(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년09월30일
(11) 등록번호 10-1994236
(24) 등록일자 2019년06월24일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 9/14* (2006.01)
(52) CPC특허분류
H04L 9/3073 (2013.01)
H04L 9/14 (2013.01)
(21) 출원번호 10-2017-0051875
(22) 출원일자 2017년04월21일
심사청구일자 2017년12월01일
(65) 공개번호 10-2018-0118478
(43) 공개일자 2018년10월31일
(56) 선행기술조사문헌
Angle-Based Outlier Detection in High-dimensional Data(Hans-Peter Kriegel et al, 2008.08.27.)
KR1020130084669 A
KR1020150070383 A
WO2016088251 A1

(73) 특허권자
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
양대헌
인천광역시 남구 인하로 100 (용현동)
강전일
인천광역시 남구 인하로 100 (용현동)
(뒷면에 계속)
(74) 대리인
팬코리아특허법인

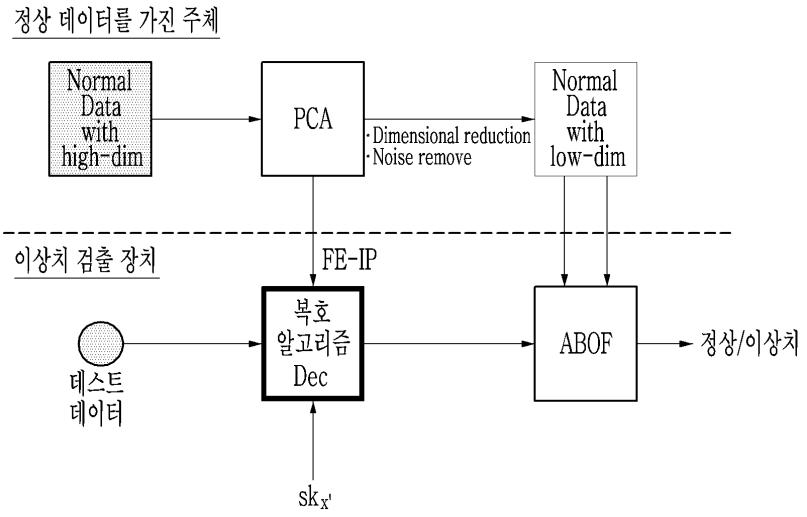
전체 청구항 수 : 총 5 항 심사관 : 장상배

(54) 발명의 명칭 **프라이버시 보존형 각도 기반 이상치 검출 방법 및 장치**

(57) 요 약

고차원의 정상 데이터를 가진 주체가 주성분 분석(principal component analysis)을 통해 상기 정상 데이터로부터 사상행렬과 저차원 데이터에 해당하는 가중 벡터를 생성하고, 상기 사상행렬의 각 행의 값에 대한 암호문을 생성한 후, 상기 암호문과 상기 가중 벡터를 공개한다. 그런 다음, 테스트 데이터에 대한 이상치를 검사하는 장치가 상기 테스트 데이터에 대한 비밀키를 신뢰할 수 있는 주체로부터 수신한 후, 공개된 상기 암호문과 상기 가중 벡터를 이용하여 상기 테스트 데이터에 대한 가중 벡터를 계산하며, 상기 테스트 데이터의 가중 벡터와 상기 공개된 가중 벡터를 이용하여 각도 기반 이상치 정도(Angle-Based Outlier Factor, ABOF)의 값을 계산하여 상기 테스트 데이터가 이상치인지 판단한다.

대 표 도 - 도2



(72) 발명자

장룡호

인천광역시 남구 인하로 100 (용현동)

김선진

대전광역시 유성구 왕가봉로 23, 1101동 602호 (노은동, 열매마을아파트 11단지)

김영민

대전광역시 유성구 전민로30번길 15, 101호 (전민동, 아이캐슬)

박홍규

대전광역시 서구 월평새뜸로4번길 53, 302호 (월평동, 채움빌라)

표철식

대전광역시 서구 청사로 148, 1914호 (둔산동, 매그놀리아)

이 발명을 지원한 국가연구개발사업

과제고유번호	CRC-15-05-ETRI
부처명	미래창조과학부
연구관리전문기관	국가과학기술연구회
연구사업명	융합연구사업
연구과제명	자가학습형 지식융합 슈퍼브레인 핵심기술개발
기 여 율	1/1
주관기관	한국전자통신연구원
연구기간	2015.12.01~2016.11.30

