(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0044553
(43) 공개일자 2016년04월25일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 17/18* (2006.01)
G06F 21/60 (2013.01)
(52) CPC특허분류
G06F 21/6245 (2013.01)
G06F 17/18 (2013.01)
(21) 출원번호 10-2016-7007121
(22) 출원일자(국제) 2013년11월21일
심사청구일자 없음
(85) 번역문제출일자 2016년03월17일
(86) 국제출원번호 PCT/US2013/071290
(87) 국제공개번호 WO 2015/026386
국제공개일자 2015년02월26일
(30) 우선권주장
61/867,546 2013년08월19일 미국(US)

(71) 출원인
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 잔 다르크 뤼 1-5
(72) 발명자
파와즈, 나디아
미국 95050 캘리포니아주 산타클라라 벨로미 스트리트 1531
카카키, 압바살리 마흐도미
미국 02143 매사추세츠주 서머빌 에이피티 2 오크 스트리트 35
(74) 대리인
양영준, 전경석, 백만기

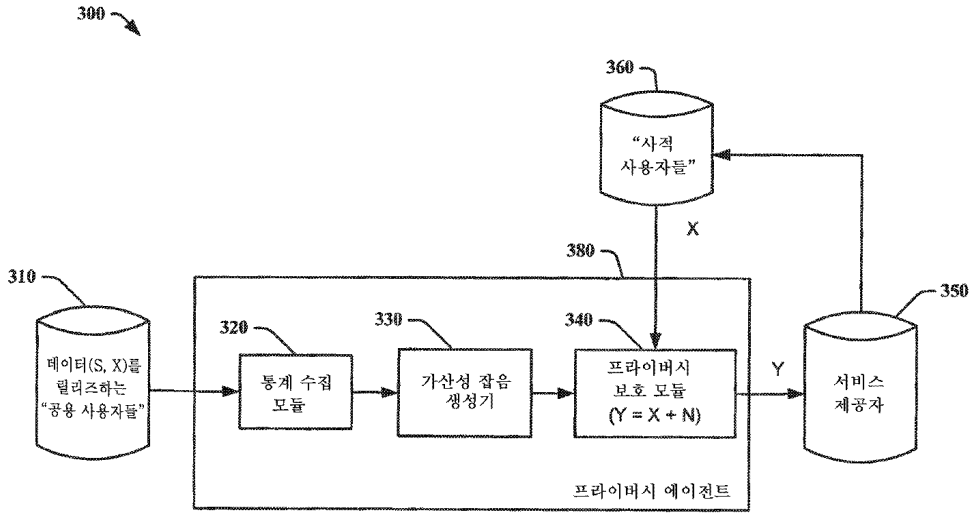
전체 청구항 수 : 총 21 항

(54) 발명의 명칭 **가산성 잡음을 통한 유틸리티-인식 프라이버시 보호 매핑을 위한 방법 및 장치**

(57) 요 약

본 실시예들은 일부 유틸리티를 얻을 희망으로, (S로 표시된) 사적 데이터와 연관되는, (X로 표시된) 일부 공용 데이터를 분석가에게 릴리즈하기를 원하는 사용자가 마주치게 되는 프라이버시-유틸리티 트레이드오프에 초점이 맞추어져 있다. 잡음이 프라이버시 보호 메커니즘, 즉 Y=X+N으로서 추가되는 경우 -Y는 분석가에게 실제로 릴리즈되는 데이터이고 N은 잡음임- , 우리는 가우시안 잡음을 추가하는 것이 연속 데이터 X에 대한 1_2-노름 왜곡 하에서 최적이라는 것을 보여준다. 우리는 가우시안 메커니즘에 의해 최악의 경우의 정보 누설을 최소화하는 가우시안 잡음을 추가하는 메커니즘을 표시한다. 가우시안 메커니즘에 대한 파라미터들은 X의 공분산의 고유벡터들 및 고유값들에 기초하여 결정된다. 우리는 또한 이산 데이터 X에 대한 확률 프라이버시 보호 매핑 메커니즘을 전개하고, 여기서 랜덤 이산 잡음은 최대-엔트로피 분산을 따른다.

대 표 도



(52) CPC특허분류
G06F 21/602 (2013.01)

명 세 서

청구범위

청구항 1

사용자를 위한 사용자 데이터를 처리하기 위한 방법으로서,

사적 데이터와 공용 데이터를 포함하는 상기 사용자 데이터에 액세스하는 단계 -상기 사적 데이터는 제1 데이터 카테고리에 대응하고, 상기 공용 데이터는 제2 데이터 카테고리에 대응함- ;

상기 제1 데이터 카테고리의 공분산 행렬을 결정하는 단계(120);

상기 공분산 행렬에 응답하여 가우시안 잡음을 생성하는 단계(130);

상기 사용자의 공용 데이터에 상기 생성된 가우시안 잡음을 추가함으로써 상기 공용 데이터를 수정하는 단계(140); 및

서비스 제공자와 데이터 수집 에이전시 중 적어도 하나에게 상기 수정된 데이터를 릴리즈(release)하는 단계(150)

를 포함하는 방법.

청구항 2

제1항에 있어서,

상기 공용 데이터는 상기 사용자가 공개적으로 릴리즈될 수 있는 것으로 표시한 데이터를 포함하고, 상기 사적 데이터는 상기 사용자가 공개적으로 릴리즈되지 않도록 표시한 데이터를 포함하는 방법.

청구항 3

제1항에 있어서,

상기 가우시안 잡음을 생성하는 단계는,

상기 공분산 행렬의 고유값들 및 고유벡터들을 결정하는 단계; 및

각각, 상기 결정된 고유값들 및 고유벡터들에 응답하여 또 다른 고유값들 및 고유벡터들을 결정하는 단계

를 포함하고,

상기 가우시안 잡음은 상기 또 다른 고유값들 및 고유벡터들에 응답하여 생성되는 방법.

청구항 4

제1항에 있어서,

상기 결정된 또 다른 고유벡터들은 상기 공분산 행렬의 상기 결정된 고유벡터들과 실질적으로 동일한 방법.

청구항 5

제1항에 있어서,

상기 가우시안 잡음을 생성하는 단계는 왜곡 제약에 추가로 응답하는 방법.

청구항 6

제1항에 있어서,

상기 가우시안 잡음을 생성하는 단계는 상기 제2 데이터 카테고리의 정보와 독립적으로 생성하는 단계를 포함하는 방법.

청구항 7

제1항에 있어서,

상기 릴리즈 데이터에 기초하여 서비스를 수신하는 단계를 더 포함하는 방법.

