(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06Q 20/00A2 (2006.01)

(11) 공개번호 10-2007-0007185
(43) 공개일자 2007년01월12일

(21) 출원번호 10-2006-7023434
(22) 출원일자 2006년11월08일
심사청구일자 없음
번역문 제출일자 2006년11월08일
(86) 국제출원번호 PCT/IB2005/051452
국제출원일자 2005년05월04일
(87) 국제공개번호 WO 2005/109734
국제공개일자 2005년11월17일

(30) 우선권주장 04102012.4 2004년05월10일 유럽특허청(EPO)(EP)

(71) 출원인 코닌클리케 필립스 일렉트로닉스 엔.브이.
네델란드왕국, 아인드호펜, 그로네보드스베그 1

(72) 발명자 웨이, 공밍
네덜란드, 아인트호벤 엔엘-5656 에이에이, 프로프. 홀스트란 6
리, 펭
네덜란드, 아인트호벤 엔엘-5656 에이에이, 프로프. 홀스트란 6
루이트젠스, 스티븐, 비.
네덜란드, 아인트호벤 엔엘-5656 에이에이, 프로프. 홀스트란 6
헤, 다윈
네덜란드, 아인트호벤 엔엘-5656 에이에이, 프로프. 홀스트란 6
유, 웨닝
네덜란드, 아인트호벤 엔엘-5656 에이에이, 프로프. 홀스트란 6
폰티즌, 윌헬머스, 에프., 제이.
네덜란드, 아인트호벤 엔엘-5656 에이에이, 프로프. 홀스트란 6

(74) 대리인 문경진

전체 청구항 수 : 총 12 항

(54) 바이오메트릭 데이터를 가지고 보안된 거래를 기록할 수있는 개인용 통신 장치

(57) 요약

거래(240)의 검증 가능한 기록을 생성하기 위한 예를 들면, 휴대폰과 같은 개인용 통신 장치(10)가 설명되는데, 이 거래(240)는 정보의 교환을 포함한다. 이 장치는 수신 소자, 보호 소자, 메모리 및 기록 소자를 포함한다. 수신 소자는 이 장치의 사용자(100)와 원격 개인간의 거래를 수신하고, 원격 개인의 바이오메트릭 데이터(BIOKY)를 수신할 수 있다. 보호 소자는 바이오메트릭 데이터(BIOKY)를 사용해서 음성 대화를 보호할 수 있다. 기록 소자는 메모리(30)에서 바이오메트릭 데이터를 사용해서 보호된 거래를 기록할 수 있다. 통신 장치(10)가 또한 설명되는데, 이 통신 장치는 거래의 인증을 지원하기 위해 동작 가능한 동일한 휴대폰일 수 있다. 통신 장치는 메모리(30)와 인증 소자를 포함한다. 만약 바이오메트릭 측정 수단(80)에 의해 측정된 바이오메트릭 데이터(BIOKY)가 음성 대화(240)를 보호하기 위해 사용된 보다 이전의 바이오메트릭 데이터(BIOKY)에 대응한다면, 인증 소자는 메모리에 저장된 보호된 거래로의 액세스를 제공할 수 있다.

대표도

도 1

특허청구의 범위

청구항 1.

거래(240)의 검증가능한 기록을 생성하기 위한 개인용 통신 장치(10)로서, 상기 거래는 정보의 교환을 포함하고, 상기 장치(10)는:

a) 상기 장치의 사용자(100)와 원격 개인간의 거래를 수신하고, 상기 원격 개인의 바이오메트릭 데이터를 수신하기 위한 수신 소자;

b) 상기 바이오메트릭 데이터를 가지고 상기 거래를 보호하기 위한 보호 소자;

c) 상기 보호된 거래(240)를 저장하기 위한 메모리(30); 및

d) 상기 바이오메트릭 데이터를 가지고 보호된 상기 거래(240)를 상기 메모리(30)상에 기록하기 위한 기록 소자를 포함하는, 개인용 통신 장치.

청구항 2.

제1항에 있어서, 상기 보호 소자는 하나 이상의 액세스 키(RANKY)를 생성함으로써 상기 바이오메트릭 데이터를 가지고 상기 거래를 보호하고, 하나 이상의 액세스 키(RANKY)를 가지고 상기 거래를 암호화하고, 상기 바이오메트릭 데이터를 가지고 상기 하나 이상의 액세스 키를 보호하고, 상기 보호된 하나 이상의 액세스 키를 상기 메모리(30)에 저장할 수 있는, 개인용 통신 장치.

청구항 3.

제2항에 있어서, 상기 메모리는 키로커(keylocker)(330)를 포함하고, 상기 보호 소자는 상기 키로커(330)에 있는 상기 바이오메트릭 데이터와 함께 상기 하나 이상의 액세스 키(RANKY)를 저장함으로써 상기 보호된 하나 이상의 액세스 키를 상기 메모리(30)에 저장할 수 있는, 개인용 통신 장치.

청구항 4.

제2항에 있어서, 상기 보호 소자는 상기 보호된 거래(240)를 액세스하는 데 사용하기 위한 하나 이상의 보안 키(ENCKY)를 생성하기 위해 바이오메트릭 키(BIOKY)를 사용해서, 상기 하나 이상의 액세스 키(RANKY)를 암호화함으로써 상기 바이오메트릭 데이터를 가지고 상기 하나 이상의 액세스 키를 보호할 수 있고, 상기 바이오메트릭 키(BIOKY)는 상기 바이오메트릭 데이터에 대응하거나 상기 바이오메트릭 데이터로부터 생성되는, 개인용 통신 장치.

청구항 5.

제1항에 있어서, 상기 수신 소자는 바이오메트릭 측정 수단(80)으로부터 바이오메트릭 데이터를 수신할 수 있으며, 상기 바이오메트릭 측정 수단(80)은 인간의 하나 이상의 손가락의 지문 이미징, 음성 발성의 음성 내용의 분석, 이미지 분석을 수반하는 얼굴 이미징, 인간 홍채 이미지 분석, 치아 이미징, 또는 귀 윤곽 분석중의 하나 이상을 포함하는, 개인용 통신 장치.

청구항 6.

컴퓨팅 수단을 제1항의 개인용 통신 장치(10)로서 기능할 수 있게 하는 상기 컴퓨팅 수단 상에 실행 가능한 소프트웨어.

청구항 7.

거래의 인증을 지원하기 위해 동작 가능한 개인용 통신 장치(10)로서,

상기 거래는 정보 교환을 포함하는, 개인용 통신 장치(10)에 있어서,

a) 보다 이전의 바이오메트릭 데이터를 가지고 보호된 거래(240)를 저장하기 위한 메모리(30); 및

b) 만약 바이오메트릭 측정 수단(80)에 의해 측정된 바이오메트릭 데이터가 상기 보다 이전의 바이오메트릭 데이터에 대응한다면, 상기 보호된 거래로의 액세스를 제공하기 위한 인증 소자를 포함하는 것을 특징으로 하는, 개인용 통신 장치.

청구항 8.

