는 컴퓨터 프로그램 제품의 형태를 사용할 수 있다.

[0065] 본 발명은 본 발명의 구현예에 기초한 방법, 디바이스(시스템) 및 컴퓨터 프로그램 제품의 흐름도 및/또는 블록도를 참조하여 설명된다. 컴퓨터 프로그램 명령어는 흐름도 및/또는 블록도에서의 각각의 절차 및/또는 각각의 블록 및 흐름도 및/또는 블록도에서의 절차 및/또는 블록의 조합을 구현하는 데 사용될 수 있다는 것을 이해해야 한다. 이 컴퓨터 프로그램 명령어는 범용 컴퓨터, 전용 컴퓨터, 임베디드 프로세서, 또는 다른 프로그램 가능 데이터 처리 디바이스의 프로세서에 제공되어 머신을 생성할 수 있다. 이와 같이, 명령어는 컴퓨터 또는 다른 프로그램 가능 데이터 처리 디바이스의 프로세서에 의해 실행되어 흐름도의 하나 이상의 절차 및/또는 블록도의 하나 이상의 블록에서의 특정 기능을 구현하는 디바이스를 생성한다.

[0066] 이 컴퓨터 프로그램 명령어는 컴퓨터 판독 가능 메모리에 저장되어, 컴퓨터 또는 다른 프로그램 가능 데이터 처리 디바이스가 특정 방식으로 동작하도록 명령할 수 있다. 이와 같이, 컴퓨터 판독 가능 메모리에 저장된 명령어는 명령 디바이스를 포함하는 인공물(artifact)을 생성한다. 명령 디바이스는 흐름도의 하나 이상의 절차 및/또는 블록도의 하나 이상의 블록에서의 특정 기능을 구현한다.

[0067] 이 컴퓨터 프로그램 명령어는 컴퓨터 또는 다른 프로그램 가능 데이터 처리 디바이스 상에 로딩될 수 있고 그에 따라, 일련의 동작 및 단계가 컴퓨터 또는 다른 프로그램 가능 디바이스 상에서 수행되어, 컴퓨터로 구현되는 처리를 생성할 수 있다. 따라서, 컴퓨터 또는 다른 프로그램 가능 디바이스 상에서 실행되는 명령어는 흐름도의 하나 이상의 절차 및/또는 블록도의 하나 이상의 블록에서의 특정 기능을 구현하는 단계를 제공한다.

[0068] 통상적인 구성에서, 컴퓨팅 디바이스는 하나 이상의 프로세서(CPU), 입력/출력 인터페이스, 네트워크 인터페이스 및 메모리를 포함한다.

[0069] 메모리는 판독 전용 메모리(ROM) 또는 플래시 메모리(플래시 RAM)와 같은 컴퓨터 판독 가능 매체에서 비 영구 메모리, RAM 및/또는 비 휘발성 메모리 등을 포함할 수 있다. 메모리는 컴퓨터 판독 가능 매체의 일 예이다.

[0070] 컴퓨터 판독 가능 매체는 임의의 방법 또는 기술을 사용하여 정보를 저장할 수 있는 영구적, 비 영구적, 이동식 및 비 이동식 매체를 포함한다. 정보는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈, 또는 다른 데이터일 수 있다. 컴퓨터 저장 매체의 예는 위상 변화 랜덤 액세스 메모리(PRAM), 스태틱 RAM(SRAM), 다이나믹 RAM(DRAM), 다른 타입의 RAM, ROM(read-only memory), EEPROM(electrically erasable programmable read-only memory), 플래시 메모리 또는 다른 메모리 기술, CD-ROM, DVD 또는 다른 광학 저장 디바이스, 자기 테이프, 자기 디스크 저장 디바이스, 다른 자기 저장 디바이스, 또는 임의의 다른 비 전송 매체를 포함하지만 이에 국한되지는 않는다. 컴퓨터 저장 매체는 컴퓨팅 디바이스에 의해 액세스될 수 있는 정보를 저장하는 데 사용될 수 있다. 본 명세서에서 기술된 바와 같이, 컴퓨터 판독 가능 매체는 임시 매체, 예를 들어, 변조된 데이터 신호 및 반송파를 포함하지 않는다.

[0071] "포함하는", "구비하는", 또는 임의의 다른 변형 용어는 비 배타적인 포함을 포괄하는 것이어서, 일련의 요소를 포함하는 프로세스, 방법, 제품 또는 디바이스가 이러한 요소를 포함할 뿐만 아니라, 명시적으로 나열되지 않은 다른 요소를 포함하거나, 그러한 프로세스, 방법, 제품 또는 디바이스에 고유한 요소를 추가로 포함한다는 것에 추가로 주목할 가치가 있다. "무언가를 포함하는"에서 무언가의 요소는 그 무언가의 요소를 포함하는 프로세스, 방법, 제품, 또는 디바이스에서 추가적인 많은 제약없이 추가적인 동일한 요소의 존재를 배제하는 것이 아니다.