청구항 8

사용자를 위해 사용자 데이터를 처리하기 위한 방법으로서,

사적 데이터와 공용 데이터를 포함하는 상기 사용자 데이터에 액세스하는 단계;

유틸리티 D에 대한 제약에 액세스하는 단계(220) -상기 유틸리티는 상기 사용자의 상기 공용 데이터 및 릴리즈 데이터에 응답함- ;

상기 유틸리티 제약에 응답하여 랜덤 잡음 Z를 생성하는 단계(230) -상기 랜덤 잡음은 상기 유틸리티 제약 하에서 최대 엔트로피 확률 분포를 따름- ;

상기 사용자에 대한 상기 릴리즈 데이터를 생성하기 위해 상기 사용자의 상기 공용 데이터에 상기 생성된 잡음을 추가하는 단계(140); 및

서비스 제공자와 데이터 수집 에이전시 중 적어도 하나에게 상기 릴리즈 데이터를 릴리즈하는 단계(150)

를 포함하는 방법.

청구항 9

제8항에 있어서,

상기 랜덤 잡음은 분포(distribution) $P[Z=i]=AB^{-|i|^p}$ 를 따르고, A와 B는 $\sum_{i=-\infty}^{\infty} A\,B^{-|i|^p}=1$ 가 되도록 선택되고, p 는 정수인 방법.

청구항 10

제9항에 있어서, $\mathbb{E}[|Z|^p]^{\frac{1}{p}}=D$ 인 방법.

청구항 11

사용자를 위해 사용자 데이터를 처리하기 위한 장치로서,

사적 데이터와 공용 데이터를 포함하는, 상기 사용자 데이터의 제1 데이터 카테고리의 공분산 행렬을 결정하도록 구성된 통계 수집 모듈(320) -상기 사적 데이터는 상기 제1 데이터 카테고리에 대응하고, 상기 공용 데이터는 제2 데이터 카테고리에 대응함- ;

상기 공분산 행렬에 응답하여 가우시안 잡음을 생성하도록 구성된 가산성 잡음 생성기(330); 및

상기 사용자의 상기 공용 데이터에 상기 생성된 가우시안 잡음을 추가함으로써 상기 공용 데이터를 수정하고, 및

서비스 제공자와 데이터 수집 에이전시 중 적어도 하나에게 상기 수정된 데이터를 릴리즈하도록 구성된 프라이버시 보호 모듈(340)

을 포함하는 장치.

청구항 12

제11항에 있어서,

상기 공용 데이터는 상기 사용자가 공개적으로 릴리즈될 수 있는 것으로 표시한 데이터를 포함하고, 상기 사적 데이터는 상기 사용자가 공개적으로 릴리즈되지 않도록 표시한 데이터를 포함하는 장치.

청구항 13

제11항에 있어서,

상기 가산성 잡음 생성기(330)는,

상기 공분산 행렬의 고유값들 및 고유벡터들을 결정하고,

각각, 상기 결정된 고유값들 및 고유벡터들에 응답하여 또 다른 고유값들 및 고유벡터들을 결정하도록 구성되고, 상기 가우시안 잡음은 상기 또 다른 고유값들 및 고유벡터들에 응답하여 생성되는 장치.

청구항 14

제11항에 있어서,

상기 결정된 또 다른 고유벡터들은 상기 공분산 행렬의 상기 결정된 고유벡터들과 실질적으로 동일한 장치.

청구항 15

제11항에 있어서,

상기 가산성 잡음 생성기는 왜곡 제약에 응답하도록 구성되는 장치.

청구항 16

제11항에 있어서,

상기 가산성 잡음 생성기는 상기 제2 데이터 카테고리의 정보와 독립적으로 상기 가우시안 잡음을 생성하는 장치.

청구항 17

제11항에 있어서,

상기 릴리즈 데이터에 기초하여 서비스를 수신하도록 구성된 프로세서를 더 포함하는 장치.

청구항 18

사용자를 위해 사용자 데이터를 처리하기 위한 장치로서,

유틸리티 D에 대한 제약에 액세스하도록 구성된 통계 수집 모듈(320) -상기 유틸리티는 상기 사용자의 공용 데이터 및 릴리즈 데이터에 응답함- ;

상기 유틸리티 제약에 응답하여 랜덤 잡음 Z를 생성하도록 구성된 가산성 잡음 생성기 -상기 랜덤 잡음은 상기 유틸리티 제약 하에서 최대 엔트로피 확률 분포를 따름- ; 및

사적 데이터 및 공용 데이터를 포함하는 상기 사용자 데이터에 액세스하고,

상기 사용자에 대한 릴리즈 데이터를 생성하기 위해 상기 사용자의 상기 공용 데이터에 상기 생성된 잡음을 추가하며, 및

서비스 제공자와 데이터 수집 에이전시 중 적어도 하나에게 상기 릴리즈 데이터를 릴리즈하도록 구성된 프라이버시 보호 모듈(340)

을 포함하는 장치.

청구항 19

제18항에 있어서,

상기 랜덤 잡음은 분포 $P[Z=i]=AB^{-|i|^p}$ 를 따르고, A와 B는 $\sum_{i=-\infty}^{\infty} A\,B^{-|i|^p}=1$ 가 되도록 선택되고, p 는 정수인 장치.

청구항 20

제19항에 있어서, $\mathbb{E}[|Z|^p]^{\frac{1}{p}} = D$ 인 장치.

청구항 21

제1항 내지 제10항에 따라, 사용자를 위해 사용자 데이터를 처리하기 위한 명령어들을 저장하는 컴퓨터 판독가능 저장 매체.

발명의 설명

기 술 분 야

[0001] 관련 출원들에 대한 상호 참조

[0002] 본원은 하기 미국 가출원의 출원일의 이익을 주장하며, 이는 모든 목적을 위해 그 전체가 참조로서 본 명세서에 포함된다: 2013년 8월 19일자로 출원되고, "Method and Apparatus for Utility-Aware Privacy Preserving Mapping through Additive Noise"라는 발명의 명칭의 일련번호 제61/867.546호.

[0003] 본원은 2012년 8월 20일자로 출원되고, "A Framework for Privacy against Statistical Inference"라는 발명의 명칭의 미국 가특허 출원 제61/691,090호(이하 "Fawaz")에 관련된다. 이 가출원은 그 전체가 참조로서 본 명세서에 명시적으로 포함된다.

[0004] 또한, 본원은: (1) "Method and Apparatus for Utility-Aware Privacy Preserving Mapping against Inference Attacks"라는 명칭의 대리인 정리번호 PU130120, 및 (2) "Method and Apparatus for Utility-Aware Privacy Preserving Mapping in View of Collusion and Composition"이라는 명칭의 대리인 정리번호 PU130121에 관련되고, 이들은 함께 양도되고, 그 전체가 참조로서 포함되며, 본 명세서와 함께 제출되었다.

[0005] 본 발명은 프라이버시를 보호하기 위한 방법 및 장치에 관한 것으로, 특히 프라이버시를 보호하기 위해 사용자 데이터에 잡음을 추가하기 위한 방법 및 장치에 관한 것이다.