제7항에 있어서, 상기 바이오메트릭 데이터가 상기 보다 이전의 바이오메트릭 데이터에 대응한다는 조건하에, 상기 인증 소자는 상기 보호된 거래를 복호화하기 위한 하나 이상의 액세스 키(RANKY)를 제공할 수 있고, 상기 개인용 통신 장치는, 상기 보호된 거래(240)의 적어도 일부를 복호화하기 위해 상기 하나 이상의 액세스 키(RANKY)를 사용하기 위한 복호화 소자(20)를 더 포함하는, 개인용 통신 장치.

청구항 9.

제8항에 있어서, 상기 인증 소자는 하나 이상의 측정된 바이오메트릭 키(BIOKY)를 가지고 하나 이상의 보안 키(ENCKY)를 복호화함으로써 상기 하나 이상의 검증된 액세스 키(RANKY)를 획득할 수 있는, 개인용 통신 장치.

청구항 10.

제8항에 있어서, 상기 하나 이상의 액세스 키는 보다 이전의 바이오메트릭 데이터와 연관된 키로커(330)에서 유지되어, 그 결과 상기 측정된 바이오메트릭 데이터의 상기 키로커(330)로의 제공(presentation)은, 상기 측정된 바이오메트릭 데이터에 대응하는 상기 키로커(330)에 있는 상기 보다 이전의 바이오메트릭 데이터에 따라, 상기 하나 이상의 액세스 키(RANKY)로의 액세스를 가능케하는, 개인용 통신 장치.

청구항 11.

제7항에 있어서, 상기 인증 소자는 바이오메트릭 측정 수단(80)으로부터 바이오메트릭 데이터를 수신할 수 있으며, 상기 바이오메트릭 측정 수단(80)은 인간 손의 하나 이상의 손가락의 지문 이미징, 음성 발성의 음성 내용의 분석, 이미지 분석을 수반하는 얼굴 이미징, 인간 홍채 이미지 분석, 치아 이미징, 또는 귀 윤곽 분석 중의 하나 이상을 포함하는, 개인용 통신 장치.

청구항 12.

컴퓨팅 수단을 제7항의 개인용 통신 장치(10)로서 기능할 수 있게 하는 상기 컴퓨팅 수단 상에 실행 가능한 소프트웨어.

명세서

기술분야

본 발명은 검증 가능한 데이터 파일을 생성하기 위한 개인용 통신 장치에 관한 것이다. 본 발명은 데이터 파일의 인증(authenticity)을 검증하기 위한 개인용 통신 장치에 관한 것이다. 본 발명은 컴퓨팅 수단을, 검증 가능한 데이터 파일을 생성하고 및/또는 데이터 파일의 인증을 검증하기 위한 개인용 통신 장치로서 기능할 수 있게 하는 컴퓨터 수단 상에서 실행 가능한 소프트웨어에 또한 관련이 있다.

배경기술

데이터 파일과 데이터 전송 과정의 인증은 거래에서, 예를 들면, 전자 금융 시스템에서의 거래에 대해, 잘 알려져 있고, 아주 중요하다. 이러한 금융 시스템에서 하나의 은행 구좌로부터 다른 구좌로 현금을 이체하기 위한 요청이 사기(fraudulent)인지를 아는 것은 중요하다. 종종 이러한 거래는 수반된 당사자간의 법률적인 구속력이 있는 계약의 형태를 잠재적으로 취할 수 있다. 유사한 고려는 또한 이메일 통신에 의한 계약에 또한 관련이 있고, 구두 계약에도 또한 증가하고 있다. 구두 계약이 전자 통신 매체 예를 들면 휴대폰을 통해 행해 졌을 때, 대화하는 개인의 인증은 중요하다. 만약 주어진 화자가 모호하지 않다고 식별될 수 있다면, 화자의 기록은 인증된 것으로 잠재적으로 반박할 수 없게 검증될 수 있다.

공개된 미국 특허 US2002/0107816는 구두 거래를 보안적으로 기록하기 위한 방법과 시스템을 설명한다. 이 방법은:

a) 디지털 오디오 파일로서 거래의 제공과 수령을 기록하는 단계;

b) 기록된 디지털 오디오 파일로부터 음성 보안 토큰을 생성하는 단계; 및

c) 생성된 음성 보안 토큰을 판매자와 구매자에게 제공하는 단계를 포함한다.

발명의 상세한 설명

본 발명자들은 음성/오디오 기록은 매우 개인적이고 사적인 실체일 수 있다는 것을 인식하여 왔다. 예를 들면, 가능하게 공갈자들의 손에 넘어가는 사적인 문제에 관련된 음성 기록은 음성 기록을 생성하는 개인으로부터 돈을 갈취하기 위해 사용될수 있다. 하지만, 본 발명자들은 휴대용 통신 디바이스 예를 들면 휴대폰은 미래에 이러한 통신 디바이스에 병합된 예를 들면 소형 광 데이터 저장 매체 형태의 상당한 저장 용량과 연관된 판독/기록 드라이브가 장착될 것이라는 것을 또한 예견했다. 초창기의 이메일 메시지가 가능한 나중의 참조를 위해 저장되고 보관된 이메일 통신 시스템과 유사한 방식으로, 유사한 동작 방식은 미래의 휴대폰과도 관련이 있을 것이라는 것이 예견되었다. 따라서, 미래의 휴대폰은 착탈 가능한 데이터 캐리어를 포함하여 예를 들면 1 Gbyte 이상의 상대적으로 대용량 메모리를 포함할 것이며, 예를 들면, 미래의 응용에서, 휴대폰 사용자는 기록된 통신문, 편지 등의 수집과 유사한 방식으로 과거 전화 대화의 완벽한 라이브러리(library)를 잠재적으로 구축할 수 있다. 음성 대화를 기록할 수 있는 개인 통신 디바이스는 본 명세서에 참조로 병합된 특허 US2003/0032448('logbook emulet')로부터 알려진다. 따라서, 데이터 캐리어에 기록된 과거에 기록된 대화의 인증과 보안이 바람직하고, 본 발명에서 다루어 진다.

본 발명의 목적은 예를 들면 음성 대화와 같은 거래를 인증하기 위한 개인용 통신 장치를 제공하는 것이다.

본 발명의 제1 양상에 따라, 개인용 통신 장치가 거래의 검증가능한 기록을 생성하기 위해 제공되는데, 이 거래는 정보 교환을 포함하며, 이 장치는:

a) 상기 장치의 사용자와 원격 개인간의 거래를 수신하고, 상기 원격 개인의 바이오메트릭 데이터를 수신하기 위한 수신 소자;

b) 상기 바이오메트릭 데이터를 가지고 상기 거래를 보호하기 위한 보호 소자;

c) 상기 보호된 거래를 저장하기 위한 메모리; 및

d) 상기 메모리에 상기 바이오메트릭 데이터를 가지고 보호된 상기 거래를 기록하기 위한 기록 소자를 포함한다.

비호환 바이오메트릭 데이터를 갖는 권한 없는 제3자가 거래를 해독할 수 없어서 그 콘텐츠에 대해 액세스할 수 없으므로 본 발명은 이롭다. 추가적으로, 만약 제3자가 거래를 해독할 수 있다면, 이것이 이 당사자가 이 거래에서의 참가자였다는 증거다. 바이오메트릭 데이터는 쉽게 위조 및/또는 손실될 수 없다. 거래는 예를 들면, 음성 대화, 비디오 통신 또는 기록된 메시지일 수 있다. 개인용 통신 장치는 예를 들면, 휴대폰 또는 휴대폰을 위한 추가 기기일 수 있다. 휴대폰을 위한 부가 기기는 휴대폰에 물리적으로 부착될 수 있거나, 블루투스(Bluetooth)와 같은 무선 기술을 사용함으로써 휴대폰을 가지고 통신할 수 있다.