명 세 서

청구범위

청구항 1

프라이버시 보존형 각도 기반 이상치 검출 방법으로서,

고차원의 정상 데이터를 가진 주체가, 상기 정상 데이터로부터 사상행렬과 저차원 데이터에 해당하는 가중 벡터를 생성하고, 상기 사상행렬의 각 행의 값에 대한 암호문을 생성한 후, 상기 암호문과 상기 가중 벡터를 공개하는 단계,

테스트 데이터에 대한 이상치를 검사하는 장치가, 신뢰할 수 있는 주체로부터 상기 테스트 데이터에 대한 비밀키를 수신하는 단계,

상기 장치가, 공개된 상기 암호문과 상기 가중 벡터를 이용하여 상기 테스트 데이터에 대한 가중 벡터를 계산하는 단계, 그리고

상기 장치가, 상기 테스트 데이터의 가중 벡터와 상기 공개된 가중 벡터를 이용하여 상기 테스트 데이터가 이상치인지 판단하는 단계

를 포함하는 프라이버시 보존형 각도 기반 이상치 검출 방법.

청구항 2

제1항에서,

상기 판단하는 단계는 상기 테스트 데이터의 가중 벡터와 상기 공개된 가중 벡터를 이용하여 각도 기반 이상치 정도(Angle-Based Outlier Factor, ABOF)의 값을 계산하여 상기 테스트 데이터가 이상치인지 확인하는 단계를 포함하는 프라이버시 보존형 각도 기반 이상치 검출 방법.

청구항 3

제1항에서,

상기 신뢰할 수 있는 주체가, 마스터 공개키 및 마스터 비밀키를 생성하고, 상기 마스터 공개키를 공개하는 단계

를 더 포함하고,

상기 암호문과 상기 가중 벡터를 공개하는 단계는 상기 마스터 공개키를 이용하여 상기 사상행렬의 각 행의 값에 대한 암호문을 생성하는 단계를 포함하는 프라이버시 보존형 각도 기반 이상치 검출 방법.

청구항 4

제3항에서,

상기 테스트 데이터에 대한 가중 벡터를 계산하는 단계는

상기 마스터 공개키, 상기 공개된 암호문, 상기 가중 벡터 및 상기 테스트 데이터에 대한 비밀키를 이용하여 내적 함수 암호 기법의 복호 알고리즘을 통해서 상기 테스트 데이터에 대한 가중 벡터를 구하는 단계를 포함하는 프라이버시 보존형 각도 기반 이상치 검출 방법.

청구항 5

제1항에서,

상기 암호문과 상기 가중 벡터를 공개하는 단계는 주성분 분석(principal component analysis)을 통해 상기 정상 데이터로부터 사상행렬과 저차원 데이터에 해당하는 가중 벡터를 생성하는 단계를 포함하는 프라이버시 보존형 각도 기반 이상치 검출 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 프라이버시 보존형 각도 기반 이상치 검출 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 이상치 검출은 데이터 마이닝의 한 기법으로서, 주어진 데이터 내에서 특이한 패턴을 보이거나, 변칙적 혹은 빈도가 적은 객체(데이터)들을 찾아내는 작업이다.

[0003] 기존의 정상 객체와 이상 객체를 판별하는 기법들은 다차원 데이터에 대해서는 잘 동작하지 않는 것으로 알려져 있다. 거리 기반 이상치 검출과 같은 방법은 저차원 형태의 데이터에서는 비교적 잘 동작하나, 차원이 높아질수록 객체간의 거리, 근접도 등의 수치가 객체들간의 상관도를 잘 반영하지 못하는 문제로 인해 고차원(high dimension) 데이터에서는 낮은 성능을 나타낸다.

[0004] 고차원 데이터에서 효과적인 이상치 검출 방법으로, 각도 기반 이상치 검출 기법이 제안되었다.

[0005] 각도 기반 이상치 검출은 한 객체를 중심으로 다른 개체들간의 각도를 통해 이상치를 판별한다. 만약 개체가 군집 내부에 있다면 다른 개체들과의 각도의 변화 정도가 클 것이고, 군집 외부에 있다면 각도의 변화가 작을 것이다. 이러한 특성을 활용하여 각도 기반 이상치 정도(Angle-Based Outlier Factor, ABOF)를 정의하는데, ABOF는 한 개체와 이를 제외한 모든 두 개체 쌍에 대해서 각도를 측정하고, 각도의 변화량을 나타내는 분산에 거리 가중치를 계산한 값으로 정의된다. 어떤 개체들에 대해서 각각의 ABOF의 값을 구해 정렬할 수 있으며, 값이 작을수록 이상치 정도가 높다고 할 수 있다.