배 경 기 술

[0006] 빅 데이터(Big Data)의 시대에, 사용자 데이터의 수집 및 마이닝(mining)은 복수의 사설 및 공공 기관에 의한 빠르게 성장하고 일반적인 실무가 되고 있다. 예를 들어, 기술 회사들은 사용자 데이터를 활용하여 그들의 고객들에게 개인맞춤화된 서비스들을 제공하거나, 정부 기관들은 데이터에 의존하여 다양한 과제들, 예로서 국가 보안, 국민 건강, 예산 및 기금 할당을 다루거나, 의료 기관들은 데이터를 분석하여 질병들에 대한 원인들 및 잠재적인 치료법들을 발견한다. 일부 예들에서, 사용자 데이터의 수집, 분석, 또는 제삼자들과의 공유는 사용자의 동의 또는 자각 없이 수행된다. 다른 예들에서, 사용자는 데이터를 특정 분석자에게 자발적으로 릴리즈하여 그에 대한 응답으로 서비스를 획득하는데, 예를 들어 제품 등급들을 릴리즈하여 추천들을 획득한다. 이러한 서비스, 또는 사용자가 사용자 데이터에 대한 액세스의 허용으로부터 얻는 다른 이익은 유틸리티로서 지칭될 수 있다. 어느 경우에나, 수집되는 데이터의 일부는 예를 들어 정치적 견해, 건강 상태, 수입 레벨과 같이 사용자에 의해 민감한 것으로 간주될 수 있거나, 예를 들어 제품 등급들과 같이 언뜻 보아서는 무해한 것으로 보이지만 그와 상관된 더 민감한 데이터의 추론을 유발할 수 있으므로, 프라이버시 위험들이 발생한다. 후자의 위험은 사적 데이터를 공개적으로 릴리즈된 데이터와의 그 상관을 이용하여 추론하는 기술인 추론 공격으로 지칭된다.

발명의 내용

과제의 해결 수단

[0007] 본 원리들은 사용자를 위해 사용자 데이터를 처리하기 위한 방법을 제공하며, 이 방법은 사적 데이터와 공용 데이터를 포함하는 사용자 데이터에 액세스하는 단계 -사적 데이터는 제1 데이터 카테고리에 대응하고, 공용 데이터는 제2 데이터 카테고리에 대응함- ; 제1 데이터 카테고리의 공분산 행렬을 결정하는 단계; 공분산 행렬에 응답하여 가우시안 잡음을 생성하는 단계; 사용자의 공용 데이터에 생성된 가우시안 잡음을 추가함으로써 공용 데이터를 수정하는 단계; 및 후술되는 바와 같이 서비스 제공자와 데이터 수집 에이전시 중 적어도 하나에게 수정

된 데이터를 릴리즈하는 단계를 포함한다. 본 원리들은 또한 이들 단계들을 수행하기 위한 장치를 제공한다.

[0008] 본 원리들은 또한 사용자를 위해 사용자 데이터를 처리하기 위한 방법을 제공하며, 이 방법은 사적 데이터와 공용 데이터를 포함하는 사용자 데이터에 액세스하는 단계; 유틸리티 D에 대한 제약에 액세스하는 단계 -유틸리티는 사용자의 공용 데이터 및 릴리즈 데이터에 응답함- ; 유틸리티 제약에 응답하여 랜덤 잡음 Z를 생성하는 단계 -랜덤 잡음은 유틸리티 제약 하에서 최대 엔트로피 확률 분포를 따름- ; 및 후술되는 바와 같이 사용자에 대한 릴리즈 데이터를 생성하기 위해 사용자의 공용 데이터에 생성된 잡음을 추가하는 단계를 포함한다. 본 원리들은 또한 이들 단계들을 수행하기 위한 장치를 제공한다.

[0009] 또한, 본 원리들은 전술한 방법들에 따라 사용자를 위해 사용자 데이터를 처리하기 위한 명령어들이 저장되는 컴퓨터 판독가능 저장 매체를 제공한다.

도면의 간단한 설명

[0010] 도 1은 본 원리들의 실시예에 따라, 연속적인 데이터에 가우시안 잡음을 추가함으로써 프라이버시를 보호하기 위한 예시적인 방법을 묘사한 흐름도이다.

도 2는 본 원리들의 실시예에 따라, 이산 데이터에 이산 잡음을 추가함으로써 프라이버시를 보호하기 위한 예시적인 방법을 묘사한 흐름도이다.

도 3은 본 원리들의 실시예에 따른, 예시적인 프라이버시 에이전트를 묘사한 블록도이다.

도 4는 본 원리들의 일 실시예에 따른, 다중 프라이버시 에이전트를 갖는 예시적인 시스템을 묘사한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0011] 우리는 Fawaz에서 기술된 설정을 고려하며, 여기서 사용자는 상관되는 2가지 종류의 데이터를 갖는다: 사적으로 남기고 싶은 일부 데이터와, 분석가에게 릴리즈할 의향이 있으며 일부 유틸리티를 파생시킬 수 있는 비-사적 데이터 예를 들어, 서비스 제공자에게의 미디어 선호의 릴리즈(release)는 보다 정확한 콘텐츠 추천들을 접수하기 위한 것이다.

[0012] 본 출원에서 사용되는 바와 같이, 예를 들어, 서비스 제공자의 시스템의 일부일 수 있는, 용어 분석가는 사용자에게 유틸리티를 제공하기 위해 표면상 데이터를 사용하는, 릴리즈 데이터의 수령인을 지칭한다. 분석가는 릴리즈 데이터의 합법적인 수령인이다. 그러나, 분석가는 또한 릴리즈 데이터를 위법으로 이용하고 사용자의 사적 데이터에 관한 일부 정보를 추론할 수 있다. 이것은 프라이버시와 유틸리티 요구 간의 갈등을 만든다. 유틸리티를 유지하는 동안 추론 위협을 감소시키기 위해, 사용자는 유틸리티 제약 하에서 설계된, "프라이버시 보호 매핑(privacy preserving mapping)"이라고 불리는 조건부 확률 매핑(conditional probabilistic mapping)에 따라 생성된, 데이터의 "왜곡된 버전"을 릴리즈할 수 있다.

[0013] 본 출원에서, 우리는 사용자가 "사적 데이터"로서 사적으로 남기고 싶은 데이터, 사용자가 "공용 데이터(public data)"로서 릴리즈할 의향이 있는 데이터, 및 사용자가 실제로 "릴리즈 데이터(released data)"로서 릴리즈한 데이터를 참조한다. 예를 들어, 사용자는 그의 정치적인 견해를 사적으로 유지하기를 원할 수 있고, 그의 TV 순위들을 수정하여 릴리즈할 의향이 있을 수 있다(예를 들어, 사용자의 프로그램의 실제 순위는 4이지만, 그는 순위를 3으로 릴리즈한다). 이 경우에, 사용자의 정치적인 견해는 이 사용자에 대한 사적 데이터인 것으로 간주되고, 텔레비전 순위들은 공용 데이터인 것으로 간주되며, 릴리즈된 수정된 TV 순위들은 릴리즈 데이터인 것으로 간주된다. 또 다른 사용자는 수정 없이 정치적인 견해와 TV 순위들 양쪽 모두를 릴리즈할 의향이 있을 수 있으며, 그에 따라 이 다른 사용자의 경우, 정치적인 견해와 TV 순위들만이 고려될 때, 사적 데이터, 공용 데이터 및 릴리즈 데이터 간에 차이가 없다는 것에 유의해야 한다. 많은 사람들이 정치적인 견해와 TV 순위들을 릴리즈하면, 분석가는 정치적인 견해와 TV 순위들 간의 상관을 유도해 낼 수 있기 때문에, 정치적인 견해를 사적으로 유지하기를 원하는 사용자의 정치적인 견해를 추론할 수 있다.