개인용 통신 장치에서, 보호 소자는 바람직하게 하나 이상의 액세스 키(RANKY)를 생성함으로써 상기 바이오메트릭 데이터를 가지고 상기 거래를 보호하고, 하나 이상의 액세스 키(RANKY)를 가지고 상기 거래를 암호화하고, 상기 바이오메트릭 데이터를 가지고 상기 하나 이상의 액세스 키를 보호하고, 상기 메모리에 상기 보호된 하나 이상의 액세스 키를 저장할 수 있다. 이런 경우에, 다수의 개인들이 거래가 한 번 이상 암호화되는 것이 요구될 필요가 없이, 단일 거래로의 액세스가 허용될 수 있다. 만약 거래가 음성 대화 또는 비디오 통신과 같은 대형 데이터 파일로 이루어진다면, 이것은 특히 이롭다.

개인용 통신 장치에서, 메모리는 바람직하게 키로커를 포함하고, 보호 소자는 키로커에 있는 바이오메트릭 데이터와 함께 하나 이상의 액세스 키(RANKY)을 저장함으로써 메모리에서 보호된 하나 이상의 액세스 키를 저장할 수 있다. 디지털 권한 관리(DRM) 시스템은 종종 키, 즉, 디지털 권리를 저장하기 위한 키로커를 사용한다. 이들 시스템에서 키로커는 또한 (디지털) 권리 로커로 알려져 있다. 신뢰된 DRM 애플리케이션만이 키로커에 저장된 키로의 액세스가 허용된다.

개인용 통신 장치에서, 보호 소자는 바람직하게 상기 보호된 음성 대화를 액세스하는 데 사용하기 위한 하나 이상의 보안 키(ENCKY)를 생성하기 위해 바이오메트릭 키(BIOKY)를 사용해서, 상기 하나 이상의 액세스 키(RANKY)를 암호화함으로써 상기 바이오메트릭 데이터를 가지고 상기 하나 이상의 액세스 키를 보호할 수 있고, 상기 바이오메트릭 키(BIOKY)는 상기 바이오메트릭 데이터에 대응하거나 상기 바이오메트릭 데이터로부터 생성된다.

개인용 통신 장치에서, 상기 수신 소자는 바람직하게 바이오메트릭 측정 수단으로부터 바이오메트릭 데이터를 수신할 수 있으며, 상기 바이오메트릭 측정 수단은 인간의 하나 이상의 손가락의 지문 이미징, 음성 발성의 음성 내용의 분석, 이미지 분석을 수반하는 안면 이미징, 인간 홍채 이미지 분석, 치아 이미징, 또는 귀 윤곽 분석 중의 하나 이상을 포함한다.

본 발명의 제2 양상에 따라, 거래의 인증을 지원하기 위해 동작 가능한 개인용 통신 장치가 제공되는데, 상기 거래는 정보 교환을 포함하고, 상기 장치는:

a) 보다 이전의 바이오메트릭 데이터를 가지고 보호된 거래를 저장하기 위한 메모리; 및

b) 만약 바이오메트릭 측정 수단에 의해 측정된 바이오메트릭 데이터가 보다 이전의 바이오메트릭 데이터에 대응한다면, 상기 보호된 거래로의 액세스를 제공하기 위한 인증 소자를 포함하는 것을 특징으로 한다.

개인용 통신 장치에서, 상기 바이오메트릭 데이터가 상기 보다 이전의 바이오메트릭 데이터에 대응한다는 조건하에, 상기 인증 소자는 바람직하게 상기 보호된 거래를 복호화하기 위한 하나 이상의 액세스 키(RANKY)를 제공할 수 있고, 상기 개인용 통신 장치는 바람직하게 상기 보호된 거래의 적어도 일부를 복호화하기 위해 상기 하나 이상의 액세스 키(RANKY)를 사용하기 위한 복호화 소자를 더 포함한다.

개인용 통신 장치에서, 상기 인증 소자는 하나 이상의 측정된 바이오메트릭 키(BIOKY)를 가지고 하나 이상의 보안 키(ENCKY)를 복호화함으로써 상기 하나 이상의 검증된 액세스 키(RANKY)를 바람직하게 획득할 수 있다.

개인용 통신 장치에서, 상기 하나 이상의 액세스 키는 보다 이전의 바이오메트릭 데이터와 연관된 키로커(330)에서 바람직하게 유지되고, 그 결과 상기 측정된 바이오메트릭 데이터의 상기 키로커로의 제시(presentation)는 상기 측정된 바이오메트릭 데이터에 대응하는 상기 키로커에 있는 보다 이전의 바이오메트릭 데이터에 따라, 상기 하나 이상의 액세스 키(RANKY)로의 액세스를 가능케한다.

개인용 통신 장치에서, 바람직하게 상기 인증 소자는 바이오메트릭 측정 수단으로부터 바이오메트릭 데이터를 수신할 수 있으며, 상기 바이오메트릭 측정 수단은 인간 손의 하나 이상의 손가락의 지문 이미징, 음성 발성의 음성 내용의 분석, 이미지 분석을 수반하는 안면 이미징, 인간 홍채 이미지 분석, 치아 이미징, 또는 귀 윤곽 분석 중의 하나 이상을 포함한다.

본 발명의 특징이 본 발명의 범위를 이탈함이 없이 임의로 조합될 수 있다는 것이 인식될 것이다.

본 발명의 실시예는 아래의 도면을 참조하면서 단지 예시로서 이제 설명될 것이다.

실시예

본 발명의 개요가 이제 도 1을 참조하면서 제공될 것이다. 도 1에서, 휴대폰과 같은 개인용 통신 장치가 참조 번호(10)에 의해 일반적으로 표시된다. 장치(10)는 데이터 메모리(MEM)(30)에 연결된 데이터-처리 유닛(DPU)(20)을 포함하고, 처리 유닛(20)은 소프트웨어를 실행시키기 위한 하나 이상의 컴퓨팅 디바이스를 포함한다. 장치(10)는 처리 유닛(20)에 연결된 소형 박막 트랜지스터(TFT) 액정 디스플레이(LCD)와 같은 디스플레이 디바이스(DISP)(40)를 더 포함한다. 또한, 장치(10)는 무선 통신(60)을 송수신하기 위해 처리 유닛(20)에 연결된 무선 트랜시버(RX/TX)(50)를 포함한다. 또한, 장치(10)는 처리 유닛(20)에 연결된 오디오 인터페이스(AINT)(70)를 포함하고, 인터페이스(70)는 마이크(80)와 또한 소형 스피커 또는 피에쪼-전기(piezo-electric) 소자(90)를 포함한다. 마이크(80)와 스피커/소자(90)는 사용자(100)의 음성을 감지하고, 또한 사용자(100)가 청취할 음향을 생성하기 위해 제각기 사용된다. 처리 유닛(20)으로의 데이터 입력을 위한 키패드(KY)(110)가 또한 포함된다. 메모리(30)는 착탈가능한 데이터 캐리어, 보다 상세하게는, 판독/기록가능한 자기 데이터 캐리어와, Philips사 전유의(proprietary) 광 메모리 시스템인 "휴대용 블루(Portable Blue)"에서 채택된 SFFO 광 디스크와 같은 광 데이터 캐리어 중 적어도 하나를 사용해 바람직하게 구현될 수 있다. 처리 유닛(20)은 소프트웨어 운영 체계와, 처리 유닛(20)에서 실행하기 위한 하나 이상의 특정 소프트웨어 애플리케이션을 저장하기 위한 비휘발성 판독 전용 메모리(ROM)와 같은 로컬 메모리에 또한 바람직하게 연결된다. 하나 이상의 특정 소프트웨어 애플리케이션은 다음의 기능:

- 이 장치의 사용자(100)와 원격 개인간의 음성 대화를 수신하고, 원격 개인의 바이오메트릭 데이터를 수신하기 위한 무선 트랜시버(50)를 사용하는 수신 기능;

- 바이오메트릭 데이터를 사용해서 음성 대화를 보호하는 보호 기능;

- 메모리(30)의 바이오메트릭 데이터를 사용해 보호된 음성 대화(240)를 기록하는 기록 기능을 수행할 수 있다.

대안적으로 또는 추가적으로, 만약 바이오메트릭 측정 수단(80)에 의해 측정된 바이오메트릭 데이터가 보다 이전의 바이오메트릭 데이터에 대응한다면, 하나 이상의 특별한 소프트웨어 애플리케이션은 보다 이전의 바이오메트릭 데이터와 메모리(30)에 저장된 음성 대화(240)로의 액세스를 제공하는 인증 기능을 제공할 수 있다. 이러한 소프트웨어 애플리케이션 중의 하나는 바람직하게 신뢰된 소자인데, 이 소자의 동작은 아래에서 보다 상세히 설명될 것이다. 실행할 수 있는 소프트웨어 애플리케이션으로서 신뢰된 소자를 구현하는 것에 대안적으로, 이 소자는 장치(10)에 병합된 응용 주문형 집적 회로(ASIC)의 형태로 적어도 부분적으로 특정 처리 하드웨어로서 구현될 수 있으며, ASIC는 제3자가 복사하기에 매우 어려운 기능을 제공한다.

장치(10)의 동작이 이제 도 1과 도 2를 참조해서 설명될 것이다. 도 2에서 200으로 표시되는 신뢰된 소자(TRCOM)는 대응하는 암호화된 데이터 콘텐츠(ENCDCON)(230)를 생성하기 위해 랜덤 암호키(RANKY)(220)를 사용하여 데이터 콘텐츠(210)를 처리함으로써, 대화 또는 구두 거래에 대응하는 데이터 콘텐츠(DCON)(210)를 암호화하기 위한 보호 소자로서 사용된다. 후속하여, 암호화된 데이터 콘텐츠(ENCDCON)(230)는 기록 소자에 의해 메모리(30)의 데이터 캐리어(CAR)(250)에 데이터 파일(DFIL)로서 저장된다. 신뢰된 소자(TRCOM)(200)는 대화 또는 구두 거래에 관련된 각 참여자의 하나 이상의 바이오메트릭 키(BIOKY)(260)를 랜덤 키(RANKY)(220)와 연관시키기(ASSOC) 위해 채택된다. 이러한 연관(ASSOC)은 이제 설명될, 제1 또는 제2 절차에 의해 구현될 수 있다.

도 3에서 설명되는 제1 절차(PROC1)에서, 신뢰된 소자(TRCOM)(200)는 하나 이상의 바이오메트릭 키(BIOKY)(260)를 안전하게 수신한다. 소자(TRCOM)(200)는 대응하는 암호화된 랜덤 키(ENCKY)(300)를 생성하기 위해 상기 언급된 랜덤 키(RANKY)(220)를 암호화할 수 있는데, 이 암호화는 하나 이상의 바이오메트릭 키(BIOKY)(260)를 이용한다. 또한, 소자(TRCOM)(200)는 하나 이상의 바이오메트릭 키(BIOKY)(260)중의 임의 하나를 가지고 암호화된 랜덤 키(ENCKY)(300)를 해독화하기 위해 인증 소자로서의 역할을 담당할 수 있다. 단지 암호화된 랜덤 키(ENCKY)(300)는 도 1에서 도시된 메모리(MEM)(30)에 궁극적으로 저장된다. 제1 절차(PROC1)는, 암호화된 랜덤 키(ENCKY)(300)가 향상된 보안을 달성하기 위한 "키로커"와 같은 안전한 메모리에서 저장될 필요가 없다는 이점을 가지는데, 즉, 암호화된 랜덤 키(ENCKY)(300)는 여전히 보안을 유지하면서, "키로커" 메모리라고 지정될 필요가 없는 표준 메모리(STNMEM)에서 저장될 수 있다.

도 4에서 설명된 제2 절차(PROC2)에서, 보호 소자로서 작동하는 신뢰된 소자(TRCOM)(200)는 하나 이상의 바이오메트릭 키(BIOKY)(260)를 안전하게 수신하고, 그후 랜덤 키(RANKY)(220)와 함께 키로커(KYLCK)(330)에 안전하게 이 키를 저장한다. 키로커(KYLCK)(330)는 키를 저장하기 위한 안정한 저장소이다. 또한, 신뢰된 소자(TRCOM)(200)는 랜덤 키(RANKY)(220)를 키로커(KYLCK)(330)에 저장된 하나 이상의 바이오메트릭 키(BIOKY)(260)와 또한 연관시킬 수 있다. 만약 소자(TRCOM)(200)가 키로커(KYLCK)(330)에 저장된 랜덤 키(RANKY)(220)에 대응하는 하나 이상의 바이오메트릭 키(BIOKY) 중의 임의의 하나를 키로커(KYLCK)(330)에 제공할 수 있다면, 신뢰된 소자(TRCOM)(200)는 키로커(KYLCK)(330)로부터 예를 들면 랜덤 키(RANKY)(220)와 같은 랜덤 키를 단지 검색하기(RTR) 위해 동작가능하다.

랜덤 키(RANKY)(220)의 복구는 예를 들면, 랜덤 키(RANKY)(260)를 사용해서 파일(DFIL)(240)이 복호화되는 것을 허용함으로써 데이터 파일(DFIL)(240)이 인증되는 것을 가능케한다.