[0006] 이러한 각도 기반 이상치 검출 기법에서 정확한 검출을 위해서는 검사를 수행하는 주체가 주어진 값과 기존의 정상 데이터를 모두 알아야만 한다. 그러나 기존의 정상 데이터에 개인 프라이버시를 침해할 수 있는 요소가 들어 있다면, 해당 주체에게 데이터를 바로 알려줄 수 없는 문제점이 있다.

발명의 내용

해결하려는 과제

[0007] 본 발명이 해결하려는 과제는 개인 프라이버시의 침해 없이 각도 기반으로 데이터의 이상치를 효과적으로 검출할 수 있는 프라이버시 보존형 각도 기반 이상치 검출 방법 및 장치를 제공하는 것이다.

과제의 해결 수단

[0008] 본 발명의 한 실시 예에 따르면, 프라이버시 보존형 각도 기반 이상치 검출 방법이 제공된다. 프라이버시 보존형 각도 기반 이상치 검출 방법은 고차원의 정상 데이터를 가진 주체가, 주성분 분석(principal component analysis)을 통해 상기 정상 데이터로부터 사상행렬과 저차원 데이터에 해당하는 가중 벡터를 생성하고, 상기 사상행렬의 각 행의 값에 대한 암호문을 생성한 후, 상기 암호문과 상기 가중 벡터를 공개하는 단계, 테스트 데이터에 대한 이상치를 검사하는 장치가, 상기 테스트 데이터에 대한 비밀키를 신뢰할 수 있는 주체로부터 수신하는 단계, 상기 장치가, 공개된 상기 암호문과 상기 가중 벡터를 이용하여 상기 테스트 데이터에 대한 가중 벡터를 계산하는 단계, 그리고 상기 장치가, 상기 테스트 데이터의 가중 벡터와 상기 공개된 가중 벡터를 이용하여 각도 기반 이상치 정도(Angle-Based Outlier Factor, ABOF)의 값을 계산하여 상기 테스트 데이터가 이상치인지 판단하는 단계를 포함한다.

발명의 효과

[0009] 본 발명의 실시 예에 의하면, 각도 기반으로 이상치를 검출하기 위해 정상 데이터를 노출시켜야만 했던 기존 방법과 다르게 정상 데이터를 노출시키지 않으면서도 고차원 데이터에서 효과적으로 이상치를 검출할 수 있다.

도면의 간단한 설명

[0010] 도 1은 본 발명의 실시 예에서 적용되는 FE-IP을 개략적으로 설명하기 위한 도면이다.

도 2는 본 발명의 실시 예에 따른 프라이버시 보존형 각도 기반 이상치 검출 방법을 개략적으로 나타낸 도면이

다.

도 3은 발명의 실시 예에 따른 프라이버시 보존형 각도 기반 이상치 검출 방법을 설명한 흐름도이다.

도 4는 본 발명의 실시 예에 따른 프라이버시 보존형 각도 기반 이상치 검출 장치를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0011] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시 예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0012] 명세서 및 청구범위 전체에서, 어떤 부분이 어떤 구성 요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다.

[0013] 이제 본 발명의 실시 예에 따른 프라이버시 보존형 각도 기반 이상치 검출 방법 및 장치에 대하여 도면을 참고로 하여 상세하게 설명한다.

[0014] 본 발명의 실시 예에서는 보존형 각도 기반 이상치 검출을 위해 내적 함수 암호(Functional Encryption inner product, FE-IP) 기법을 사용한다. 먼저, FE 기법과 FE-IP 기법에 대해 설명한다.

[0015] FE는 임의의 데이터의 암호문 사이의 사칙연산이 가능하게 하는 동형 암호화(homomorphic encryption)와 다르게 원하는 함수를 적용한 값을 얻을 수 있도록 하는 암호 기법이다. 함수 암호화 FE는 수학식 1과 같이 4개의 알고리즘으로 구성된다.

수학식 1

[0016]
$$\mathrm{Setup}(1^{\lambda}) \rightarrow (mpk, msk)$$
$$\mathrm{KeyDer}(\mathrm{msk}, \mathrm{k}) \rightarrow (sk_k)$$
$$\mathrm{Enc}(\mathrm{mpk}, \mathrm{x}) \rightarrow c$$
$$\mathrm{Dec}(\mathrm{mpk}, sk_k, k, c) \rightarrow F(k, x)$$

[0017] 셋업 알고리즘 setup은 보안 파라미터 1^{λ}를 입력으로 사용하여 마스터 비밀키 msk와 마스터 공개키 mpk를 생성한다.

