(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년11월18일
(11) 등록번호 10-1677114
(24) 등록일자 2016년11월11일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *G06F 21/62* (2013.01)
H04L 9/00 (2006.01)
(52) CPC특허분류
H04L 9/30 (2013.01)
G06F 21/6245 (2013.01)
(21) 출원번호 10-2015-0121883
(22) 출원일자 2015년08월28일
심사청구일자 2015년08월28일
(56) 선행기술조사문헌
KR101438274 B1*
US20050169520 A1*
KR101475747 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이보영
경기도 의왕시 내손로 13 106동 2103호 (내손동,포일자이아파트)
최원석
서울특별시 강북구 삼양로 256 105동 501호 (미아동,삼성래미안미아1차아파트)
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
(74) 대리인
김등용, 김홍석

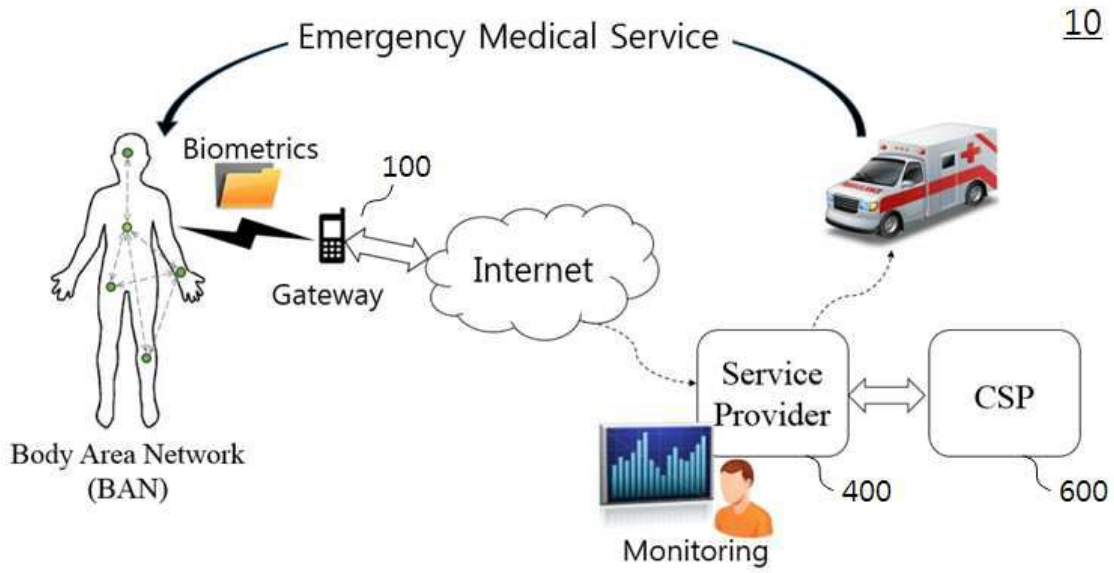
전체 청구항 수 : 총 7 항 심사관 : 전용해

(54) 발명의 명칭 **동형 암호를 이용한 생체정보의 이상치 탐색 방법**

(57) 요 약

동형 암호 성질을 이용한 생체 정보 이상치 탐색 방법이 개시된다. 상기 이상치 탐색 방법은 암호화 서비스 공급자(CSP) 서버가 공개 파라미터 및 마스터키를 생성하는 단계, 상기 암호화 서비스 공급자(CSP) 서버가 상기 공개 파라미터를 사용자 단말기로 전송하는 단계, 상기 사용자 단말기가 상기 공개 파라미터를 이용하여 공개키 및 개인키를 생성하는 단계, 상기 사용자 단말기가 상기 공개키를 이용하여 생체정보 데이터를 암호화하는 단계, 상기 사용자 단말기가 상기 암호화된 생체정보 데이터를 서비스 공급자 서버로 전송하는 단계, 상기 서비스 공급자 서버가 상기 암호화 서비스 공급자(CSP) 서버와의 인터렉션을 통하여 상기 암호화된 생체정보 데이터를 분석하고 이상신호를 검출하기 위한 연산을 수행하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/008 (2013.01)

명 세 서

청구범위

청구항 1

사용자의 생체정보 데이터를 수집하는 사용자 단말기, 암호화 서비스를 제공하는 암호화 서비스 공급자(CSP) 서버, 및 사용자로부터 수신한 암호화된 생체정보 데이터를 분석하여 서비스를 제공하는 서비스 공급자 서버를 포함하는 생체정보 이상치 탐색 시스템이 생체정보 이상치를 탐색하는 방법에 있어서,

암호화 서비스 공급자(CSP) 서버가 공개 파라미터 및 마스터키를 생성하는 단계;

상기 암호화 서비스 공급자(CSP) 서버가 상기 공개 파라미터를 사용자 단말기로 전송하는 단계;

상기 사용자 단말기가 상기 공개 파라미터를 이용하여 공개키 및 개인키를 생성하는 단계;

상기 사용자 단말기가 덧셈 연산이 가능한 동형 암호 기법을 이용하여 상기 공개키로 생체정보 데이터를 암호화하여 암호화된 생체정보 데이터를 생성하는 단계;

상기 사용자 단말기가 상기 암호화된 생체정보 데이터를 서비스 공급자 서버로 전송하는 단계;

상기 서비스 공급자 서버가 상기 암호화 서비스 공급자(CSP) 서버와의 인터렉션을 통하여 상기 암호화된 생체정보 데이터의 이상신호를 검출하기 위한 연산을 수행하는 단계;를 포함하되,

상기 서비스 공급자 서버가 상기 암호화 서비스 공급자(CSP) 서버와의 인터렉션을 통하여 상기 연산을 수행하는 단계는,

상기 서비스 공급자 서버가 덧셈 연산이 가능한 동형 암호 기법을 이용하여 덧셈 연산을 수행하는 과정, 및

상기 암호화 서비스 공급자(CSP) 서버가 상기 서비스 공급자 서버의 요청에 따라 상기 마스터키를 이용하여 뺄셈, 곱셈, 또는 나눗셈 연산을 수행하는 과정을 포함하는,

생체정보 이상치 탐색 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 서비스 공급자 서버가 상기 암호화 서비스 공급자(CSP) 서버와의 인터렉션을 통하여 상기 연산을 수행하는 단계는,

상기 서비스 공급자 서버가 덧셈에 대한 동형 암호 성질을 이용하여 상기 암호화된 생체정보 데이터에 노이즈를 추가하는 과정;

상기 서비스 공급자 서버가 노이즈가 추가된 암호화된 생체정보 데이터를 상기 암호화 서비스 공급자(CSP) 서버로 전송하고 뺄셈, 곱셈, 또는 나눗셈 연산 중 적어도 하나 이상의 연산의 수행을 요청하는 과정;

상기 암호화 서비스 공급자(CSP) 서버가 상기 마스터키를 이용하여 상기 노이즈가 추가된 암호화된 생체정보 데이터를 노이즈가 추가된 상태로 복호화하는 과정;

상기 암호화 서비스 공급자(CSP) 서버가 노이즈가 추가된 상태로 복호화된 생체정보 데이터의 뺄셈, 곱셈, 또는 나눗셈 연산을 수행하여 연산 결과를 생성하는 과정;

상기 암호화 서비스 공급자(CSP) 서버가 상기 공개키를 이용하여 상기 연산 결과를 암호화하여 암호화된 연산

결과를 생성하는 과정;

상기 서비스 공급자 서버가 상기 암호화 서비스 공급자(CSP) 서버로부터 상기 암호화된 연산 결과를 수신하는 과정; 및

상기 서비스 공급자 서버가 상기 연산 결과에서 덧셈에 대한 동형 암호 성질을 이용하여 노이즈를 제거하는 과정;을 포함하는,

생체정보 이상치 탐색 방법.