[0014] 사적 데이터에 관하여, 이것은 사용자가 공개적으로 릴리즈되지 않아야 하는 것을 나타내는 것을 물론이고 릴리즈한 다른 데이터로부터 추론되기를 원하지 않는다는 것을 나타내는 데이터를 지칭한다. 공용 데이터는 사용자가 프라이버시 에이전트로 하여금 사적 데이터의 추론을 방지하기 위해 아마도 왜곡된 방식으로 릴리즈하도록 허용한 데이터이다.

[0015] 일 실시예에서, 공용 데이터는 서비스 제공자가 사용자에게 서비스를 제공하기 위해 사용자에게 요청한 데이터

이다. 그러나, 사용자는 서비스 제공자에게 릴리즈하기 전에 왜곡할 것이다(즉, 수정할 것이다). 또 다른 실시예에서, 공용 데이터는 릴리즈(release)가 사적 데이터의 추론에 대항하여 보호하는 형태를 취하는 한 릴리즈되는 것을 꺼리지 않는다는 점에서 사용자가 "공용(public)"인 것으로 표시되는 데이터이다.

[0016] 앞서 논의한 바와 같이, 데이터의 특정 카테고리가 사적 데이터 또는 공용 데이터로서 고려될지의 여부는 특정 사용자의 관점에 기초한다. 표기의 용이성을 위해, 우리는 현재 사용자의 관점에서 데이터의 특정 카테고리를 사적 데이터 또는 공용 데이터라고 칭한다. 예를 들어, 정치적인 사적 견해를 유지하기를 원하는 현재 사용자에 대한 프라이버시 보호 매핑을 설계하려고 할 때, 우리는 그의 정치적인 견해를 릴리즈할 의향이 있는 다른 사용자와 현재 사용자 양쪽 모두에 대해 정치적인 견해를 사적 데이터라고 칭한다.

[0017] 본 원리에서, 우리는 릴리즈 데이터와 공용 데이터 간의 왜곡을 유틸리티의 척도로서 이용한다. 왜곡이 더 큰 경우, 릴리즈 데이터는 공용 데이터와 상당히 상이하고, 더 많은 프라이버시가 보호되지만, 왜곡 데이터로부터 파생된 유틸리티는 사용자에 대해 더 낮아질 수 있다. 한편, 왜곡이 더 작은 경우, 릴리즈 데이터는 공용 데이터의 보다 정확한 표현이고 사용자는 더 많은 유틸리티를 받을 수 있고, 예를 들어 보다 정확한 콘텐츠 추천을 받을 수 있다.

[0018] 일 실시예에서, 통계적 추론에 대항하여 프라이버시를 보호하기 위해, 우리는 왜곡 제약에 종속되고, 사적 데이터와 릴리즈 데이터 간의 상호 정보(mutual information)량으로서 정의되는 정보 누설을 최소화하는 최적화 문제를 해결함으로써 사적-유틸리티 트레이드오프를 모델링하고 프라이버시 보호 매핑을 설계한다.

[0019] Fawaz에서, 프라이버시 보호 매핑을 찾는 것은, 사적 데이터와 릴리즈 데이터를 링크하는 사전 결합 분포(joint distribution)가 알려져 있고 최적화 문제에 대한 입력으로서 제공될 수 있다고 하는 기본적인 가정에 의존한다. 실제로, 참된 사전 분포는 알려져 있지 않지만, 일부 종래의 통계들은 관찰될 수 있는 한 세트의 샘플 데이터로부터 추정될 수 있다. 예를 들어, 사전 결합 분포는, 프라이버시에 대한 관심을 가지고 있지 않으며 또한 그들의 프라이버시에 관해 관심있는 사용자들에 의해 사적 또는 공용 데이터인 것으로 고려될 수 있는 상이한 데이터의 카테고리들을 공개적으로 릴리즈하는 한 세트의 사용자들로부터 추정될 수 있다. 대안적으로, 사적 데이터가 관찰될 수 없을 때, 릴리즈될 공용 데이터의 주변 분포, 또는 단순히 그것의 2차 순서 통계(order statistics)가, 단지 그들의 공용 데이터를 릴리즈한 한 세트의 사용자들로부터 추정될 수 있다. 다음으로, 이 샘플들의 세트에 기초하여 추정된 통계는 그들의 프라이버시에 대해 관심있는, 새로운 사용자들에게 적용되게 될 프라이버시 보호 매핑 메커니즘을 설계하는데 사용된다. 실제로, 예를 들어 적은 수의 관찰가능한 샘플들로 인해 또는 관찰가능한 데이터의 불완전성으로 인해, 추정된 사전 통계와 참된 사전 통계 간의 불일치가 존재할 수도 있다.

[0020] 이 문제를 공식화하기 위해, 공용 데이터는 확률 분포 P_X를 가진 랜덤 변수 $X \in \mathcal{X}$로 표시된다. X는 랜덤 변수 $S \in \mathcal{S}$로 표시된 사적 데이터와 상관된다. S와 X의 상관은 결합 분포 $P_{S,X}$에 의해 정의된다. 랜덤 변수 $Y \in \mathcal{Y}$로 표시된 릴리즈 데이터는 X의 왜곡된 버전이다. Y는 커널 $P_{Y|X}$을 통해 X를 통과시키는 것을 통해 달성된다. 본 출원에서, 용어 "커널(kernel)"은 확률적으로 데이터 X를 데이터 Y에 매핑하는 조건부 확률을 지칭한다. 즉, 커널 $P_{Y|X}$은 우리가 설계하기를 원하는 프라이버시 보호 매핑이다. Y는 본 출원에서, X만의 확률함수(probabilistic function)이기 때문에, 우리는 S→X→Y가 마르코프 체인(Markov chain)을 형성한다고 가정한다. 따라서, 우리가 $P_{Y|X}$를 정의하면, 우리는 결합 분포 $P_{S,X,Y} = P_{Y|X}P_{S,X}$와 특히 결합 분포 $P_{S,Y}$를 갖는다.

[0021] 다음에서, 우리는 첫번째로 프라이버시 개념을 정의하고나서, 정확도 개념을 정의한다.