[0072] 당업자는 본 출원의 구현예가 방법, 시스템, 또는 컴퓨터 프로그램 제품으로서 제공될 수 있음을 이해해야 한다. 따라서, 본 출원은 하드웨어 전용 구현예, 소프트웨어 전용 구현예, 또는 소프트웨어와 하드웨어의 조합을 갖는 구현예의 형태를 사용할 수 있다. 또한, 본 출원은 컴퓨터 사용 가능 프로그램 코드를 포함하는 하나 이상의 컴퓨터 사용 가능 저장 매체(자기 디스크 메모리, CD-ROM 및 광학 메모리를 포함하지만 이에 국한되지 않음) 상에 구현되는 컴퓨터 프로그램 제품의 형태를 사용할 수 있다.

[0073] 본 출원은 프로그램 모듈과 같은 컴퓨터에 의해 실행되는 컴퓨터 실행 가능 명령어의 공통 콘텍스트로 기술될 수 있다. 일반적으로, 프로그램 모듈은 특정의 작업을 실행하거나 특정의 추상화 데이터 타입을 구현하는

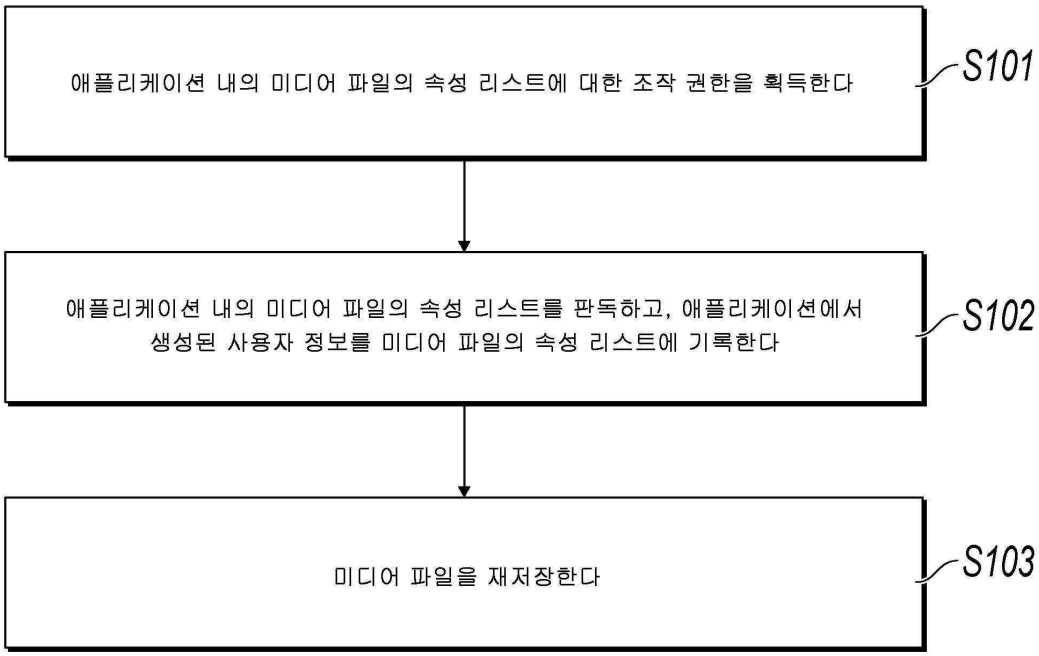
루틴, 프로그램, 객체, 컴포넌트, 데이터 구조 등을 포함한다. 본 출원은 분산 컴퓨팅 환경에서도 실행될 수 있다. 이러한 분산 컴퓨팅 환경에서, 작업은 통신 네트워크를 사용하여 접속된 원격 처리 디바이스에 의해 실행된다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 저장 디바이스를 포함하는 로컬 및 원격 컴퓨터 저장 매체에 위치할 수 있다.

[0074] 본 명세서에서의 구현예는 점진적으로 설명된다. 구현예에서 동일하거나 유사한 부분에 대해서는 그 구현예를 참조할 수 있다. 각각의 구현예는 다른 구현예와의 차이점에 중점을 둔다. 특히, 시스템 구현예는 방법 구현예와 유사하므로 간략하게 설명된다. 관련 부분에 대해서는 방법 구현예의 관련 설명을 참조할 수 있다.