본 발명자는 바이오메트릭 키의 사용은 인증을 달성하기 위한 본 발명의 방법을 구현하기 위해 중요하다는 것을 인식하였다. "바이오메트릭"은 예를 들면:

a) 특징적인 음성상의 세부 사항;

b) 코, 입의 이마의 종횡비와 같은 얼굴의 공간적 특징적 세부 사항;

c) 지문 세부 사항;

d) 홍채 세부 사항;

e) 앞니의 공간적 종횡비와 같은 치과적 세부 사항; 및

f) 귀(귓바퀴)의 공간적 프로파일 세부 사항으로서 이에 국한되지는 않지만 이들 중의 하나 이상과 같은 "일부의 생물학적 특징의 측정값"으로서 해석될 것이다. 음성적 세부 사항의 사용은, 인증된 사용자(100)가 장치(10)를 사용하고 있을 때, 사용자(100)의 음성을 변환하기 위한 마이크(80)와, 대응하는 바이오메트릭 파라미터를 추출하기 위해 필요한 음성 신호 데이터 처리를 수행하고, 이에 따라 바이오메트릭 키(BIOKY)(260)를 유도하기 위한 데이터-처리 유닛(DPU)(20)에서의 처리 용량을 이미 포함하고 있는 장치(10) 때문에 가장 바람직하다. 이롭게, 장치(10)는 바이오메트릭 키(BIOKY)(260)를 생성하기 위한 데이터 처리 유닛(DPU)(20)에 연결된 소형 디지털 카메라를 포함한다. 바이오메트릭 키는, 사용자(100)의 분리 불가능한 부분이고, 따라서 쉽게 복사되거나 손실될 수 없다는 이점을 지닌다. 하지만, 성형 외과의 현재 유행은 바이오메트릭 인증을 잠재적으로 덜 신뢰할만하게 할 수 있는데, 예를 들면, 안면 세부 사항은 안면 리프트(lift), 입술 이식, 코 성형술, 안검 형성술(blepharoplasty) 및/또는 두개골 궤도 뼈 깎기(cranial orbital bond grind)에 의해 수정될 수 있다. 또한, 지문은 흉터 사고(손상), 피부 마모와 피부 이식에 의해 수정될 수 있다. 하지만, 이러한 바이오메트릭를 사용하는 것과 연관된 문제점은 예를 들면, 지문-유도된 키를 홍체-유도된 키와 결합하여 사용함으로써 각 사용자에 대해 하나 이상의 바이오메트릭 키를 사용하는 것에 의해 해소될 수 있다. 각 바이오메트릭 키의 측정은 이러한 복수의 바이오메트릭 키가 사용될때마다 요구되지는 않는데, 그 이유는 키로커는 하나의 바이오메트릭 키의 다른 하나와의 연관을 저장하기 위해 구성될 수 있기 때문이다.

랜덤 키(RANKY)(220)는 하나의 음향 기록으로부터 다른 하나로 바람직하게 동적으로 변경되는데, 그 결과 만약 메모리(30)에 저장된 파일과 관련된 하나의 랜덤 키(RANKY0)(220)가 제3자에 의해 발견된다면, 모든 기록이 위태롭게 되는 것은 아니다. 메모리(30)에 저장될 음향 기록의 임시 시작 순간은 랜덤 키(RANKY)(220)를 생성하기 위해 랜덤 시드(seed)로서 이롭게 사용될 수 있다. 대안적으로, 메모리(MEM)(30)에서 대화를 기록할 때, 가장 근접한 이동전화의 무선 기둥(mast)으로부터 지리적 좌표 기준을 수신하는 장치(10)에 의해 결정되는 장치(10)의 공간적 위치는, 랜덤 키(RANKY)(220)를 생성하기 위해 사용되는 시드로서 또한 사용될 수 있다. 또 하나의 추가 대안으로서, 시간적 및 지리적 입력의 조합은 랜덤 키(RANKY)(220)를 생성하기 위해 사용될 수 있다.

랜덤 키(RANKY)(220)는 실시간에 사용자(100)로부터의 대화를 암호화하기 위해 처리 유닛(DPU)(20)에 의해 바람직하게 적용될 수 있어서, 그 결과 부분적으로 암호화되지 않은 파일이 메모리(MEM)(30)에 부주의하게 기록되지 않는다. 장치(10)를 사용해서 대화를 완성할 때, 장치(10)는 원격 개인과 선택적으로 사용자(100)가 자신의 고유 액세스 키, 예를 들면, 바이오메트릭 키(BIOKY)(260)를 생성하기 위한 목적에서, 원격 개인의 지문, 음성 인증을 위한 원격 개인의 기준 구문의 발성, 또는 원격 개인의 얼굴의 모습을 입력할 것을 요청한다.

원격 개인이 예를 들면, 메모리(MEM)(30)에 거래를 기록한 사용자(100)에게 전화를 걸음으로써 메모리(MEM)(30)에 저장된 기록 중의 하나를 액세스하기를 원하는 상황에서, 원격 개인이 하나 이상의 바이오메트릭 키(BIOKY)(260) 내에 포함된 바이오메트릭 키를 가지고 있다는 전제 하에, 원격 개인은 기록에 잠재적으로 액세스할 수 있다. 원격 개인으로부터의 바이오메트릭 키는 원격 개인으로부터 장치(10)에 암호화된 휴대폰 메시지로서 잠재적으로 전송될 수 있다. 장치(10)는 메모리(MEM)(30) 내에 저장된 사용자(100)의 대화를 액세스하기 위해 다중 원격 개인을 위한 다수의 바이오메트릭 키를 지원하기 위해 배열될 수 있다.

사용자(100)가 장치(10)에 의해 그 메모리(MEM)(30)내에 기록된 보다 이전의 대화를 참조하기를 원할 때, 그 장치의 처리 유닛(DPU)(20)이 예를 들면, 지문 판독을 위해 장치에 손가락을 제시하거나, 처리 유닛(20)이 예를 들면, 시간적 스펙트럼 분석을 통해 분석하도록 동작가능한 특별한 구문을 발성함으로써 사용자에게 바이오메트릭 파라미터의 제공을 상기시키는 방식으로, 장치(10)는 바람직하게 프로그래밍되고, 이에 따라 장치(10)는 그 대화에 대응하는 메모리(MEM)(30)에 저장된 데이터 파일로의 액세스를 사용자(100)에게 허용하는 바이오메트릭 키를 생성하기 위한 바이오메트릭 파라미터를 유도할 수 있다.

도 5는 이동 데이터 매체상에 대화를 기록하기 위한 본 발명에 의해 제안된 방법의 흐름도이다. 연상 기호와 방법 단계는 테이블 1을 참조하여 해석될 것이다.

테이블 1:

단계	연상기호	해석
400	ClIPtThru	호출이 연결된다
410	GetTimLocInfmNet	네트워크로부터 시간/위치 정보를 얻는다
420	GenEncKy1frmTimLocInfm	시간/위치 정보로부터 암호화 키인 키1을 생성한다
430	EncConwthEncKy1	암호화 키인 키1을 가지고 대화를 암호화한다
440	WllConEnd?	대화가 종료될 것인가?
450	SavEncConBdDat	종료된 암호화된 대화 본체 데이터를 메모리(MEM)(30)에 저장한다
460	GetFng/Vce	장치(10)에서 내장된 지문 스캐너를 통해 지문을 얻거나 장치(10) 그 자체를 통해 음성 지문을 얻고, 만약 요구된다면, 원격 화자는 또한 무선 네트워크를 통해 그의 스캐닝된 지문/음성 지문을 전송할 수 있다.
470	HashFngVceGenEncKy2	암호화 키인 키2를 생성하기 위해 지문/음성 지문을 해시(hash)한다.
480	EncKy1wthKy2GenFng/Vce	대응하는 암호화된 키1을 생성하기 위해 키2를 사용하여 키1을 암호화한다
490	StEncKy1inMem	암호화된 키1을 메모리(MEM)(30)에 저장한다.