[0018] 비밀키 생성 알고리즘 KeyDer은 마스터 비밀키 msk와 주어진 함수키 k를 입력으로 사용하여 k에 대한 비밀키 sk_k를 생성한다.

[0019] 암호 알고리즘 Enc는 마스터 공개키 mpk와 평문(plaintext) x를 입력으로 사용하여 x에 대한 암호문(ciphertext) c를 생성한다. 즉 마스터 공개키 mpk를 알면 누구라도 x에 대한 암호문 c를 생성할 수 있다.

[0020] 다음, 복호 알고리즘 Dec는 마스터 공개키 mpk, 함수키 k, 비밀키 sk_k와 x에 대한 암호문 c를 입력으로 하여, 함수 F(k,x)의 출력 값을 계산할 수 있다.

[0021] 이러한 FE 기법을 이용한 FE-IP 기법은 도 1을 참고로 하여 설명한다.

[0022] 도 1은 본 발명의 실시 예에서 적용되는 FE-IP을 개략적으로 설명하기 위한 도면이다.

[0023] 도 1을 참고하면, 신뢰할 수 있는 주체인 TTP(Trust third party)가 셋업 알고리즘 setup을 통해서 마스터 비밀키 msk와 마스터 공개키 mpk를 생성한다. TTP는 벡터 u를 가진 A와 벡터 x를 가진 B에게 마스터 공개키 mpk를 공개한다(S10, S20).

[0024] 다음, A가 TTP에게 벡터 u를 전달하면(S30), TTP는 마스터 비밀키 msk와 벡터 u를 입력으로 사용하여 비밀키 생성 알고리즘 KeyDer을 통해서 벡터 u에 대한 비밀키 sk_u를 생성하고, 비밀키 sk_u를 A에게 전달한다(S40).

[0025] B는 마스터 공개키 mpk와 벡터 x를 입력으로 사용하여 암호 알고리즘 Enc을 통해서 벡터 x에 대한 암호문 C를 생성하고, 암호문 C를 A에게 전달한다(S50).

[0026] A는 복호 알고리즘 Dec을 통해서 벡터 u, 벡터 u에 대한 비밀키 sk_u, 그리고 벡터 x에 대한 암호문 C로부터 벡터 u와 벡터 x의 내적을 계산하여 출력한다. 이러한 FE-IP 기법에서는 A가 벡터 u와 벡터 x의 내적을 계산할 수 있지만, 벡터 u와 벡터 x의 내적을 가지고 벡터 x에 대한 정보를 추출할 수는 없다.

[0027] 따라서, 본 발명의 실시 예에서는 이상치 검사를 하는 주체 즉, 프라이버시 보존형 각도 기반 이상치 검출 장치(이하, "이상치 검출 장치"라 함)가 어떤 데이터 값이 주어졌을 때, FE-IP 기법을 사용하여 개인 프라이버시 침해 없이 프라이버시 보호를 위해 원래 데이터 집합(set)의 변형된 값으로도 데이터 값이 이상치인지 검출할 수 있는 방법을 제안한다.

[0028] 도 2는 본 발명의 실시 예에 따른 프라이버시 보존형 각도 기반 이상치 검출 방법을 개략적으로 나타낸 도면이고, 도 3은 발명의 실시 예에 따른 프라이버시 보존형 각도 기반 이상치 검출 방법을 설명한 흐름도이다.

[0029] 먼저, TTP가 FE-IP를 위한 마스터 비밀키 msk와 마스터 공개키 mpk를 생성하였다고 가정한다. 마스터 공개키 mpk는 공개된다. 다음과 같은 과정을 통하여 정상 데이터가 노출되지 않고도 이상치 검출이 가능해진다.

[0030] 도 2를 참고하면, 정상 데이터를 가진 주체는 고차원의 데이터를 포함하는 정상 데이터(normal data)를 저차원의 데이터로 변환한다. 이러한 변환은 주성분 분석(principal component analysis, PCA)를 이용할 수 있다.