청구항 5

제1항에 있어서,

상기 서비스 공급자 서버가 상기 암호화된 생체정보 데이터의 이상신호를 검출하기 위한 연산을 수행하는 단계는,

사용자의 생체정보 데이터를 이용하여 마할라노비스 거리를 계산하는 단계; 및

상기 마할라노비스 거리와 이상치 탐지를 위한 임계치와의 비교를 통해 이상치를 탐지하는 단계;를 포함하되,

상기 마할라노비스 거리는 수학식 $MD_i^2 = (X_i - \mu)^T \Sigma^{-1} (X_i - \mu)$ (여기서 μ는 각각의 속성의 평균값들의 행렬을 의미하고, Σ는 사용자의 생체정보 데이터들간의 공분산 행렬을 의미한다)에 의해 산출되는 것을 특징으로 하는,

생체정보 이상치 탐색 방법.

청구항 6

서비스 공급자 서버가 마스터키를 보유한 암호화 서비스 공급자(CSP) 서버와의 인터렉션을 통하여 서비스 사용자의 생체정보 이상신호를 검출하는 방법에 있어서,

상기 서비스 공급자 서버가 사용자 단말기로부터 덧셈연산이 가능한 동형 암호 기법으로 암호화된 생체정보 데이터를 수신하는 단계; 및

상기 서비스 공급자 서버가 상기 암호화된 생체정보 데이터의 이상신호를 검출하기 위한 연산을 수행하는 단계;를 포함하되,

상기 암호화된 생체정보 데이터는 상기 사용자 단말기가 상기 암호화 서비스 공급자(CSP) 서버로부터 수신한 공개 파라미터를 이용하여 생성한 공개키로 암호화된 생체정보 데이터이며,

상기 이상신호를 검출하기 위한 연산을 수행하는 단계는 상기 서비스 공급자 서버가 상기 암호화 서비스 공급자(CSP) 서버와의 인터렉션을 통하여 연산을 수행하는 것을 특징으로 하고,

상기 이상신호를 검출하기 위한 연산을 수행하는 단계는,

상기 서비스 공급자 서버가 덧셈 연산이 가능한 동형 암호 기법을 이용하여 덧셈 연산을 수행하는 과정, 및

상기 서비스 공급자 서버가 뺄셈, 곱셈 또는 나눗셈 연산에 대한 암호화된 연산 결과를 획득하기 위하여, 상기 마스터키를 보유한 상기 암호화 서비스 공급자(CSP) 서버에게 뺄셈, 곱셈, 또는 나눗셈 연산 중 적어도 하나 이상의 연산의 수행을 요청하고, 암호화된 연산 결과를 수신하는 과정을 포함하는,

서비스 공급자 서버의 생체정보 이상신호 검출 방법.

청구항 7

제6항에 있어서,

상기 이상신호를 검출하기 위한 연산을 수행하는 단계는,

상기 서비스 공급자 서버가 덧셈에 대한 동형 암호 성질을 이용하여 상기 암호화된 생체정보 데이터에 노이즈를 추가하고 노이즈가 추가된 암호화된 생체정보 데이터를 생성하는 과정;

상기 서비스 공급자 서버가 상기 노이즈가 추가된 암호화된 생체정보 데이터를 상기 암호화 서비스 공급자(CSP) 서버로 전송하고 뺄셈, 곱셈, 또는 나눗셈 연산 중 적어도 하나 이상의 연산의 수행을 요청하는 과정;

상기 서비스 공급자 서버가 상기 암호화 서비스 공급자(CSP) 서버로부터 상기 암호화된 연산 결과를 수신하는 과정; 및

상기 서비스 공급자 서버가 덧셈에 대한 동형 암호 성질을 이용하여 상기 암호화된 연산 결과에서 노이즈를 제거하는 과정;을 포함하되,

상기 노이즈는 덧셈 연산이 가능한 동형 암호 기법을 이용하여 상기 공개키로 암호화된 노이즈이며,

상기 암호화된 연산 결과는 상기 암호화 서비스 공급자(CSP) 서버가 상기 마스터키를 이용하여 상기 노이즈가 추가된 암호화된 생체정보 데이터를 노이즈가 추가된 상태로 복호화하고, 상기 암호화 서비스 공급자(CSP) 서버가 노이즈가 추가된 상태로 복호화된 생체정보 데이터에 대한 뺄셈, 곱셈, 또는 나눗셈 연산을 수행하여 연산 결과를 생성하고, 상기 암호화 서비스 공급자(CSP) 서버가 상기 공개키로 상기 연산 결과를 암호화하여 생성하는 것을 특징으로 하는,

서비스 공급자 서버의 생체정보 이상신호 검출 방법.

청구항 8

제6항에 있어서,

상기 이상신호를 검출하기 위한 연산을 수행하는 단계는,

사용자의 생체정보 데이터를 이용하여 마할라노비스 거리를 계산하는 단계; 및

상기 마할라노비스 거리와 이상치 탐지를 위한 임계치와의 비교를 통해 이상치를 탐지하는 단계;를 포함하는,

서비스 공급자 서버의 생체정보 이상신호 검출 방법.

청구항 9

마스터키를 보유한 암호화 서비스 공급자(CSP) 서버가 서비스 공급자 서버의 요청에 따른 생체정보의 이상치를 탐색을 위한 연산을 수행하는 방법에 있어서,

상기 서비스 공급자 서버로부터 동형 암호 성질을 이용하여 노이즈가 추가된 암호문을 수신하는 단계;

상기 마스터키를 이용하여 상기 노이즈가 추가된 암호문을 노이즈가 추가된 상태로 복호화하는 단계;

상기 서비스 공급자 서버가 요청한 연산을 수행하고 연산 결과를 생성하는 단계;

사용자 단말기에서 생성된 공개키로 상기 연산 결과를 암호화하여 암호화된 연산 결과를 생성하는 단계;

상기 암호화된 연산 결과를 상기 서비스 공급자 서버로 전송하는 단계;를 포함하되,

상기 노이즈가 추가된 암호문은 상기 서비스 공급자 서버가 상기 사용자 단말기로부터 수신한 암호문에 덧셈 연산이 가능한 동형 암호 성질을 이용하여 노이즈를 추가하여 생성되고,

상기 암호문은 상기 사용자 단말기에서 수집한 생체정보 데이터를 상기 공개키를 이용하여 덧셈 연산이 가능한 동형 암호 기법으로 암호화하여 생성되며,

상기 생체정보의 이상치를 탐색을 위한 연산은 덧셈, 뺄셈, 곱셈, 또는 나눗셈에 대한 연산 중 적어도 하나 이상의 연산을 포함하되, 덧셈에 대한 연산은 덧셈 연산이 가능한 동형 암호 기법을 이용하여 상기 서비스 공급자 서버에 의하여 수행되며, 뺄셈, 곱셈 또는 나눗셈에 대한 연산은 상기 서비스 공급자 서버의 요청에 따라 상기 암호화 서비스 공급자(CSP) 서버가 수행하는,

암호화 서비스 공급자(CSP) 서버의 이상치 탐색을 위한 연산 수행 방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 동형 암호를 이용한 생체 정보의 이상치 탐색 방법에 관한 것으로, 특히 서비스 공급자 서버가 메시지의 암호문에 동형 암호 성질을 이용하여 노이즈를 추가하고 노이즈가 추가된 암호문을 암호화 서비스 공급자(CSP) 서버에 전송하여 연산을 수행할 수 있는 동형 암호를 이용한 생체 정보의 이상치 탐색 방법에 관한 것이다.