단계(400)에서, 전화 호출은 장치(10)로부터 통신 네트워크에 연결된다. 그후에, 단계(410)에서, 장치(10)는 랜덤 암호화 키(RANKY)(220)를 생성하기 위한 시드로서 작용하기 위한 호출 시간 정보와 지리적 위치 정보 중의 적어도 하나를 가지고 통신 네트워크로부터 제공된다. 후속하여, 단계(420)에서, 처리 유닛(DPU)(20)는 호출 시간과 위치 정보 중의 적어도 하나로부터 랜덤 키(RANKY)(220), 즉, 키1을 생성한다. 단계(430)에서, 사용자(100)가 통화를 생성하고 실시간에 통화를 암호화시키는 동안, 장치(10)는 통화를 적응시킨다. 그후 단계(440)에서, 장치(10)는 통화가 종료됐는지를 검사한다. 만약 통화가 아직 종료되지 않았다면, 장치(10)는 단계(430)를 계속하여 수행한다. 반대로, 만약 통화가 단계(440)에서 종료되었다고 발견되면, 장치(10)는 단계(450)로 진행하며, 처리 유닛(DPU)(20)은 메모리(MEM)(30)에서 데이터 캐리어(CAR)(250)에 대화의 암호화된 본체를 저장하기 위해 동작한다. 단계(460)에서, 장치(10)는 예를 들면, 장치(10) 내에 포함되고, 처리 유닛(DPU)(20)에 연결된 내장된 지문 스캐너를 통해 유도된 실제 지문의 이미지와 같은 바이오메트릭 지문, 또는, 마이크(80)를 사용해서 획득된 음성 신호의 바이오메트릭 분석 "지문"을 획득한다. 추가적으로, 또는 대안적으로, 장치(10)는 통신 네트워크를 거쳐 원격 화자로부터 하나 이상의 원격 지문을 수신한다. 또한, 단계(470)에서, 지문이 하나 이상의 바이오메트릭 키(BIOKY)(260), 즉 키2를 생성하기 위해 처리된다. 또한, 후속 단계(480)에서, 랜덤 키(RANKY)(220), 즉 키1은 대응하는 암호화된 키(ENCKY)(300)를 생성하기 위해 하나 이상의 바이오메트릭 키(BIOKY)(260)를 이용해 암호화된다. 마지막으로, 단계(490)에서, 장치(10)는 메모리(MEM)(30)에 암호화된 키(ENCKY)(300)를 저장한다. 따라서, 도 5의 흐름도는 상기 언급된 제1 절차(PROC1)를 활용한다.

도 6은 도 3에서 도시된 제1 절차(PROC1)에 따라 메모리(MEM)(30)에 대화를 기록하기 위한 키 계층을 설명한다. 도 6에서 사용된 연상 기호는 테이블 2와 동일한 의미를 가지고 있다.

테이블 2:

단계	연상기호	해석
500	RlTimConDat	실시간 대화 데이터
510	EncConKy1	키1(RANKY)을 가지고 대화를 암호화한다
520	Tim/LocInRnKy	시간/위치 정보/랜덤 키
530	GenEncKy1	암호화 키인 키1(RANKY)을 생성한다
540	EncConDatSc	암호화된 대화 데이터 섹터
550	InptFng/Vce	지문/음성 "지문"을 입력한다
560	Hsh	해시 기능
570	GenKy2forKy1Enc	바이오메트릭 키(BIOKY), 즉 키2를 생성한다
580	EncKy1wthKy2	키2를 가지고 키1을 암호화한다
590	EncKy1inKyLck	(예, 키로커에) 저장된 암호화된 키1

또한, 도 7은 장치(10) 내에 기록된 대화를 검색하는 방법의 흐름도를 도시한다. 도 7에서 이용된 연상 기호는 테이블 3과 동일한 의미를 갖는다.

테이블 3:

단계	연상기호	해석
600	InpFing/Vce	지문/음성 "지문"을 입력한다
610	Hsh	해시 기능
620	GenCanKy2	후보키인 키2를 생성한다
630	DecKy1byKy2forCanKy1	후보 키1을 생성하기 위해 키2(BIOKY)를 사용해서 암호화된 키1(ENCKY)를 복호화한다
640	DecVceDatawthCanKy1	복호화된 데이터를 생성하기 위해 후보 복호화키1을 사용해서 메모리(MEM)(30)내에 저장된 음성 데이터를 디코딩한다
650	CckDecDataPlybyFone	복호화된 데이터가 장치(10)에서 재생될 수 있는 지를 검사한다.
660	Cont	계속한다
670	NoVldUse/stp	유효 사용자가 아니므로, 중단한다

도 7에서, 바이오메트릭 파라미터는 단계(600)에서 측정되고, 그후 단계(620)에서 후보 키2, 즉, 후보 바이오메트릭 키(BIOKY)를 생성하기 위해 단계(610)에서 해시 기능에 의해 처리된다. 후속하여, 단계(630)에서, 처리 유닛(DPU)(20)는 대응하는 후보 키1(후보 RANKY)를 생성하기 위해 암호화된 키1(ENCKY)를 해독하기 위해 후보 키2를 적용하는 것을 시도한다. 그후, 단계(640)에서, 처리 유닛(DPU)(20)은 후보 키1을 사용해서 메모리(MEM)(30)에 저장된 암호화된 음성 데이터를 해독하는 것을 시도한다. 장치(10)는 음성 데이터가 후보 키1을 사용해서 해독화될 수 있는 지를 단계(650)에서 처리 유닛(DPU)(20)에서 검사한다. 데이터의 복호화가 성공적이지 않으면, 장치(10)는 이것을 예를 들면 권한 없는 제3자가 이 데이터로의 액세스를 획득하려고 시도하는 것과 같은, 단계(600)에서 획득된 부정확한 바이오메트릭 데이터라고 해석한다. 이러한 상황에서, 처리 유닛(DPU)(20)은 단계(670)로 진행한다. 반대로, 만약 데이터가 후보 키1을 사용해서 성공적으로 디코딩될 수 있다면, 처리 유닛(DPU)(20)은 요구되는 데이터의 부분이 디코딩될 때까지 단계(640)에서 그 데이터 디코딩 동작을 계속한다.

첨부된 청구항들에서 괄호안의 숫자와 기호는 단지 청구항들의 이해를 돕기 위한 것으로 의도되고, 그 범위에 어떠한 방식으로든 영향을 주는 것으로 의도되지 않는다.

전술된 본원의 실시예들은 첨부된 청구항들에서 한정된 본 발명의 범위를 이탈하지 않고 수정될 수 있다는 것이 인식될 것이다.

"포함하다","병합하다", "존재하다" 및 "가진다"와 같은 동사들과 그 어형 변화들의 사용은 상세한 설명과 그 연관된 청구항들을 해석할 때, 명시적으로 한정되지 않는 다른 항목 또는 소자의 존재를 허용하기 위해 비-배타적인 방식으로 해석되어야 한다. 단수형으로의 참조는 또한 복수 사용으로의 참조로서 해석되어야 하고, 그 반대도 마찬가지이다.

'실행할 수 있는 소프트웨어'는 인터넷 또는 임의의 다른 방식으로 시장에서 팔리는(marketable) 네트워크를 통해 다운로딩할 수 있는 플로피 디스크와 같은 컴퓨터-판독가능한 매체 상에 저장된 임의의 소프트웨어 제품을 의미하는 것으로 이해되어야 한다.