[0022] **정의 1.** S→X→Y를 가정한다. 커널 $P_{Y|X}$은 결합 분포 $P_{S,X,Y} = P_{Y|X}P_{S,X}$에 기인한 분포 $P_{S,Y}$가 수학식 (1) $D(P_{S,Y}||P_S P_Y) \triangleq \mathbb{E}_{S,Y}\left[\log \frac{P(S|Y)}{P(S)}\right] \triangleq I(S;Y) = \epsilon H(S)$을 충족할 경우에 ϵ-발산 사적(divergence private)이라고 불리고, 여기서, D(.)은 K-L 발산이고, $\mathbb{E}(.)$은 랜덤 변수의 기대값이고, H(.)는 엔트로피이고, $\epsilon \in [0,1]$는 누설 인수라고 불리고, 상호 정보량 I(S;Y)은 정보 누설을 나타낸다.

[0023] 우리는 ϵ=0일 경우에 메커니즘이 풀 프라이버시(full privacy)를 갖는다고 말한다. 극단적인 경우들에서,

ϵ=0은 릴리즈된 랜덤 변수 Y가 사적 랜덤 변수 S와 별개라는 것을 의미하고, ϵ=1은 S가 Y로부터 완벽하게 복구가능하다는 것을 의미한다(S는 Y의 결정 함수(deterministic function)이다). 우리는 Y가 풀 프라이버시(ϵ=0)를 갖도록 S와 완전히 독립적이라고 가정할 수 있지만, 이것은 빈약한 정확도 레벨로 이어질 수 있다는 것에 유의해야 한다. 우리는 다음과 같이 정확도를 정의한다.

[0024] 정의 2. $d:\mathcal{X}\times\mathcal{Y}\to\mathbb{R}^+$를 왜곡 측도라고 하자. 커널 $P_{Y|X}$은 $\mathbb{E}[d(X,Y)]\le D$인 경우에 D-정확이라고 불려진다.

[0025] 프라이버시 보호 매핑의 누설 인수 ϵ와 왜곡 레벨 D간에 트레이드오프가 있다.

[0026] 본 원리는 사전 부분적인 통계 지식만이 활용가능할 때 유틸리티-인식 프라이버시 보호 매핑을 설계하는 방법들을 제안한다. 보다 구체적으로, 본 원리는 가산성 잡음 메커니즘들의 클래스로 프라이버시 보호 매핑 메커니즘들을 제공하고, 여기서 잡음은 공용 데이터가 릴리즈되기 전에 공용 데이터에 추가된다. 분석시, 우리는 잡음의 평균값이 0이라고 가정한다. 메커니즘은 또한 평균이 제로가 아닐 경우에 적용될 수도 있다. 일례에서, 결과들은 엔트로피가 평균에 민감하지 않기 때문에 비-제로 평균의 경우에도 동일하다. 메커니즘들은 연속 데이터와 이산 데이터 양쪽 둘다에 대해 릴리즈될 데이터의 2차 모멘트들의 지식만을 필요로 한다.

[0027] 가우시안 메커니즘

[0028] 일 실시예에서, 우리는 연속 공용 데이터 X와 신호에 잡음을 부가함으로써, 즉 Y=X+N으로 달성될 수 있는 프라이버시 보호 매핑 방식들을 고려한다. 예시적인 연속 공용 데이터는 사용자의 키 또는 혈압일 수 있다. 매핑은 P_X와 $P_{S,X}$에 대한 지식없이, VAR(X)(또는 다차원 X인 경우에 공분산 행렬)을 알고 있음으로써 획득된다. 첫번째로, 우리는 잡음이 프라이버시를 보호하기 위해 공용 데이터에 추가될 때 모든 프라이버시 보호 매핑 메커니즘들 중에서, 가우시안 잡음을 추가하는 것이 최적이라는 것을 보일 것이다.

[0029] S→X→Y 이기 때문에, 우리는 I(S;Y)≤I(X;Y)를 갖는다. 정보 누설 I(S;Y)을 바운드(bound)하기 위해, 우리는 I(X;Y)로 바운드한다. $X=f(S)$가 S의 결정 함수인 경우, I(S;Y)=I(X;Y)이고 바운드는 타이트(tight)하다(이것은 예를 들어, 어떤 행렬 A의 경우에 X=AS일 때 선형 회귀시 발생한다).

[0030] $X\in\mathbb{R}^n$이라고 하자. C_X에 의해 X의 공분산 행렬을 표시한다. Y=X+N이라고 하고, 여기서 N은 평균 0과 공분산 행렬 C_N을 가지면서, X와는 별개의 잡음이다. 우리는 하나의 랜덤 변수만이 있을 때 분산 (σ_N^2)의 표기를 사용하고, 다수개 있을 때 분산(C_N)을 사용한다는 것에 유의해야 한다. 우리는 다음 결과를 갖는다.

[0031] **명제 2.** P_X는 프라이버시 보호 매핑의 설계시 알려져 있지 않았고 우리는 어떤 σ_X의 경우에 단지 $\mathrm{VAR}(X)\le\sigma_X^2$를 알고 있다고 가정한다. 또한, 신호 X에 독립적 잡음 N을 추가함으로써 획득되는 프라이버시 보호 메커니즘들의 클래스를 고려한다. 잡음은 어떤 σ_N의 경우에 σ_N^2보다 크지 않은 분산(ℓ_2-노름 왜곡(norm distortion))과 제로 평균을 갖는다. 우리는 하기 의미에서, 가우시안 잡음이 최선이라는 것을 보일 것이다:

[0032] $$\max_{P_X:X\perp\!\!\!\perp N_G,\,\mathrm{VAR}(X)\le\sigma_X^2} I(X;X+N_G)\le\max_{P_X:X\perp\!\!\!\perp N,\,\mathrm{VAR}(X)\le\sigma_X^2} I(X;X+N),\quad(15)$$

[0033] 여기서, N_G는 가우시안 잡음을 나타내고 N은 랜덤 변수이어서 $\mathbb{E}[N_G]=\mathbb{E}[N]=0$이고 $\mathrm{VAR}(N_G)=\mathrm{VAR}(N)=\sigma_N^2$이다. 이것은 N_G를 이용한 최악의 경우의 정보 누설은 N을 이용한 최악의 경우의 정보 누설보다 크지 않다는 것을 의미한다.

[0034] 증명: 가우시안 안장점 정리를 이용하면, 우리는

[0035] $$\max_{P_X:X\perp\!\!\!\perp N_G,\,\mathrm{VAR}(X)\le\sigma_X^2} I(X;X+N_G)$$
$$=I(X_G;X_G+N_G)\le I(X_G;X_G+N)$$
$$\le\max_{P_X:X\perp\!\!\!\perp N,\,\mathrm{VAR}(X)\le\sigma_X^2} I(X;X+N),\quad(16)$$을 가지고

[0036] 여기서 X_G는 제로 평균과 분산 σ_X^2을 가진 가우시안 분포를 갖는다. 이것은 증명을 완료한다. □

[0037] 이제 우리는 잡음이 프라이버시를 보호하기 위해 추가될 때, 가우시안 잡음을 추가하는 것이 ℓ_2-노름 왜곡 제약하에서, 가산성 잡음들의 패밀리중에서 최적의 해결책이라는 것을 알았다. 다음에서, 우리는 가우시안 잡음이 공용 데이터에 추가되게 될 최적의 파라미터들을 결정한다. 우리는 가우시안 메커니즘에 의해 가우시안 잡음을 그러한 파라미터들에 추가하는 메커니즘을 표시한다.