배 경 기 술

[0002] 본 특허는 실시간으로 전송되는 생체정보를 통해 응급 상황으로 판단될 때에는 보호자 혹은 구급대원에게 알릴 수 있는 Emergency Medical Service(EMS)서비스 환경을 제시하고 있다. EMS 서비스는 병원 밖에서 환자나 상해를 입은 사람을 돌보는 서비스를 말한다. 고혈압, 심부전증과 같은 질병이 있는 환자 혹은 노인들은 지속적으로 모니터링이 필요 하지만 병원 외의 장소에서는 의료진의 보살핌이 불가능하기 때문에 센서를 이용하여 환자들의 상태를 실시간으로 확인할 수 있는 시스템이 필요하다. EMS는 IoT환경에 맞게 변화할 것이며, 센서를 통해 측정되는 데이터를 의료진이 지속적으로 모니터링하며 응급상황임을 판단했을 때에 환자에게 즉각적으로 의료진을 파견하여 골든타임 내에 조치를 취함으로써 환자의 생존 확률을 높일 수 있다.

[0003] 이때 수집하는 생체정보들은 개인의 의료기록과 동등한 수준으로 관리가 되어야 한다. 미국은 의료정보 보안법(HIPAA; Health Insurance Portability and Accountability Act of 1996)을 통해 건강 정보를 보호하고 있으며, 국내에는 원격 의료와 관련된 법안이 의료법 제 30조의2에서 다루고 있다. 국내 현행 의료법에 의하면 전자의무기록의 경우에는 규정된 시설을 두어야 하고, 이를 관리·보존토록 규정하는 등 전자의무기록에 대해 제약사항을 두어 개인의료 기록을 보호하고 있다.

[0004] 이처럼 국내/외에서 의료법을 통해 사용자의 의료 기록에 대하여 보호하고 있으며 센서를 통해 추출되는 생체정보 역시 상기 의료 기록과 마찬가지로 사용자의 질병 유무, 생활 패턴과 같이 프라이버시와 관련된 정보가 포함되기 때문에 기술적인 보호조치가 필요하다. 다양한 분야에서 서비스 공급자의 권한으로 데이터를 복호화 함으로서 사고들이 빈번히 일어나고 있으며 이러한 정보 유출 사고들은 서비스 공급자에게 많은 권한이 주어지면서 사용자의 데이터를 모두 복호화할 수 있기 때문에 문제가 되고 있다.

[0005] 따라서, 사용자의 보안을 위하여 서비스 공급자는 원본 데이터와 중간 연산 결과에 대하여 알 수 없어야 하며 사용자의 프라이버시를 보존하며 데이터를 분석할 수 있어야 한다.

[0006] 또한, 사용자의 단말기와 같이 전력을 지속적으로 공급하기 힘든 상황에서 사용자와 서비스 공급자가 지속적으로 인터렉션(Interaction)을 하게 되면 배터리의 소모량이 많아지는 문제가 있다. 따라서 사용자는 데이터를 한 번 전송하면 더 이상 연산에 관여하지 않는 환경(Non-Interaction)이 요구된다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 대한민국 등록특허 제10-1475747호

발명의 내용

해결하려는 과제

[0008] 본 발명이 이루고자 하는 기술적인 과제는 서비스 공급자가 사용자로부터 암호화된 생체정보 데이터를 수신하고, 상기 생체정보 데이터에 동형 암호를 이용하여 노이즈를 추가한 암호문을 암호화 서비스 공급자(CSP) 서버에 전송하여, 암호화 서비스 공급자(CSP) 서버와의 인터렉션을 통해 생체정보 이상치 검출을 위한 연산을 수행함으로써, 사용자의 메시지와 연산 결과에 대한 프라이버시를 보장할 수 있는 생체정보 이상치 탐색 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 본 발명의 실시 예에 따른 동형 암호를 이용한 생체 정보의 이상치 탐색 방법은 암호화 서비스 공급자(CSP) 서버가 공개 파라미터 및 마스터키를 생성하는 단계; 상기 암호화 서비스 공급자(CSP) 서버가 상기 공개 파라미터를 사용자 단말기로 전송하는 단계; 상기 사용자 단말기가 상기 공개 파라미터를 이용하여 공개키 및 개인키를

생성하는 단계; 상기 사용자 단말기가 상기 공개키를 이용하여 생체정보 데이터를 암호화하는 단계; 상기 사용자 단말기가 상기 암호화된 생체정보 데이터를 서비스 공급자 서버로 전송하는 단계; 상기 서비스 공급자 서버가 상기 암호화 서비스 공급자(CSP) 서버와의 인터렉션을 통하여 상기 암호화된 생체정보 데이터를 분석하고 이상신호를 검출하기 위한 연산을 수행하는 단계를 포함한다.

발명의 효과

[0010] 본 발명의 실시 예에 따른 동형 암호를 이용한 생체 정보의 이상치 탐색 방법은 사용자의 생체정보를 포함하는 사용자 데이터를 암호화하여 서비스 공급자 서버로 전송하고 상기 서비스 공급자 서버가 암호화 서비스 공급자(CSP) 서버와의 인터렉션을 통하여 연산을 수행하기 때문에 상기 단말기의 연산량을 최소화할 수 있는 효과가 있다.

[0011] 또한, 서비스 공급자 서버 및암호화 서비스 공급자(CSP) 서버에 대하여 상기 사용자들의 입력 값과 연산 결과에 대한 프라이버시를 보호할 수 있는 효과가 있다.

[0012] 또한, 사용자 단말기는 서비스 공급자 서버에 사용자 데이터를 전송 후 서비스 공급자 서버 또는 암호화 서비스 공급자(CSP) 서버의 연산에 관여하지 않으므로 상기 사용자의 단말기와 상기 서버(들)와의 통신량을 감소시킬 수 있는 효과가 있으며, 또한 효율적인 연산을 제공할 수 있는 효과가 있다.

도면의 간단한 설명

[0013] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시예에 따른 동형 암호를 이용한 생체정보의 이상치 탐색 시스템의 개략도이다.

도 2는 도 1에 도시된 사용자 단말기의 기능 블럭도이다.

도 3은 도 1에 도시된 서비스 공급자 서버의 기능 블럭도이다.

도 4는 도 1에 도시된 암호화 서비스 공급자(CSP) 서버의 기능 블럭도이다.

도 5는 도 1에 도시된 동형 암호를 이용한 생체정보의 이상치 탐색 시스템을 이용한 이상치 탐색 방법을 설명하기 위한 흐름도이다.

도 6은 본 발명의 일 실시예에 따른 서비스 공급자 서버가 암호화 서비스 공급자(CSP) 서버와의 인터렉션을 통하여 연산을 수행하는 과정을 도시한다.