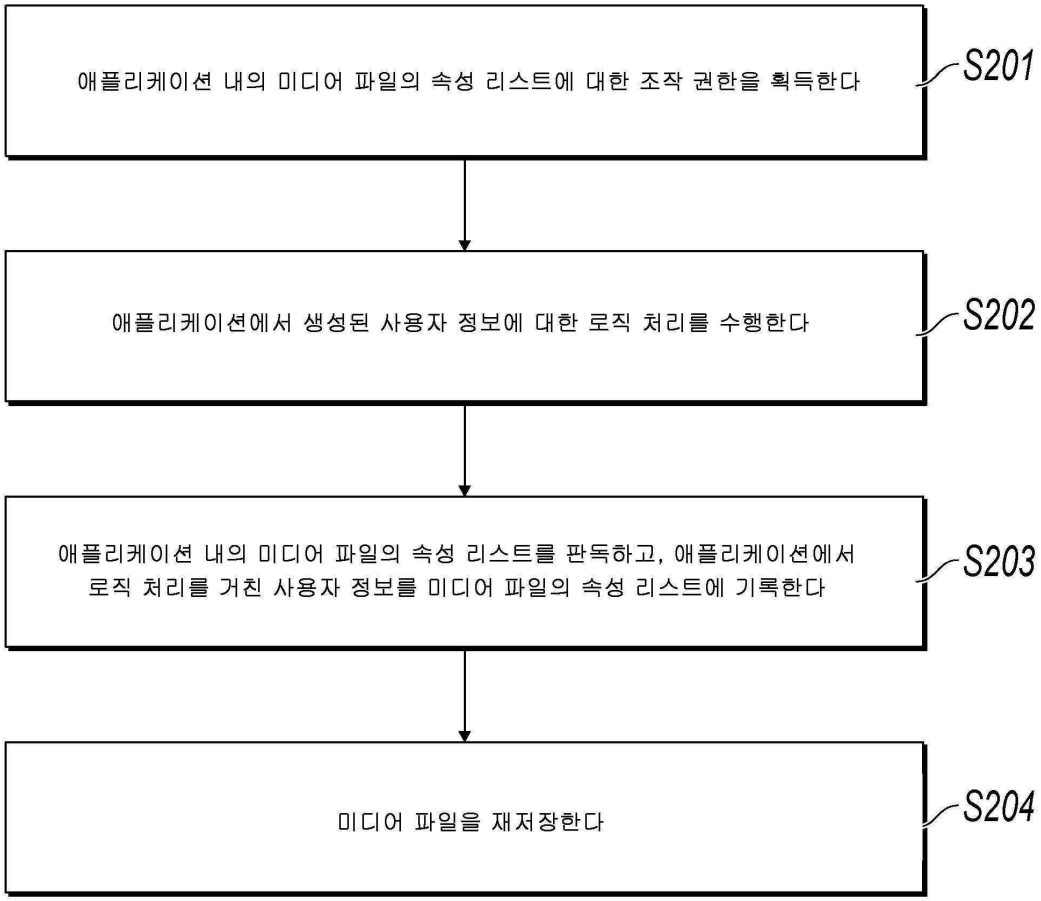
[0075] 전술한 설명은 단지 본 발명의 구현예일 뿐이며, 본 출원을 제한하려는 것이 아니다. 당업자라면 본 출원에 대해 다양한 수정 및 변경을 가할 수 있다. 본원의 사상 및 원리 내에서 이루어진 임의의 수정, 등가의 치환, 개선 등은 본원의 청구범위의 보호 범위에 속해야 한다.

도면

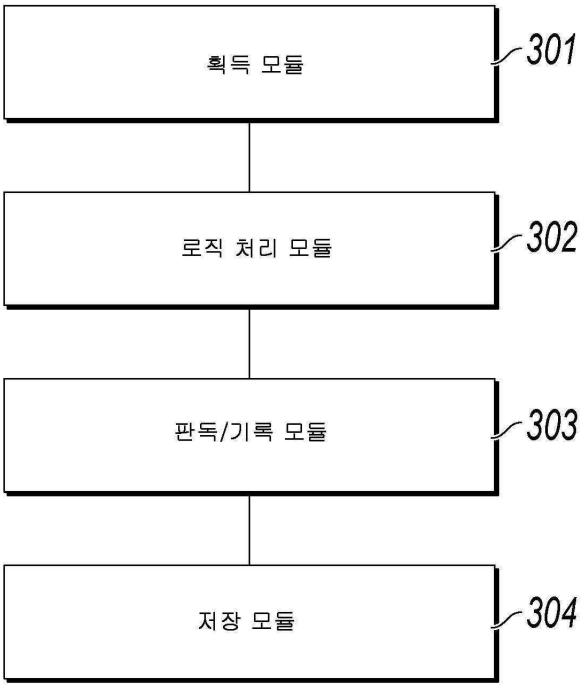
도면1



도면2


애플리케이션 내의 미디어 파일의 속성 리스트에 대한 조작 권한을 획득한다
S201
애플리케이션에서 생성된 사용자 정보에 대한 로직 처리를 수행한다
S202
애플리케이션 내의 미디어 파일의 속성 리스트를 판독하고, 애플리케이션에서 로직 처리를 거친 사용자 정보를 미디어 파일의 속성 리스트에 기록한다
S203
미디어 파일을 재저장한다
S204

도면3


획득 모듈
301
로직 처리 모듈
302
판독/기록 모듈
303
저장 모듈
304