산업상 이용 가능성

본 발명은 검증 가능한 데이터 파일을 생성하기 위한 개인용 통신 장치에 이용 가능하고, 데이터 파일의 인증을 검증하기 위한 개인용 통신 장치에 또한 이용 가능하다.

도면의 간단한 설명

도 1은 본 발명에 따른 개인 통신 장치의 개략도.

도 2는 메모리 디바이스(MEM)에서 데이터 캐리어(CAR)상에 데이터 파일(DFIL)로서 저장하기 위해, 암호화된 데이터(ENCDCON)를 생성하도록 하나 이상의 연관된 바이오메트릭 키(BIOKY)를 구비한 랜덤 키(RANKY)를 이용하는 신뢰된 소자(TRCOM)을 적용함으로써 데이터 콘텐츠(DCON)를 암호화하는 방법과 관련이 있는 흐름도.

도 3은 도 2에서 설명된 방법에서 사용하기 위한 제1 절차를 표시한 도면.

도 4는 도 2에서 설명된 방법에서 사용하기 위한 제2 절차를 도시한 도면.

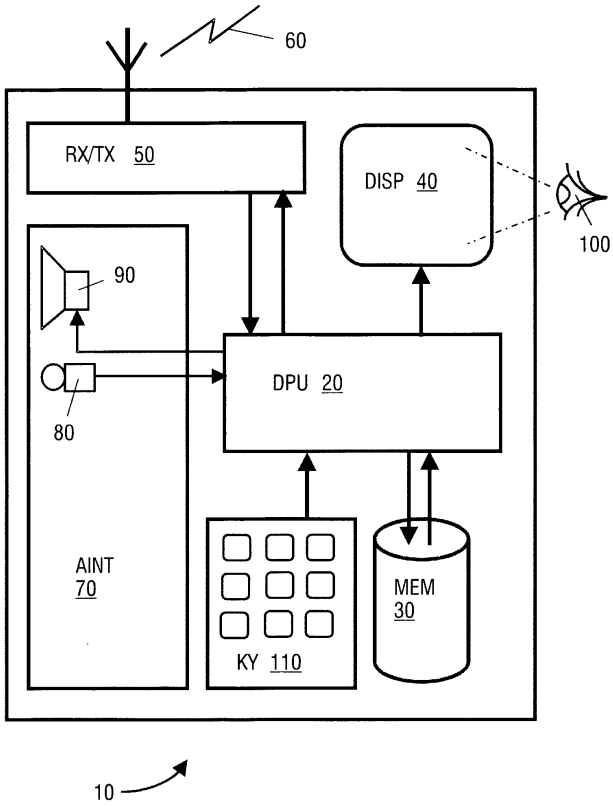
도 5는 도 1의 장치 내에서 대화를 기록하기 위한 단계의 흐름도.

도 6은 도 3에서 그래픽으로 도시된 제1 절차(PROC1)를 이용하는, 도 1의 장치의 메모리내에 대화를 기록 하기 위한 주요 계층을 도시한 도면.

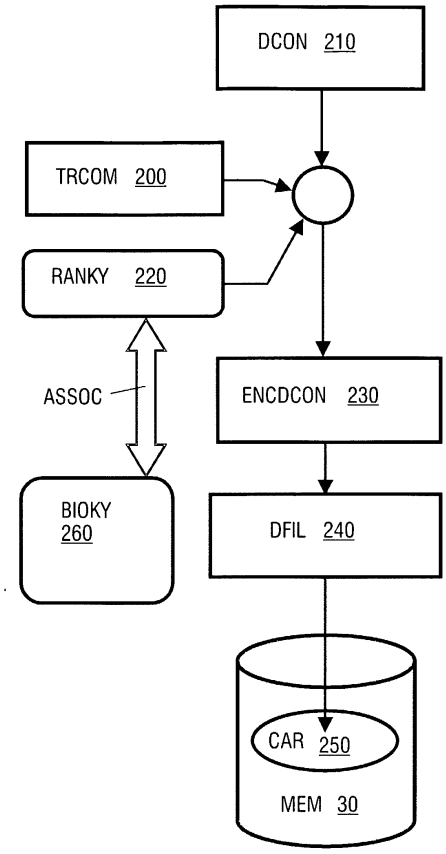
도 7은 도 1의 장치에서 바이오메트릭 파라미터를 사용해서 암호화된 음성 기록을 복호화하기 위해 수행 가능한 단계의 흐름도.