도 7은 본 발명의 일 실시예에 따른 서비스 공급자 서버가 노이즈를 제거하는 과정을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0014] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0015] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0016] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0017] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등

도 마찬가지로 해석되어야 한다.

[0018] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0019] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0020] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0021] 우선, 본 발명에서는 덧셈에 대한 동형 성질을 갖는 동형 암호 기법을 이용한다. 예를 들어, 2003년 Bresson, Catalano 및 Pointcheval이 제안한 기법(이하, BCP 암호 기법이라 함)일 수 있다. BCP 암호 기법은 Paillier 암호 기법을 기반으로 설계된 것으로써, 사용자의 개인키를 가지고 복호화하거나 마스터키를 가지고 복호화하는 두 개의 복호화 알고리즘이 있는 점을 특징으로 한다.

[0022] 본 발명이 상기 BCP 암호 기법에 제한되는 것은 아니며, 암호 기법의 이름과는 무관하게 상기 BCP 암호 기법과 동일하거나 유사한 알고리즘을 제공하는 암호 기법을 이용할 수도 있다.

[0023] 이하, 도 1 내지 도 4를 참조하여, 본 발명의 일 실시예에 따라 동형 암호를 이용하여 생체정보의 이상치를 탐색하는 시스템에 대해 상술한다.

[0024] 도 1은 본 발명의 일 실시예에 따른 동형 암호를 이용한 생체정보의 이상치 탐색 시스템(10)을 도시한다. 도 1을 참조하면, 동형 암호를 이용한 생체정보의 이상치 검출 시스템(10)은 사용자 단말기(100), 서비스 공급자 서버(400), 및 암호화 서비스 공급자(CSP) 서버(600)를 포함한다.

[0025] 사용자 단말기는 네트워크 망을 통하여 서비스 공급자 서버(400) 및 CSP 서버(600)와 통신할 수 있다. 일 실시예에 따른 네트워크 망은, 개방형 인터넷, 폐쇄형 인트라넷을 포함한 유선 인터넷망, 이동 통신망과 연동된 무선 인터넷 통신망 뿐만 아니라, 각종 데이터 통신이 가능한 컴퓨터 네트워크 등의 가능한 통신 수단을 포함하는 넓은 개념이다.

[0026] 도 2는 도 1에 도시된 사용자 단말기(100)의 기능 블럭도이다.

[0027] 도 1과 도 2를 참조하면, 사용자 단말기(100)는 키생성 모듈(110), 암호화 모듈(120), 통신 모듈(170), 메모리(180), 및 제어 모듈(190)을 포함한다.

[0028] 본 명세서에서 사용되는 모듈이라 함은 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 모듈은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나 한 종류의 하드웨어를 의미하는 것은 아니다.

[0029] 사용자 단말기(100)는 사용자의 생체정보를 수집하고 네트워크 망을 통하여 전송할 수 있는 기기로, BAN(Body Area Network)를 이루며 신체에 부착되어 있는 센서 또는 사용자 단말기(100)에 연결 또는 포함되어 있는 센서 등을 통해 추출되는 생체정보를 실시간으로 수집한다. 이때, 상기 사용자 단말기(100)는 2 이상의 단말기를 포함할 수도 있다.

[0030] 사용자 단말기(100)의 키생성 모듈(110)은 제어 모듈(190)의 제어 하에, CSP 서버(600)로부터 수신된 공개 파라미터(Public Parameter, PP=(N,k,g))를 이용하여 키생성 알고리즘을 수행한다. 즉, 키생성 모듈(110)는 임의의 a($a \in Z_{N^2}$)를 선택하고 상기 공개 파라미터(PP)를 이용하여 h($h = g^a \bmod N^2$)를 계산함으로써, 공개키($pk \leftarrow h$)와 개인키($sk \leftarrow a$)를 생성한다.

[0031] 암호화 모듈(130)은 제어 모듈(190)의 제어 하에, 암호화 알고리즘을 수행하여 생체정보 데이터

($m \in Z_N$)를 암호화한다. 즉, 암호화 모듈(110)은 상기 공개키(pk)와 CSP 서버(600)로부터 수신한 공개 파라미터(PP)를 이용하여 상기 생체정보 데이터(m)에 대해 임의의 난수($r \in Z_{N^2}$)를 선택하여 암호문(A,B)을 생성한다. 상기 암호문(A,B)는 아래 수식을 이용하여 생성될 수 있다.

[0032]
$$A = g^r$$
$$B = h^r\ (1 + mN)\ mod\ N\text{^}2$$

[0033] 상기 생체정보 데이터는 활동량, 심박 수, 몸무게, 혈압, 혈당 등의 다양한 개인건강정보(PHI: Personal Health Information)일 수 있다.

[0034] 통신 모듈(170)은 제어 모듈(190)의 제어 하에, 개인과 사물에 부착된 센서로부터 수집된 생체정보를 유선 또는 무선 통신망을 통하여 실시간으로 수신할 수 있다.

[0035] 또한, 통신 모듈(170)은 서비스 공급자 서버(400) 또는 CSP 서버(600)와 유선 또는 무선 통신망을 통하여 통신을 수행할 수 있다. 통신 모듈(170)은 CSP 서버(600)로부터 공개 파라미터를 수신할 수 있다. 실시예에 따라, 서비스 공급자 서버(400)로부터 응급상황 알람 및 관련 데이터를 수신할 수 있다.

[0036] 또한, 통신 모듈(170)은 서비스 공급자 서버(400) 또는 CSP 서버(600)로 공개키(pk)를 전송하고, 서비스 공급자 서버(400)로 메시지(m)에 대한 암호문(A,B)을 전송할 수 있다. 실시예에 따라, 상기 공개키(pk)를 제3의 기관으로 전송하고 제3의 기관을 통하여 서비스 공급자 서버(400) 또는 CSP 서버(600)로 전송하는 것도 가능하다.

[0037] 메모리(180)는 프로그램 메모리와 데이터 메모리를 포함할 수 있다. 상기 프로그램 메모리에는 사용자 단말기(100)의 동작을 제어하기 위한 프로그램들이 저장될 수 있다. 상기 데이터 메모리에는 상기 프로그램들을 수행하는 과정 중에 발생되는 데이터들이 저장될 수 있다.

[0038] 제어 모듈(190)은 사용자 단말기(100)의 전반적인 동작을 제어한다. 즉, 키생성 모듈(110), 암호화 모듈(130), 통신 모듈(170), 및 메모리(180)의 동작을 제어할 수 있다.

[0039] 도 3는 도 1에 도시된 서비스 공급자 서버(400)의 기능 블럭도이다. 도 1과 도 3를 참조하면, 서비스 공급자 서버(400)는 연산부(410), 노이즈 추가부(420), 노이즈 제거부(430), 이상치 검출부(440), 통신부(470), 저장부(480), 및 제어부(490)을 포함한다.

[0040] 서비스 공급자 서버(400)는 사용자로부터 수신한 데이터를 분석하여 의미있는 값을 추출한다. 분석 결과를 이용하여 사용자에게 서비스(예를 들어, 응급상황 알림)를 제공한다.