[0038] 한가지 예시적 실시예에서, 주어진 C_X와 왜곡 레벨 D에 대해, 가우시안 메커니즘은 도 1에 예시된 바와 같은 단계들에 의해 진행된다.

[0039] 방법 100은 105에서 시작된다. 단계 110에서, 공용 데이터 또는 사적 데이터의 프라이버시에 관해 관심이 없는 사용자들에 의해 릴리즈된 데이터에 기초하여 통계 정보를 추정한다. 우리는 이들 사용자들을 "공용 사용자들"이라고 표시하고, 사적 데이터의 프라이버시에 관해 관심이 있는 사용자들을 "사적 사용자들"이라고 표시한다.

[0040] 통계는 웹을 크롤링(crawling)하고 상이한 데이터베이스에 액세스함으로써 수집될 수 있거나, 데이터 집계기(data aggregator), 예를 들어 bluekai.com.에 의해 제공될 수 있다. 어느 통계 정보가 수집될 수 있는지는 공용 사용자들이 무엇을 릴리즈하는지에 의존한다. 주변 분포 P_X를 특성화하는 것보다 분산을 특성화하기 위해 더 적은 데이터를 필요로 한다는 것에 유의해야 한다. 따라서, 우리는 우리가 분산을 추정할 수 있지만, 주변 분포를 정확하게 추정할 수 없는 상황에 있을 수 있다. 일 예에서, 우리는 단지 수집된 통계 정보에 기초하여 단계 120에서 공용 데이터의 평균과 분산(또는 공분산)을 얻을 수 있다.

[0041] 단계 130에서, 우리는 공분산 행렬 C_X의 고유값 분해를 취한다. 가우시안 잡음 N_G의 공분산 행렬은 C_X의 고유벡터들과 동일하게 고유벡터들을 갖는다. 게다가, C_N의 대응하는 고유값들은 하기 최적화 문제

$$\min_{\sigma_i:\ 1\le i\le n} \prod_{i=1}^{n} \frac{\sigma_i + \lambda_i}{\sigma_i}$$

[0042] $$\text{s.t. } \sum_{i=1}^{n} \sigma_i \le D, \quad (17)$$

[0043] 를 해결함으로써 주어지고

[0044] 여기서, λ_is 와 $\sigma_i \mathrm{s}\,(1 \le \lambda_i \le n)$는 각각 고유값들 C_X와 C_N를 표시한다. 다음으로, 결정된 고유벡터들과 고유값들로부터, 우리는 그것의 고유분해를 통해, 가우시안 잡음에 대한 공분산 행렬 C_N을 결정할 수 있다. 다음으로, 우리는 가우시안 잡음 $N_G \sim \mathcal{N}(0, C_N)$을 생성할 수 있다. 왜곡은 $\sum_{i=1}^{n} \mathbb{E}\left[(Y_i - X_i)^2\right] = \mathrm{tr}(C_N) = \sum_{i=1}^{n} \sigma_i \le D$로 주어지고, 여기서 tr()은 대각 원소들의 합계를 표시하고 n은 벡터 X의 차원이다.

[0045] 단계 140에서, 가우시안 잡음은 공용 데이터에 추가되는데, 즉 $Y=X+N_G$이다. 다음으로, 왜곡 데이터가 예를 들어, 단계 150에서, 서비스 제공자 또는 데이터 수집 에이전시에게 릴리즈된다. 방법 100은 단계 199에서 종료된다.

[0046] 하기 정리에서, 우리는 제안된 가우시안 메커니즘이 ℓ_2-노름 왜곡 제약하에서 최적이라는 것을 입증한다.

[0047] **정리 3.** ℓ_2-노름 왜곡과 주어진 왜곡 레벨, D을 가정하면, 상호 정보량을 최소화하는 가우시안 메커니즘에서의 최적 가우시안 잡음은:

[0048] 최적 잡음 N_G의 공분산 행렬이 C_X의 고유벡터들과 동일하게 고유 벡터들을 갖는다는 것을 충족한다. 또한, 고유값들은 (17)에서 주어진다.

[0049] 증명: 우리는 $I(X; X+N) \le \frac{1}{2}\log\left(\frac{|C_X + C_N|}{|C_N|}\right)$, (18)을 가지고,

[0050] 여기서, 부등식은 2012년, 윌리-인터사이언스(Wiley-interscience), "Elements of information theory", 티.엠. 커버(T.M. Cover)와 제이.에이. 토마스(J.A. Thomas)에 의한 책의 정리 8.6.5로부터 유래한다. 우리가 X의 분산을 알지 못하기 때문에, 우리는 상계(upper bound) $\frac{1}{2}\log\left(\frac{|C_X+C_N|}{|C_N|}\right)$를 최소화하여야 하는데, 그 이유는 이것이 가우시안 X에 의해 달성될 수 있기 때문이다. $C_X = Q\Lambda Q^t$를 얻기 위해 반확정 행렬 C_X의 고유값 분해를 고려하고, 여기서 $QQ^t = I$이고 Λ는 C_X의 고유값들을 포함하는 대각 행렬이다. 우리는 $\mathbb{E}[\sum_{i=1}^{k}(Y_i - X_i)^2] = tr(C_N) = tr(Q^tC_NQ) = \sum\sigma_i \le D$를 가지고 최적화 문제는

[0051] $\min_{C_N}\frac{|\Lambda+Q^tC_NQ|}{|Q^tC_NQ|}$, s.t. $\mathrm{tr}(Q^tC_NQ) \le D$이 된다.

[0052] 보편성의 손실없이, $\lambda_1 \ge \cdots \ge \lambda_n$라고 가정한다. $\sigma_1 \ge \cdots \ge \sigma_n$이 $Q^tC_NQ^t$의 고유값들이라고 하자. 미국 수학 협회의 회의록, "Bounds for the determinant of the sum of Hermitian matrices", 엠. 피들러(M. Fiedler)에 의한 논문의 정리 1에 따르면, 우리는 $|\Lambda + Q^tC_NQ| \ge \prod(\lambda_i+\sigma_i)$를 가지고 등식은 Q^tC_NQ가 대각 행렬인 경우에 성립한다. 따라서, 동일한 고유값들 σ_iS을 가진 대각 행렬을 이용하여, 우리는 동일 왜곡 레벨 및 더 작은 누설을 달성하는데, 이것은 최적성과 모순된다. 따라서, Q^tC_NQ는 대각 행렬이다. □

[0053] **예 3.** X는 S의 결정론적 실수치 함수이며, $X = f(S)$이고 $\mathrm{VAR}(X) = \sigma_X^2$이라고 가정한다. S→X→Y이기 때문에, 우리는 I(X;Y)=I(S;Y)를 갖는다. $N \sim \mathcal{N}(0,\sigma_N^2)$이고 Y=X+N이라고 하자. 임의의 ϵ의 경우, 우리는 (ϵ,D)-발산-왜곡 사적을 달성할 수 있고, 여기서 $D = \frac{\sigma_X^2}{e^{2\epsilon H(S)}-1}$이다.