[0031] PCA는 데이터를 한 개의 축으로 사상시켰을 때 그 분산이 가장 커지는 축을 첫 번째 주성분, 두 번째로 커지는 축을 두 번째 주성분으로 놓이도록 새로운 좌표계로 데이터를 선형 변환한다. 이 변환은 첫째 주성분이 가장 큰 분산을 가지고, 이후의 주성분들은 이전의 주성분들과 직교한다는 제약 아래에 가장 큰 분산을 갖고 있다는 식으로 정의되어있다. 중요한 성분들은 공분산 행렬의 고유 벡터이기 때문에 직교하게 된다. 즉, PCA는 가장 큰 분산을 갖는 부분공간(subspace)을 보존하는 최적의 직교 선형 변환(orthogonal linear transformation)이라는 특징을 가지며, 입력된 데이터의 공분산 행렬(covariance matrix)에 대한 고유값 분해(eigen value decomposition, EVD) 또는 이상치 분해(singular value decomposition, SVD)를 통하여 구할 수 있다. 공분산 행렬은 그 크기만큼 고유값과 고유벡터가 존재할 수 있으며, 분해를 통하여 얻어진 고유값(eigenvalue)의 절대치가 높은 고유벡터(eigenvector)를 PC(Principal Component)라고 부른다.

[0032] 주어진 데이터 $\mathrm{X} = [x_1, x_2, \cdots]^T$에 대하여, $x_i \in \mathbb{R}^n$이고, m_x를 평균 벡터라고 하였을 때, 공분산 행렬 C는 $\mathrm{E}[(\mathrm{x} - m_x)(x - m_x)^T \in \mathbb{R}^{n \times n}]$과 같다. 공분산 행렬 C는 EVD를 통하여 수학식 2와 같이 직교행렬(orthogonal matrix) P와 대각행렬 Σ로 분해될 수 있다.

수학식 2

[0033] $$\mathrm{C} = \mathrm{E}[(\mathrm{x} - m_x)(x - m_x)^T = P\Sigma P^T]$$

[0034] 이때, 대각행렬 Σ의 대각 값들은 n개의 고유값을 가지고 있으며, 직교행렬 P는 각각의 고유값에 해당하는 n개의 고유벡터를 열 단위로 가지고 있다. 이때, 고유값이 큰 순서대로 P를 재정렬한 뒤, 사전 정의된 부분공간의 크기 m만큼 선택하면, PCA를 위한 사상행렬(projection matrix) $U \in \mathbb{R}^{n \times m}$를 구할 수 있다. 또한 각각의 입력 벡터 x_i에 대한 가중 벡터(weighted vector) w_i는 수학식 3과 같이 구해질 수 있다.

수학식 3

[0035] $$w_i = U^T x_i$$

[0036] PCA에서의 사상행렬 U는 이와 같은 과정을 거치기 때문에 입력된 데이터에 따라서 다른 기저(basis)를 계산하게 되는 특징을 갖는다. 따라서 가중 벡터 w_i만을 가지고 원래의 입력 벡터 x_i를 계산할 수는 없다. 입력된 데이터가 많으면 많을수록 PCA의 기저는 입력된 데이터가 속한 모집단의 기저를 닮게 된다. 입력 벡터들 사이의 거리 관계는 가중 벡터들 사이의 거리 관계가 유지되는데, 거리 관계는 데이터의 유사도를 의미한다고 볼 수 있다. 이런 성질을 이용하여 기계 학습, 영상 인식, 통계 데이터 분석, 데이터 압축, 노이즈 제거 등에 사용될 수 있다.

[0037] 기계 학습 분야에서는 고차원의 데이터를 저차원의 데이터로 변환하는 도구로써 PCA를 이용하기도 한다. 예를 들어, PCA를 이용하여 3차원 데이터를 2차원 데이터로 변환할 수 있다. 고차원의 데이터는 계산량을 많이 요구하기 때문에, 중요한 정보는 충분히 남지만 계산 능력은 합리적인 수준으로 요구되는 저차원의 데이터를 사용하는 것이 이점이 많다. 따라서 고차원의 데이터를 저차원의 데이터로 변환하는 과정에서 사라지는 데이터는 입력된 데이터에 따라서 노이즈로 볼 수 있으므로, PCA는 노이즈 제거 효과가 있다고도 볼 수 있다. 또한 PCA는 주어진 데이터가 기존에 사상행렬을 생성하기 위해 입력된 학습 데이터와 얼마나 차이가 발생하는지 확인하기 위해서 사용될 수 있다. 즉, 주어진 데이터를 사상행렬로 사상시켜서 얻은 가중 벡터가 주어진 데이터의 가중 벡터와 얼마나 떨어져 있는가 확인함으로써, 그 차이를 확인할 수 있다.