[0041] 서비스 공급자 서버(400)의 연산부(410)는 제어부(490)의 제어 하에, 사용자 단말기(100)로부터 수신한 암호화된 데이터를 이용하여 사용자의 이상신호(예를 들어, 위급상황 등)를 검출하기 위한 연산을 수행한다. 이때, 본 발명에서는 덧셈연산이 가능한 동형암호 성질을 이용한 암호기법을 사용하므로 복호화가 불가능한 서비스 공급자 서버(400)는 덧셈을 제외한 뺄셈, 곱셈, 나눗셈 연산을 수행할 수 없다. 따라서, 덧셈 연산에 대하여는 서비스 공급자 서버(400)에서 수행하고, 나머지 연산에 대하여는 CSP 서버(600)에서 수행한다.

[0042] 구체적으로, 연산부(400)에서 덧셈 연산을 수행하는 방법은 아래와 같다.

[0043] 덧셈에 대한 동형성질을 이용하여, 두 암호문 $(A, B) = (g^r\ mod\ N^2, h^r(1 + mN) mod\ N^2)$ 와 $(A', B') = (g^{r'}\ mod\ N^2, h^{r'}(1 + m'N) mod\ N^2)$ 에 대해 각 항목의 값을 곱하면, 두 암호문의 메시지를 더한 값(m+m')의 암호문을 생성할 수 있다. 덧셈 연산 결과 출력된 암호문은 다음과 같다.

[0044]
$$(\bar{A}, \bar{B}) \leftarrow (A * A', B * B')$$
$$= (g^{r+r'} mod\ N^2, h^{r+r'}(1 + mN)(1 + m'N) mod\ N^2)$$

[0045] 노이즈 추가부(420)는 제어부(490)의 제어 하에, 사용자 단말기(100)로부터 수신된 암호문(A,B)에 노이즈를 추가한다. 이는, 덧셈 이외 기타 연산이 필요한 암호문에 대하여 CSP 서버(600)에 연산을 요청함에 있어서, CSP 서버(600)로부터 사용자의 생체정보 데이터(m)와 연산의 결과에 대한 정보를 보호하기 위함이다.

[0046] 구체적으로, 노이즈 추가부(420)는 암호화 알고리즘을 수행하여 암호문(A,B)의 암호화에 사용된 공개키(key=pk=h)로 임의의 -σ($\sigma \in Z_N$)를 암호화한 암호문($Enc_{key}(-\sigma)$)을 생성한다. 여기서 임의의 -σ는 노이즈 값으로 명명될 수 있다. 서비스 공급자 서버(400)는 두 암호문((A,B), $Enc_{key}(-\sigma)$)에 대해 덧셈에 대한 동형 성질을 이용하여 데이터를 복호화 하지 않고 노이즈가 추가된 암호문(C,D)을 생성한다.

[0047] $$(C,D) \leftarrow Add((A,B), Enc_{key}(-\sigma))$$

[0048] 노이즈 제거부(430)는 제어부(490)의 제어 하에, CPS 서버(600)로부터 수신된 암호문(Z_1,Z_2)에서 동형암호의 성질을 이용하여 노이즈를 제거한다.

[0049] 구체적으로, 뺄셈 연산에서는 노이즈 값 $-\sigma+\sigma'$ 가 추가되어 있으므로, 노이즈 제거부(430)는 상기 노이즈 값을 음수로 설정하여 덧셈 연산을 수행한다.

[0050] $$Add((Z_1,Z_2), Enc_{key}(\sigma+(-\sigma')))$$

[0051] 곱셈 연산은 두 데이터 m, m´에 대하여 각각 노이즈를 포함하여 연산 $(m-\sigma)(m'-\sigma')$을 수행하므로, 실제 데이터 mm'를 얻기 위하여 노이즈 값 $-m\sigma'-m'\sigma+\sigma\sigma'$을 제거한다. 즉, 노이즈 제거부(430)는 상기 노이즈 값을 음수로 설정하여 덧셈 연산을 수행한다.

[0052] $$(T_1,T_2) \leftarrow Enc_{key}(-\sigma\cdot\sigma')$$
$$(Z_1 A^{\sigma'} A'^{\sigma} T_1 \bmod N^2, Z_2 B^{\sigma'} B'^{\sigma} T_2 \bmod N^2)$$

[0053] 나눗셈 연산은 σ를 n으로 나눈 값을 더해주어 노이즈를 제거한다.

[0054] $$Add((Z_1,Z_2), Enc_{key}(\sigma/n))$$

[0055] 통신부(470)는 제어부(490)의 제어 하에, 사용자 단말기(100) 및 CSP 서버(600)와 통신을 수행할 수 있다. 즉, 통신부(470)는 사용자 단말기(100)로부터 공개키(pk) 및 암호문(A,B)를 수신할 수 있다. 실시예에 따라, 공개키(pk)을 제3의 기관 서버를 통하여 수신하는 것도 가능하다.

[0056] 또한, 통신부(470)는 CSP 서버(600)로 노이즈가 추가된 암호문(C,D)을 전송할 수 있으며, CSP 서버(600)로부터 노이즈가 추가된 채 연산한 결과의 암호문(Z_1, Z_2)을 수신할 수 있다.

[0057] 저장부(480)는 프로그램 메모리와 데이터 메모리를 포함할 수 있다. 상기 프로그램 메모리는 서비스 공급자 서버(400)의 동작을 제어하기 위한 프로그램들이 저장될 수 있다. 상기 데이터 메모리에는 상기 프로그램들을 수행하는 과정 중에 발생되는 데이터들이 저장될 수 있다.

[0058] 제어부(490)는 서비스 공급자 서버(400)의 전반적인 동작을 제어한다. 즉, 연산부(410), 노이즈 추가부(420), 노이즈 제거부(430), 이상치 검출부(440), 통신부(470) 및 저장부(480)의 동작을 제어할 수 있다.

[0059] 도 4는 도 1에 도시된 암호화 서비스 공급자(CSP) 서버(600)의 기능 블럭도이다. 도 1과 도 4를 참조하면, CSP 서버(600)는 셋업부(610), 복호화부(620), 연산부(630), 암호화부(640), 통신부(670), 저장부(680), 및 제어부(690)을 포함한다.

[0060] CSP 서버(600)는 서비스 공급자 서버(400)가 데이터를 분석할 때에 그것을 열어볼 수 없도록 제재를 가하는 보안과 관련된 업무를 수행한다. 또한, 서비스 공급자 서버(400)와 함께 연산을 수행한다.

[0061] CSP 서버(600)의 셋업부(610)는 제어부(490)의 제어 하에, 셋업 알고리즘을 이용하여 공개 파라미터(PP)와 마스터키(MK)를 생성한다. 셋업 알고리즘은 안전 소수(safe prime)인 p(p=2p´+1)와 q(q=2q´+1)를 생성한 뒤 상기 p와 상기 q를 곱한 N(N=p·q)을 계산한다. 상기 p´과 상기 q´은 소수(prime number)이다. 또한, 상기 셋업 알고리즘은 보안상수 k($k \in [1, N-1]$)에 대해 $g^{p'q'} \bmod N^2 = 1+kN$를 만족하는 임의의 g($g \in Z^*_{N^2}$)를 선택한다. 이때 메시지 공간은 Z_N이다. 즉, k는 1보다 크거나 같고 N보다 작은 정수 값을

갖는다. 상기 셋업 알고리즘을 이용하여, 셋업부(610)는 공개 파라미터(PP=(N,k,g))와 마스터키(MK=(p´,q´))를 생성한다. 이때, 마스터키는 트랩도어를 위한 키로서 CSP 서버가 보유하며, 사용자의 개인키(sk) 없이도 마스터키를 사용하여 데이터를 복호화할 수 있다.