[0054] **주석 1.** 이 분석은 ϵ>0에 대해서만 통한다. 우리가 완벽한 프라이버시, 즉, ϵ=0를 갖기를 원한다면, 이 방식은 $\sigma_N^2 = \infty$를 선택한다. 실제로, 이것은 Y가 X와 독립적이라는 것을 의미한다. 우리가 $Y = \mathbb{E}[X]$(결정론적 값)라고 가정하면, I(Y;S)=0이고 $\mathbb{E}[d(X,Y)] = \mathrm{VAR}(X)$이다. 따라서, VAR(X)보다 크거나 이와 동일한 왜곡 레벨의 경우, $Y = \mathbb{E}[X]$를 설정하는 결정론적 메커니즘은 ϵ=0를 달성한다.

[0055] **예 5.** 분산 $\sigma_N^2 \ge \frac{1}{\epsilon^2}2\log(2/\delta)$을 가진 가우시안 잡음을 추가함으로써, 우리가 (ϵ,δ)-차별적 프라이버시(differential privacy)를 달성할 수 있다는 것이 보여줄 수 있다. 이 방식은 왜곡 $D \ge \frac{1}{\epsilon^2}2\log(2/\delta)$와 정보의 누설 $L \le \frac{1}{2}\log\left(1+\frac{\sigma_X^2}{\frac{1}{\epsilon^2}2\log(2/\delta)}\right)$이 초래된다. 비교를 위한 질적 방식은 (ϵ,δ) 차별적 프라이버시 가우시안 메커니즘을 이용하면, 우리가 작은 누설을 달성하기 위해 큰 왜곡을 필요로 할 것이라는 것을 말한다. 한편, 본 원리에 따른 발산 프라이버시 가우시안 메커니즘을 이용하면, 최소 왜곡 D을 가지며 L 비트들을 누설시키는 방식은 임의의 (ϵ,δ)-차별적 프라이버시를 달성하고, 여기서 $\frac{1}{\epsilon^2}2\log\left(\frac{2}{\delta}\right) = \frac{\sigma_X^2}{e^{2L}-1}$이다.

[0056] 이산 메커니즘(Discrete Mechanism)

[0057] 또 다른 실시예에서, 우리는 이산 랜덤 변수 X를 고려하며, 여기서 $\mathcal{X} = \mathbb{Z}$이다. 다시, 우리는 I(S;Y)를 바운드하기 위해 I(X;Y)로 바운드한다. 왜곡 측도가 ℓ_p 노름이라고 하고, 즉 어떤 $1 \le p \le \infty$인 경우에 X와 Y간의 왜곡이 $\mathbb{E}[|X-Y|^p]^{\frac{1}{p}}$라고 하자.

[0058] **정의 5.** 주어진 $1 \le p \le \infty$에 대해, 주어진 D보다 작거나 이와 동일한 ℓ_p 노름을 가진 모든 랜덤 변수 중에서,

$P^*_{p,D}$에 의해 최대 엔트로피를 갖는 분산을 표시한다. 보다 형식적으로, $P^*_{p,D}$는 다음 최적화 $\max_{P_Z: Z\sim P_Z} H(Z),\ \text{s.t.}\ \mathbb{E}[|Z|^p]^{\frac{1}{p}} \le D$에서 최대 목적 함수를 달성하는 확률 측도이다.

[0059] 즉, 최적화 문제는 p^{th} 모멘트상의 제약에 종속되는, 최대 엔트로피 이산 확률 분포 $P^*_{p,D}$에 있게 된다. 최대 엔트로피는 $H^*(p,D)$로 표시된다.

[0060] 다음으로, 우리는 $P^*_{p,D}$와 이것의 엔트로피를 특성화한다.

[0061] **명제 3.** 임의의 $1 \le p \le \infty$에 대해, $P^*_{p,D}$는 $P^*_{p,D}[Z=i] = AB^{-|i|^p}$에 의해 주어지고, 여기서 A와 B는 $\sum_{i=-\infty}^{\infty} A\,B^{-|i|^p} = 1$이고 $\mathbb{E}[|Z|^p]^{\frac{1}{p}} = D$이 되도록 선택된다. 게다가, 우리는 $H^*(p,D) = -\log A + (\log B)D^p$를 갖는다.

[0062] 증명: $Z \sim AB^{-|i|^p}$ 및 $W \sim P_W$로 하여 $\mathbb{E}[|W|^p]^{\frac{1}{p}} \le D$가 되게 하자. $\mathbb{E}_{P_W}[|i|^p] \le D^p$이기 때문에, 우리는

$$0 \le D(P_W||P_Z) = \mathbb{E}_{P_W}[\log \frac{P_W}{P_Z}]$$

$$= -H(W) - \mathbb{E}_{P_W}[\log A - (\log B)|i|^p]$$

[0063] $$\le -H(W) - \log A + (\log B)\mathbb{E}_{P_Z}[|i|^p]$$

[0064] $$= -H(W) + H(Z)$$를 갖는다.

[0065] 따라서, H(Z)≥H(W)이고 $H^*(p,D) = -\log A + (\log B)D^p$이다. □

[0066] 우리는 이산 메커니즘에 의해 이산 공용 데이터에 잡음 $Z \sim P^*_{p,D}$를 추가하는 메커니즘을 표시한다. 한가지 예시적인 실시예에서, 이산 메커니즘은 도 2에 예시된 바와 같은 단계들에 의해 진행된다.

[0067] 방법 200은 205에서 시작된다. 단계 210에서, 왜곡 측도를 정의하기 위해, 파라미터들, 예를 들어 p와 D에 엑세스한다. 주어진 왜곡 측도 ℓ_p ($1 \le p \le \infty$)와 왜곡 레벨 D의 경우, 단계 220에서 명제 3에서 주어진 바와 같이 확률 측도 $P^*_{p,D}$를 계산한다. 분산 $P^*_{p,D}$은 단지 p와 D에 의해 결정되지만, 최종적인 프라이버시 정확도 트레이드오프는 X에 의존할 것이며, 그 이유는 왜곡 제약이 프라이버시와 정확도를 결합하기 때문이라는 것에 유의해야 한다.