도면

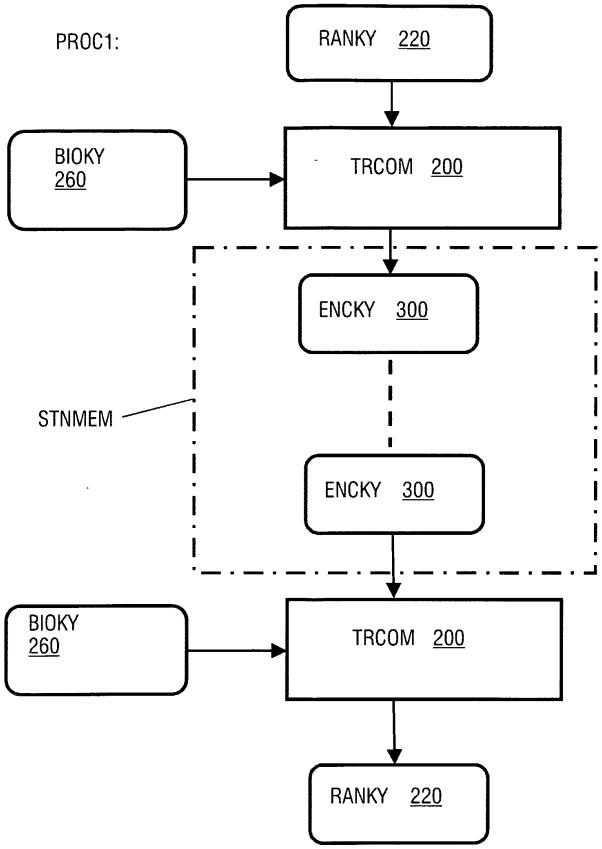
도면1


60
RX/TX 50
DISP 40
100
90
80
DPU 20
AINT
70
KY 110
MEM
30
10

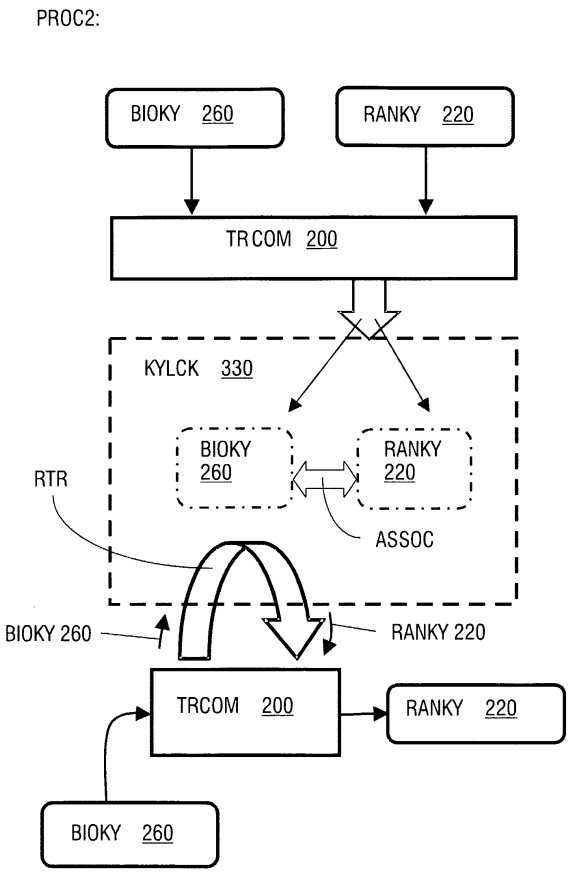
도면2


DCON 210
TRCOM 200
RANKY 220
ASSOC
ENCDCON 230
BIOKY
260
DFIL 240
CAR 250
MEM 30

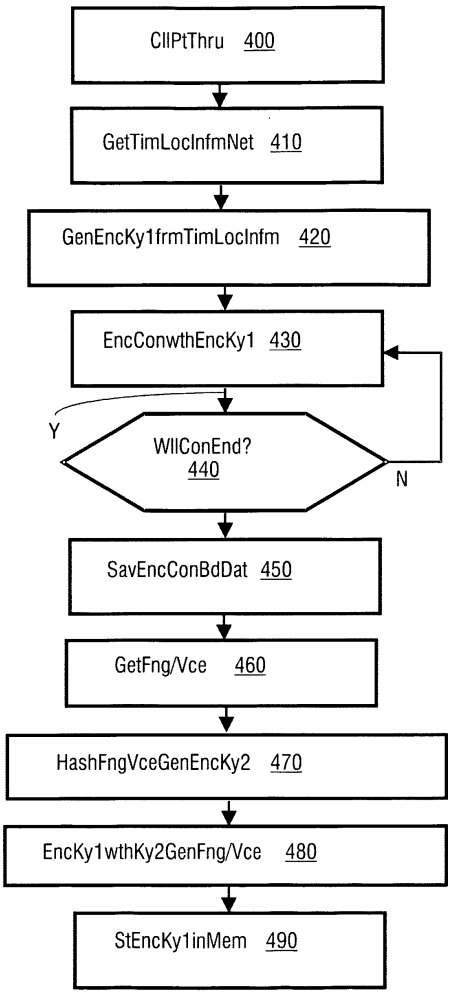
도면3


PROC1:
RANKY 220
BIOKY 260
TRCOM 200
ENCKY 300
STNMEM
ENCKY 300
BIOKY 260
TRCOM 200
RANKY 220

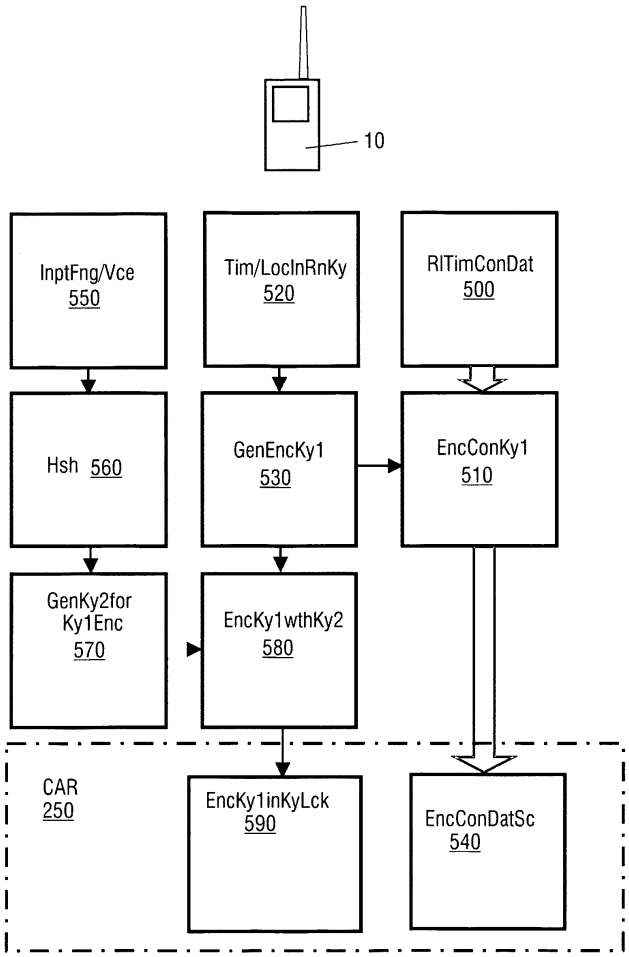
도면4


PROC2:
BIOKY 260
RANKY 220
TRCOM 200
KYLCK 330
BIOKY 260
RANKY 220
RTR
ASSOC
BIOKY 260
RANKY 220
TRCOM 200
RANKY 220
BIOKY 260

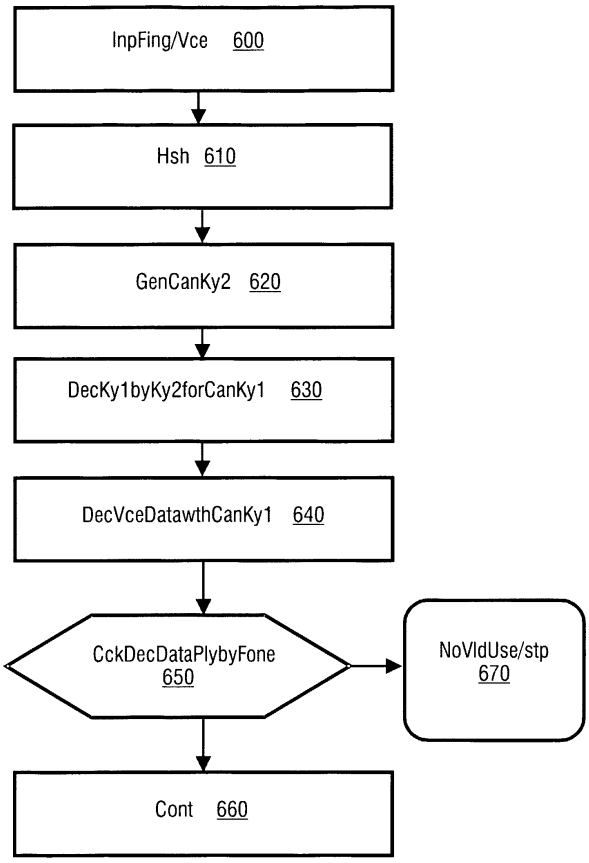
도면5


ClIPtThru 400
GetTimLocInfmNet 410
GenEncKy1frmTimLocInfm 420
EncConwthEncKy1 430
Y
WllConEnd? 440
N
SavEncConBdDat 450
GetFng/Vce 460
HashFngVceGenEncKy2 470
EncKy1wthKy2GenFng/Vce 480
StEncKy1inMem 490

도면6


10
InptFng/Vce
550
Tim/LocInRnKy
520
RlTimConDat
500
Hsh 560
GenEncKy1
530
EncConKy1
510
GenKy2for
Ky1Enc
570
EncKy1wthKy2
580
CAR
250
EncKy1inKyLck
590
EncConDatSc
540

도면7


InpFing/Vce 600
Hsh 610
GenCanKy2 620
DecKy1byKy2forCanKy1 630
DecVceDatawthCanKy1 640
CckDecDataPlybyFone 650
NoVldUse/stp 670
Cont 660