[0062] 복호화부(620)는 제어부(490)의 제어 하에, 복호화 알고리즘을 수행하여 서비스 공급자 서버(400)로부터 수신된 암호문을 복호화한다. 즉, 공개 파라미터(PP=(N,k,g)), 마스터키(MK=(p´,q´)) 및 공개기(pk)를 이용하여 서비스 공급자 서버(400)로부터 수신된 노이즈가 추가된 암호문을 복호화한다.

[0063] 구체적으로, 복호화 알고리즘은 상기 공개 파라미터 및 상기 마스터키와 상기 암호문(A,B)에 사용된 공개키(pk=h)에 대해 다음 두 식을 계산하여 상기 개인키(sk=a)와 상기 임의의 난수(r)에 대한 정보를 얻는다.

[0064]
$$a \bmod N = \frac{h^{p'q'-1} \bmod N^2}{N} \cdot k^{-1} \bmod N$$
$$r \bmod N = \frac{A^{p'q'-1} \bmod N^2}{N} \cdot k^{-1} \bmod N$$

[0065] 다음, 복호화 알고리즘은 다음의 식을 이용하여 상기 암호문(A,B)을 복호화 하고 메시지(m)을 출력한다.

[0066]
$$m = \frac{(B/g^{ar})^{p'q'-1} \bmod N^2}{N} \cdot (p'q')^{-1} \bmod N$$

[0067] 따라서, 연산부(630)는 암호화되지 않은 연산 결과를 생성할 수 있다. 연산부(630)는 제어부(690)의 제어 하에, 노이즈가 포함된 상태로 복호화된 데이터를 대상으로 연산(예를 들어, 곱셈, 뺄셈, 나눗셈)을 수행한다.

[0068] 암호화부(640)는 제어부(690)의 제어 하에, 암호화 알고리즘을 수행하여 상기 연산 결과를 사용자의 공개키(pk)를 이용하여 암호화하여 암호화된 연산 결과(Z_1, Z_2)를 생성한다. 이때, 암호화 알고리즘은 사용자 단말기(100)의 암호화 모듈(130)의 암호화 알고리즘과 동일하다.

[0069] 통신부(670)는 제어부(690)의 제어 하에, 사용자 단말기(100) 및 서비스 공급자 서버(400)와 통신을 수행할 수 있다. 즉, 통신부(670)는 사용자 단말기(100)로 공개 파라미터(PP)를 전송할 수 있으며, 사용자 단말기(100)로부터 공개키(pk)를 수신할 수 있다. 실시예에 따라, 제3의 기관을 통해 공개키(pk)를 수신할 수도 있다. 또한, 통신부(670)는 서비스 공급자 서버(400)로부터 노이즈가 추가된 암호문(C,D)를 수신할 수 있으며, 연산 결과를 다시 암호화하여 서비스 공급자 서버(400)로 전송할 수 있다.

[0070] 저장부(680)는 프로그램 메모리와 데이터 메모리를 포함할 수 있다. 상기 프로그램 메모리는 CSP 서버(600)의 동작을 제어하기 위한 프로그램들이 저장될 수 있다. 상기 데이터 메모리에는 상기 프로그램들을 수행하는 과정 중에 발생되는 데이터들이 저장될 수 있다.

[0071] 제어부(690)는 CSP 서버(600)의 전반적인 동작을 제어한다. 즉, 셋업부(610), 복호화부(620), 연산부(630), 암호화부(640), 통신부(670) 및 저장부(680)의 동작을 제어할 수 있다.

[0072] 도 5는 도 1에 도시된 동형 암호를 이용한 생체정보의 이상치 탐색 시스템을 이용한 이상치 탐색 방법을 설명하기 위한 흐름도이다. 이하에서는 상술된 내용과 중복되는 내용에 관한 기재는 생략하기로 한다.

[0073] 먼저, CSP 서버(600)는 셋업 알고리즘을 이용하여 공개 파라미터(PP=(N,k,g))와 마스터키(MK=(p´,q´))를 생성한다(S100). CSP 서버(600)는 상기 공개 파라미터(PP)를 통신망을 통하여 사용자 단말기(100)로 전송한다.

[0074] 다음, 사용자 단말기(100)는 CSP 서버(600)로부터 수신된 공개 파라미터(PP=(N,k,g))를 이용하여 키생성 알고리즘을 수행한다(S210). 즉, 사용자 단말기(100)는 상기 공개 파라미터를 이용하여 공개키($pk = h = g^a \bmod N^2$)와 개인키($sk = a \in Z_{N^2}$)를 생성한다.

[0075] 사용자 단말기(100)는 상기 공개키(pk)를 서비스 공급자 서버(400) 및 CSP 서버(600)로 전송할 수 있다.

[0076] 또한, 사용자 단말기(100)는 암호화 알고리즘을 수행하여 생체정보 데이터($m \in Z_N$)를 암호화한다

(S230). 즉, 사용자 단말기(100)는 상기 공개키(pk=h)와 상기 생체정보($m \in Z_N$)에 대해 임의의 난수($r = Z_{N^2}$)를 선택하여 암호문(A,B)을 생성한다.

[0077] $$(A,B) = (g^r \ mod \ N^2, h^r(1+mN) mod \ N^2)$$

[0078] 사용자 단말기(100)는 일정 시간마다 수집되는 생체정보 데이터를 상기 암호문(A,B)으로 암호화하여 서비스 공급자 서버(400)로 전송한다. 이때, 사용자 단말기(100)는 p개의 속성값(예를 들어, 혈압, 심박수 등)을 갖는 데이터셋 $E_{pk}(A_{i1}), E_{pk}(A_{i2}), \ldots, E_{pk}(A_{ip})$으로 묶어 통신망을 통해 서비스 공급자 서버(400)로 전송할 수 있다.

[0079] 서비스 공급자 서버(400)는 사용자 단말기(100)로부터 수신한 암호화된 데이터를 이용하여 사용자의 이상신호(예를 들어, 위급상황 등)를 검출하기 위한 연산을 수행(단계 S300 내지 단계 S600)한다. 이때, 본 발명에서는 덧셈연산이 가능한 동형암호 성질을 이용한 암호기법을 사용하므로 복호화가 불가능한 서비스 공급자 서버(400)는 덧셈을 제외한 뺄셈, 곱셈, 나눗셈 연산을 수행할 수 없다. 따라서, 덧셈 연산에 대하여는 서비스 공급자 서버(400)에서 수행(S300)하고, 나머지 연산에 대하여는 CSP 서버(600)에서 수행(S530)한다. 즉, 마스터키가 있는 CSP 서버(600)와의 인터렉션(interaction)을 통하여 연산을 수행한다.

[0080] 다음, 서비스 공급자 서버(400)와 CSP 서버(600)간 연산을 수행하는 과정을 도 6을 참조하여 상술한다. 도 6은 일 실시예에 따른 서비스 공급자 서버(400)가 CSP 서버(600)를 이용하여 뺄셈, 곱셈, 나눗셈 등의 연산을 수행하는 과정을 도시한다.