[0038] 본 발명의 실시 예에서는 정상 데이터 $\vec{x} \in \mathbb{R}^n$ 이 존재할 때, PCA를 통하여 차원은 줄어들고 거리 관계가 유지되는 저차원의 데이터 $\vec{w} \in \mathbb{R}^m$ 을 얻을 수 있다. PCA로부터 얻은 사상행렬을 $U \in \mathbb{R}^{m \times n}$ 라고 할 때, 수학식 4의 관계가 성립된다.

수학식 4

[0039] $$\vec{w} = U \cdot \vec{x}$$

[0040] $U = [\overrightarrow{u_1}, \overrightarrow{u_2}, \cdots, \overrightarrow{u_m}]^T$ 로 표현될 수 있고, 따라서 $\vec{w} = [w_1, w_2, \cdots, w_m]^T$ 라고 할 때, 모든 $1 \leq i \leq m$에 대하여 수학식 5가 만족될 수 있다.

수학식 5

[0041] $$w_i = < \overrightarrow{u_i}, \vec{x} >$$

[0042] 즉, m번의 $\overrightarrow{u_i}$ 와 $\vec{x}$ 의 내적을 통하여 $\vec{w}$ 가 구해질 수 있다.

[0043] 정상 데이터를 가진 주체는 PCA를 통하여 입력 벡터 x로부터 저차원 데이터에 해당하는 가중 벡터 w와 사상행렬 U를 구하고, 수학식 6과 같이 FE-IP의 암호 알고리즘 Enc을 통해서 U의 각 행 u_i에 대한 암호문 c_i를 계산할 수 있다.

수학식 6

[0044] $$\mathrm{Enc}(\mathrm{mpk}, \mathrm{u}_i) \rightarrow c_i$$

[0045] 정상 데이터를 가진 주체는 이렇게 얻어진 $\mathrm{C} = (\mathrm{c}_1, \mathrm{c}_2, \cdots, \mathrm{c}_m)$와 $\mathrm{W} = (w_1, w_2, \cdots)$를 공개한다.

[0046] 도 3을 보면, 이상치 검출 장치는 어떠한 값 $\overrightarrow{x'}$가 정상적인 범위에 있는지 이상치인지 확인하기 위하여, 테스트 데이터 $\overrightarrow{x'}$를 TTP에게 전달하고(S310), TTP로부터 $\overrightarrow{x'}$에 대한 비밀키 $sk_{x'}$를 수신한다(S320).

[0047] 이상치 검출 장치는 TTP로부터 $\overrightarrow{x'}$에 대한 비밀키 $sk_{x'}$를 수신하면, 공개된 암호문 집합 C와 가중 벡터 집합 W를 이용하여 테스트 데이터 $\overrightarrow{x'}$의 가중 벡터 $\overrightarrow{\mathrm{w}'}$를 모든 $1 \leq i \leq m$에 대하여 수학식 7과 같이 FE-IP의 복호 알고리즘 Dec을 통해서 반복 계산함으로써 구한다(S330).

수학식 7

[0048] $$\mathrm{w}_i' = Dec(mpk, sk_{x'}, \overrightarrow{x'}, c_i)$$

[0049] 이상치 검출 장치는 계산된 테스트 데이터 $\overrightarrow{x'}$의 가중 벡터 $\overrightarrow{\mathrm{w}'}$와 주어진 가중 벡터 집합 W를 이용하여 각도 기반 이상치 정도(Angle-Based Outlier Factor, ABOF) 기반으로 테스트 데이터 $\overrightarrow{x'}$가 정상인지 이상치인지를 검출한다(S340).

[0050] 이상치 검출 장치는 이러한 과정을 통해 정상 데이터가 노출되지 않고도 암호문 집합 C와 가중 벡터 집합 W를 이용하여 테스트 데이터 $\overrightarrow{x'}$가 이상치인지 검출할 수 있다.

[0051] 도 4는 본 발명의 실시 예에 따른 프라이버시 보존형 각도 기반 이상치 검출 장치를 나타낸 도면이다.

[0052] 도 4를 참고하면, 프라이버시 보존형 각도 기반 이상치 검출 장치(400)는 적어도 하나의 프로세서(410), 메모리(420), 저장 장치(430) 및 입출력(input/output, I/O) 인터페이스(440)를 포함한다.

[0053] 적어도 하나의 프로세서(410)는 중앙 처리 유닛(central processing unit, CPU)이나 기타 칩셋, 마이크로프로세서 등으로 구현될 수 있다.