[0081] 서비스 공급자 서버(400)는 덧셈에 대한 동형 성질을 이용하여, 사용자 단말기(100)로부터 수신된 암호문(A,B)에 노이즈를 추가한다(S400). 구체적으로 서비스 공급자 서버(400)는 암호문(A,B)의 암호화에 사용된 공개키(key=pk=h)로 임의의 -σ($\sigma \in Z_N$)를 암호화한 암호문($Enc_{key}(-\sigma)$)을 생성하고, 덧셈에 대한 동형 성질을 이용하여 노이즈가 추가된 암호문(C,D)을 생성한다.

[0082]

Add Noise	
(C, D)	$Add((A, B), Enc_{key}(-\sigma))$
(C', D')	$Add((A', B'), Enc_{key}(-\sigma'))$

[0083] 서비스 공급자 서버(400)는 노이즈가 추가된 암호문(C,D)을 CSP 서버(600)로 전송한다. 이때, 서비스 공급자 서버(400)와 CSP 서버(600)는 서로 공모하지 않은 서버로 가정한다. 이는 서비스 공급자 서버(400)와 CSP 서버(600)로부터 사용자의 생체정보 데이터(m)와 연산의 결과에 대한 정보를 보호하기 위함이다.

[0084] 다음, CSP 서버(600)는 복호화 알고리즘을 수행하여 서비스 공급자 서버(400)로부터 수신된 암호문(노이즈가 추가된 암호문)을 복호화한다(S510). 즉, 공개 파라미터(PP)와 마스터키(MK) 및 사용자 단말기(100)로부터 수신한 공개기(pk)를 이용하여 서비스 공급자 서버(400)로부터 수신된 노이즈가 추가된 암호문(C,D)을 복호화하여 메세지 z을 생성한다. 따라서, CSP 서버(600)는 암호화되지 않은 연산 결과를 생성할 수 있다.

[0085]

CSP Decryption	
z	$mDec(C, D)$
z'	$mDec(C', D')$

[0086] CSP 서버(600)는 복호화된 암호문을 대상으로 노이즈가 포함된 상태로 연산(예를 들어, 곱셈, 뺄셈, 나눗셈)을 수행한다(S530).

[0087] 다음, CSP 서버(600)는 연산 결과를 사용자의 공개키(pk)를 이용하여 암호화(S550)하고 암호화된 연산 결과(Z_1,Z_2)를 서비스 공급자 서버(400)로 전송한다.

[0088] 서비스 공급자 서버(400)는 CPS 서버(600)로부터 수신된 암호문(Z_1,Z_2)에서 동형암호의 성질을 이용하여 노이즈를 제거한다(S600, 도 7 참조)).

[0089] 단계 S300의 경우, 이상치 검출 등을 위하여 필요한 연산 과정에 따라, 단계 S400 내지 S600 전 또는 후에 수행할 수 있으며, 단계 S400 내지 S600과 동시에 수행하는 것도 가능하다.

[0090] 서비스 공급자 서버(400)에서 이상치 검출 등을 위하여 필요한 연산이 종료될 때까지 단계 S300 내지 단계 S600을 반복 수행한다.

[0091] 서비스 공급자 서버(400)는 암호화된 생체정보 데이터를 수신하고 상기 연산 결과를 이용하여 이상치를 탐색한다(S700).

[0092] 또한, 서비스 공급자 서버(400)는 상기 이상치 탐색을 통하여 응급상황을 탐지하고 의료기관 또는 사용자 등에 응급상황에 대한 알람을 전송할 수 있다.

[0093] 이하에서는 서비스 공급자 서버(400)에서 암호화된 생체정보 데이터를 이용하여 이상치를 검출하는 과정을 상술한다. 앞서 설명한 암호화 과정 및 암호화 기호는 생략하고 설명하기로 한다.

[0094] 본 발명의 일실시예에 따른 서비스 공급자 서버(400)는 마할라노비스 거리(Mahalanobis Distance, 이하 MD라고 함)를 이용하여 이상치를 탐색하고, 사용자가 현재 응급상황에 처했는지 판단한다.

[0095] 먼저, 서비스 공급자 서버(400)는 사용자의 정상상태에서의 생체정보 데이터를 수신한다. 사용자의 생체정보에 대한 데이터 셋은 다음과 같다.

[0096]
$$X = \begin{array}{c} \\ X_1 \\ X_2 \\ \vdots \\ X_n \end{array} \begin{array}{c} \begin{array}{cccc} A_1 & A_2 & \cdots & A_p \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1p} \\ x_{21} & x_{22} & \cdots & x_{2p} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{np} \end{bmatrix} \end{array}$$

[0097] 이때, 1~n 행은 시계열 단위를 나타내며, 1~p 열은 속성을 나타낸다. 시간 k에서의 데이터 셋은 $X_k = (x_{k1}, x_{k2}, \cdots, x_{kn})$로 나타낼 수 있다. 이렇게 수집된 데이터 셋을 평균 벡터와 공분산 행렬을 통하여 학습할 수 있다.

[0098] 평균 벡터(μ_k)는 시간 k에서의 속성의 평균 데이터로, 속성을 대표하는 값이다. p개의 속성에 대하여 각각 평균값은 1×p의 행렬 $\mu = (\mu_1, \mu_2, \cdots, \mu_p)$로 나타낼 수 있다. 또한, 상기 평균 벡터를 이용하여 p×p의 공분산 행렬을 구한다. 상기 평균 벡터(μ_k) 및 상기 공분산 행렬(Σ)을 구하는 식은 다음과 같다.

[0099]
$$\mu_k = \frac{1}{n}\sum_{i=1}^{n} x_{ik}$$

[0100]
$$\Sigma = \begin{vmatrix} \Sigma_{11} & \Sigma_{12} & \cdots & \Sigma_{1p} \\ \Sigma_{21} & \Sigma_{22} & \cdots & \Sigma_{2p} \\ \vdots & \vdots & & \vdots \\ \Sigma_{p1} & \Sigma_{p1} & \cdots & \Sigma_{pp} \end{vmatrix}$$

[0101]
$$\Sigma_{ij} = \frac{1}{n-1}\sum_{k=1}^{n} (x_{ki} - \mu_i)(x_{kj} - \mu_j)$$
,

[0102] 새롭게 수신되는 생체정보 데이터 셋(X_i)에 대하여 상기 평균 벡터와 상기 공분산 행렬을 연산하여 마할라노비스 거리(MD_i) 값을 생성한다.

[0103] $$MD_i^2 = (X_i - \mu)^T \Sigma^{-1} (X_i - \mu)$$

[0104] 다음, 마할라노비스 거리와 이상치 임계치를 비교하여 이상치를 탐지한다. 상기 이상치 임계치는 사용자 또는 서비스 공급자에 의하여 미리 설정될 수 있다. 이때, 응급 상황의 단계(예를 들어, 관심 단계, 주의 단계, 경계 단계, 심각 단계 등) 각각에 대하여 복수 개의 이상치 임계치를 설정하는 것도 가능하다.

[0105] 상기 연산 결과 이상치가 탐지된 경우, 서비스 공급자 서버는 의료기관 및 사용자가 미리 설정한 기관 또는 개인 등에 응급상황에 대한 알람을 전송할 수 있다.

[0106] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0107] 10 : 생체정보 이상치 검출 시스템

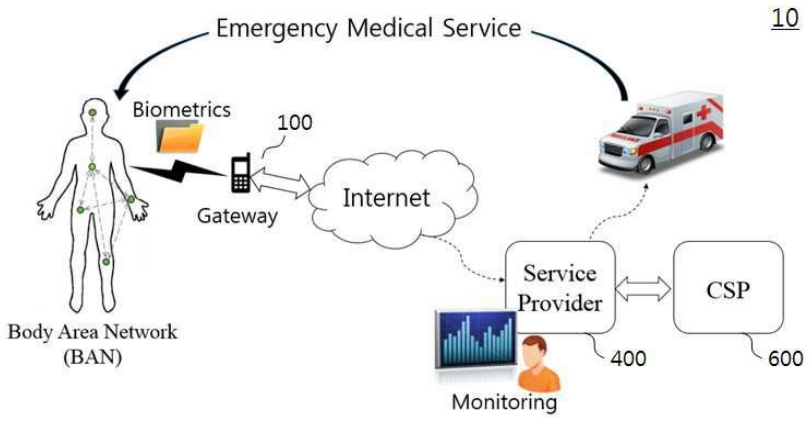
100 : 사용자 단말기

400 : 서비스 제공자 서버

600 : CSP 서버

도면

도면1



도면2

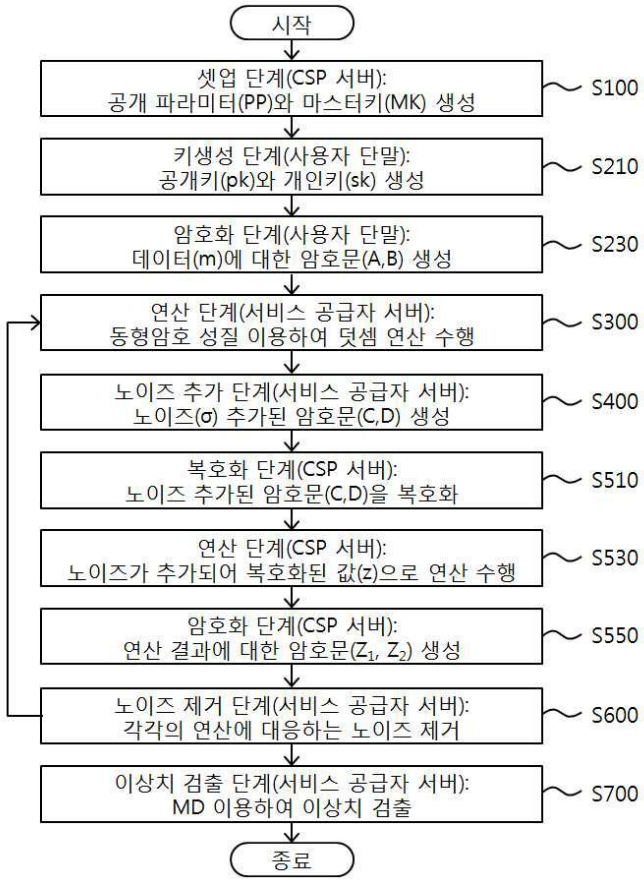
도면3


410
연산부
420
노이즈 추가부
430
노이즈 제거부
440
이상치 검출부
470
통신부
480
저장부
제어부
490
400

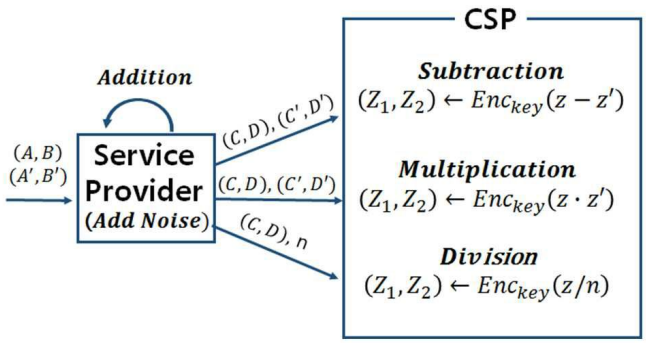
도면4


610
셋업부
620
복호화부
630
연산부
640
암호화부
670
통신부
680
저장부
제어부
690
600

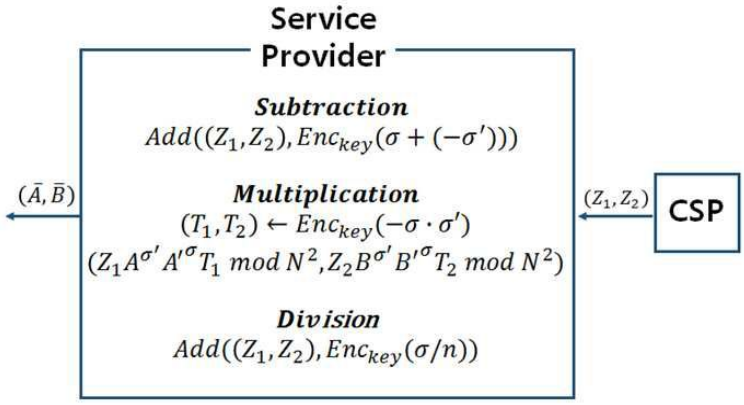
도면5


시작
셋업 단계(CSP 서버):
공개 파라미터(PP)와 마스터키(MK) 생성
S100
키생성 단계(사용자 단말):
공개키(pk)와 개인키(sk) 생성
S210
암호화 단계(사용자 단말):
데이터(m)에 대한 암호문(A,B) 생성
S230
연산 단계(서비스 공급자 서버):
동형암호 성질 이용하여 덧셈 연산 수행
S300
노이즈 추가 단계(서비스 공급자 서버):
노이즈(σ) 추가된 암호문(C,D) 생성
S400
복호화 단계(CSP 서버):
노이즈 추가된 암호문(C,D)을 복호화
S510
연산 단계(CSP 서버):
노이즈가 추가되어 복호화된 값(z)으로 연산 수행
S530
암호화 단계(CSP 서버):
연산 결과에 대한 암호문(Z1, Z2) 생성
S550
노이즈 제거 단계(서비스 공급자 서버):
각각의 연산에 대응하는 노이즈 제거
S600
이상치 검출 단계(서비스 공급자 서버):
MD 이용하여 이상치 검출
S700
종료

도면6


CSP
Addition
(A, B)
(A', B')
Service Provider
(Add Noise)
(C, D), (C', D')
(C, D), (C', D')
(C, D), n
Subtraction
$(Z_1, Z_2) \leftarrow Enc_{key}(z - z')$
Multiplication
$(Z_1, Z_2) \leftarrow Enc_{key}(z \cdot z')$
Division
$(Z_1, Z_2) \leftarrow Enc_{key}(z/n)$

도면7


Service Provider
Subtraction
$Add((Z_1, Z_2), Enc_{key}(\sigma + (-\sigma')))$
Multiplication
$(T_1, T_2) \leftarrow Enc_{key}(-\sigma \cdot \sigma')$
$(Z_1 A^{\sigma'} A'^{\sigma} T_1 \ mod\ N^2, Z_2 B^{\sigma'} B'^{\sigma} T_2 \ mod\ N^2)$
Division
$Add((Z_1, Z_2), Enc_{key}(\sigma/n))$
$(\bar{A}, \bar{B})$
(Z_1, Z_2)
CSP