[0054] 메모리(420)는 동적 랜덤 액세스 메모리(dynamic random access memory, DRAM), 램버스 DRAM(rambus DRAM, RDRAM), 동기식 DRAM(synchronous DRAM, SDRAM), 정적 RAM(static RAM, SRAM) 등의 RAM과 같은 매체로 구현될 수 있다.

[0055] 저장 장치(430)는 하드 디스크 (hard disk), CD-ROM(compact disk read only memory), CD-RW(CD rewritable), DVD-ROM(digital video disk ROM), DVD-RAM, DVD-RW 디스크, 블루레이(blu-ray) 디스크 등의 광학 디스크, 플래시 메모리, 다양한 형태의 RAM과 같은 영구 또는 휘발성 저장 장치로 구현될 수 있다.

[0056] I/O 인터페이스(440)는 프로세서(410) 및/또는 메모리(420)가 저장 장치(430)에 접근할 수 있도록 한다. 또한 I/O 인터페이스(440)는 사용자와 인터페이스를 제공할 수 있다.

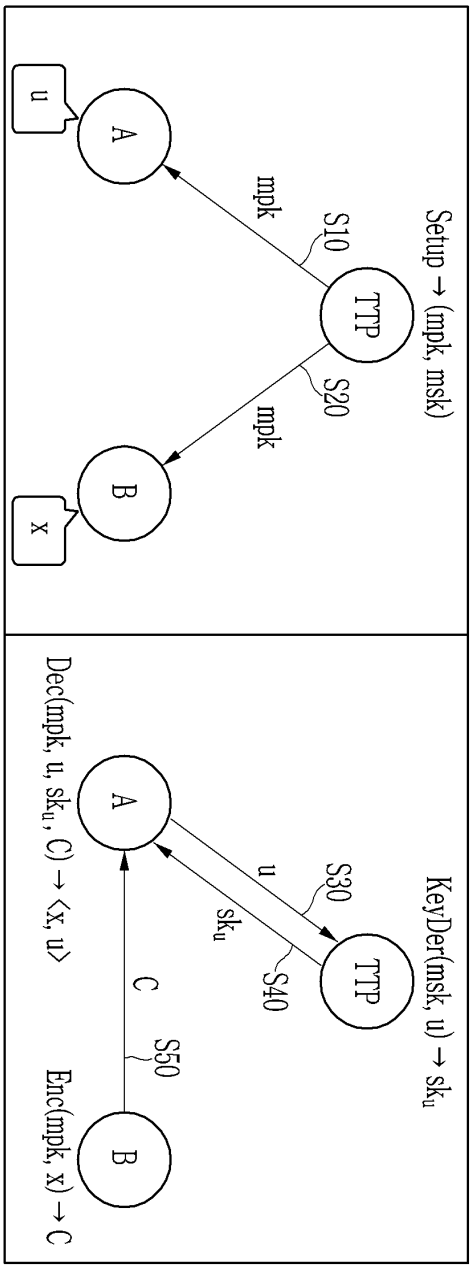
[0057] 프로세서(410)는 도 2 및 도 3에서 설명한 바와 같이 FE-IP 기법을 이용하여 프라이버시 보존형 각도 기반 이상치 검출 기능을 수행할 수 있다. 프로세서(410)는 FE-IP 기법을 이용하여 프라이버시 보존형 각도 기반 이상치 검출 기능을 구현하기 위한 프로그램 명령을 메모리(420)에 로드시켜, 도 2 및 도 3을 참고로 하여 설명한 프라

이버시 보존형 각도 기반 이상치 검출 동작이 수행되도록 제어할 수 있다. 그리고 이러한 프로그램 명령은 저장 장치(430)에 저장되어 있을 수 있으며, 또는 네트워크로 연결되어 있는 다른 시스템에 저장되어 있을 수 있다.

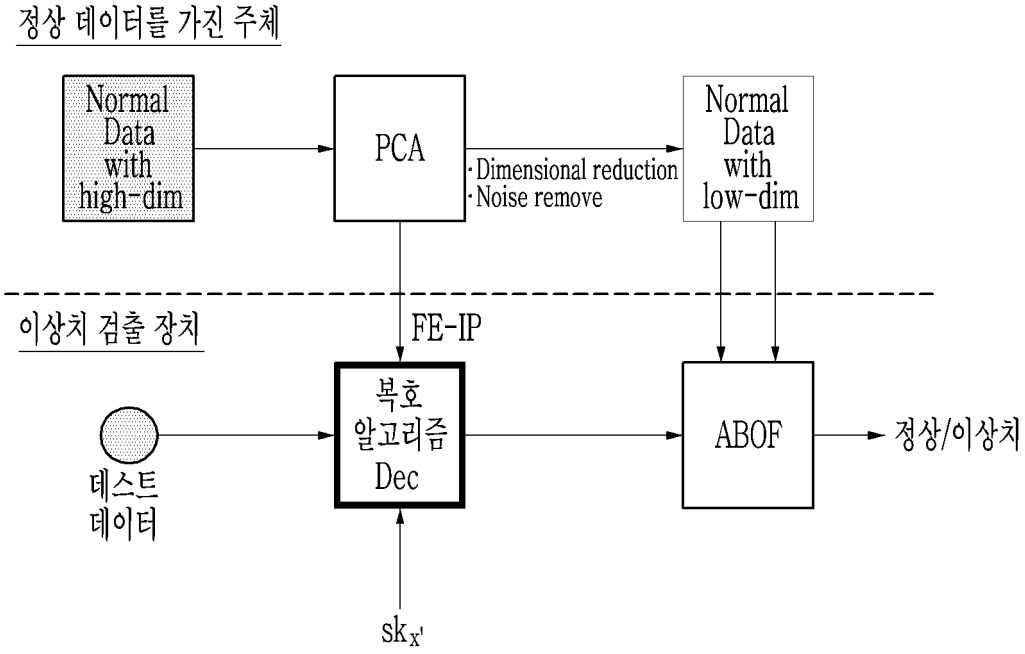
[0058] 이상에서 본 발명의 실시 예에 대하여 상세하게 설명하였지만 본 발명의 권리 범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리 범위에 속하는 것이다.

도면

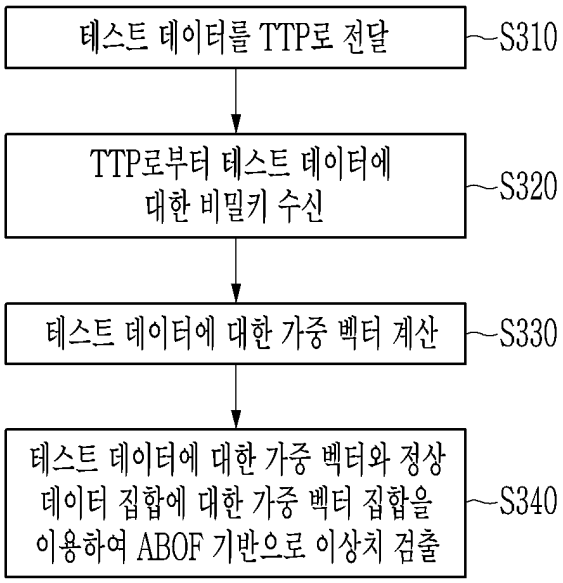
도면1



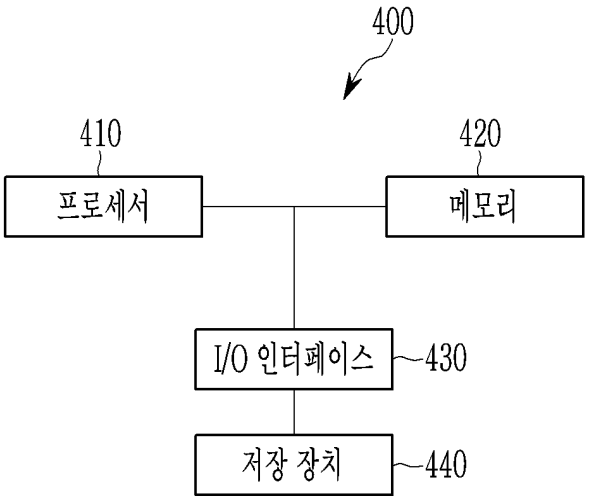
도면2


정상 데이터를 가진 주체
Normal Data with high-dim
PCA
·Dimensional reduction
·Noise remove
Normal Data with low-dim
이상치 검출 장치
FE-IP
복호 알고리즘 Dec
ABOF
정상/이상치
테스트 데이터
$sk_{x'}$

도면3


테스트 데이터를 TTP로 전달
S310
TTP로부터 테스트 데이터에 대한 비밀키 수신
S320
테스트 데이터에 대한 가중 벡터 계산
S330
테스트 데이터에 대한 가중 벡터와 정상 데이터 집합에 대한 가중 벡터 집합을 이용하여 ABOF 기반으로 이상치 검출
S340

도면4



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제3항 제6행

【변경전】

암호문을을 생성하는

【변경후】

암호문을 생성하는