[0068] 단계 230에서, 잡음은 단계 240에서 이것이 공용 데이터에 추가되기 전에, 즉 Y=X+Z되기 전에 확률 측도에 따라 생성되며, 여기서 $Z \sim P^*_{p,D}$이다. 우리는 $d(X,Y) = \mathbb{E}[|Y-X|^p]^{\frac{1}{p}} = \mathbb{E}[|Z|^p]^{\frac{1}{p}} \le D$를 갖는다. 방법 200은 단계 299에서 종료된다.

[0069] 다음으로, 우리는 상호 정보량 I(X;Y)을 분석한다. $||X||_p = \mathbb{E}[|X|^p]^{\frac{1}{p}}$가 X의 ℓ_p 노름을 표시한다고 하자. 민코프스키의 부등식을 이용하여, 우리는 $\mathbb{E}[|Y|^p]^{\frac{1}{p}} = \mathbb{E}[|X+Z|^p]^{\frac{1}{p}} \le \mathbb{E}[|X|^p]^{\frac{1}{p}} + \mathbb{E}[|Z|^p]^{\frac{1}{p}} = ||X||_p + D$를 갖는다. 따라서, 우리는 $I(S;Y) \le I(X;Y) = H(X+Z) - H(Z) \le H^*(p, ||X||_p + D) - H^*(p,D)$를 얻는다. 즉, 이산 메커니즘을 이용할 때 우리가 획득하는 프라이버시 보장(즉, 정보 누설)은 X의 평균 ℓ_p 노름과 D 양쪽 모두에 의존하는, 우측 항에 의해 상계가 지어진다.

[0070] 가산성 잡음 기술의 장점은 이것이 S에 관한 정보는 물론이고, X의 통계에 관한 많은 정보를 요구하지 않을 뿐만 아니라, 우리가 설계하는데 필요한 모든 것이 풀 커널 $P_{Y|X}$를 특정하는 것 대신에, 잡음의 파라미터들이 되는 간단한 문제로 최적화 문제를 축소시킨다는 것이다. 이것은 최적화의 사이즈를 현저하게 축소시킬 수 있으며, 또한 그에 따라 그것을 해결하기 위한 그것의 복잡도 및 연산/메모리 요구사항을 현저하게 감소시킨다.

[0071] 유리하게는, 결합 확률 분포 $P_{S,X}$의 지식없이 그리고 공용 데이터 X의 1차 및 2차 모멘트들의 지식만을 가지고, 본 원리는 연속 및 이산 데이터 양쪽 둘다에 대해, 공용 데이터에 잡음을 추가함으로써 프라이버시를 보호하는 프라이버시 보호 매핑 메커니즘을 제공한다.

[0072] 프라이버시 에이전트는 사용자에게 프라이버시 서비스를 제공하는 엔티티이다. 프라이버시 에이전트는 다음 중 어느 하나를 수행할 수 있다:

[0073] - 사용자로부터 그가 어떤 데이터를 사적인 것으로 간주하는지, 그가 어떤 데이터를 공용으로 간주하는지, 및 그가 어떤 레벨의 프라이버시를 원하는지를 수신하고;

[0074] - 프라이버시 보호 매핑을 계산하고;

[0075] - 사용자를 위한 프라이버시 보호 매핑을 구현하고(즉, 매핑에 따라 그의 데이터를 왜곡하고); 및

[0076] - 왜곡 데이터를, 예를 들어 서비스 제공자 또는 데이터 수집 에이전시에게 릴리즈한다.

[0077] 본 원리들은 사용자 데이터의 프라이버시를 보호하는 프라이버시 에이전트에서 사용될 수 있다. 도 3은 프라이버시 에이전트가 이용될 수 있는 예시적인 시스템(300)의 블록도를 나타낸다. 공용 사용자들(310)은 그들의 사적 데이터(S) 및/또는 공용 데이터(X)를 릴리즈한다. 앞서 논의한 바와 같이, 공용 사용자들은 공용 데이터를 그대로 릴리즈하는데, 즉, Y=X이다. 공용 사용자들에 의해 릴리즈된 정보는 프라이버시 에이전트에게 유용한 통계 정보가 된다.

[0078] 프라이버시 에이전트(380)는 통계 수집 모듈(320), 가산성 잡음 생성기(330) 및 프라이버시 보호 모듈(340)을 포함한다. 통계 수집 모듈(320)은 공용 데이터의 공분산을 수집하는데 사용될 수 있다. 통계 수집 모듈(320)은 또한 bluekai.com과 같은 데이터 집계기들로부터 통계를 수신할 수 있다. 이용가능한 통계 정보에 따라, 가산성 잡음 생성기(330)는 예를 들어, 가우시안 메커니즘 또는 이산 메커니즘에 기초하여 잡음을 설계한다. 프라이버시 보호 모듈(340)은 생성된 잡음을 추가함으로써, 릴리즈되기 전에 사적 사용자(360)의 공용 데이터를 왜곡한다. 일 실시예에서, 통계 수집 모듈(320), 가산성 잡음 생성기(330) 및 프라이버시 보호 모듈(340)은 각각 방법 100에서의 단계들 110, 130 및 140을 수행하는데 사용될 수 있다.

[0079] 프라이버시 에이전트는 데이터 수집 모듈에서 수집된 전체 데이터에 대한 지식 없이 작업하기 위해 통계만을 필요로 한다는 점에 유의해야 한다. 따라서, 또 다른 실시예에서, 데이터 수집 모듈은 데이터를 수집하고나서 통계를 계산하는 독립형 모듈일 수 있으며, 프라이버시 에이전트의 일부일 필요가 없다. 데이터 수집 모듈은 프라이버시 에이전트와 통계를 공유한다. 일 실시예에서, 가산성 잡음 생성기(330)와 프라이버시 보호 모듈(340)은 각각 방법 200에서의 단계들 220 및 230을 수행하는데 사용될 수 있다.

[0080] 프라이버시 에이전트는 사용자와 사용자 데이터의 수령인(예를 들어, 서비스 제공자) 사이에 위치한다. 예를 들어, 프라이버시 에이전트는 사용자 디바이스, 예를 들어 컴퓨터 또는 셋톱 박스(STB)에 위치할 수 있다. 다른 예에서, 프라이버시 에이전트는 별개의 엔티티일 수 있다.

[0081] 프라이버시 에이전트의 모든 모듈들은 하나의 디바이스에 위치할 수 있거나, 상이한 디바이스들에 걸쳐 분산될 수 있는데, 예를 들어 통계 수집 모듈(320)은 단지 통계를 모듈(330)에 릴리즈하는 데이터 집계기에 위치할 수 있고, 가산성 잡음 생성기(330)는 "프라이버시 서비스 제공자"에 또는 모듈(320)에 접속되는 사용자 디바이스 상의 사용자 단부에 위치할 수 있고, 프라이버시 보호 모듈(340)은 사용자와, 사용자가 데이터를 릴리즈하기를 원하는 대상인 서비스 제공자 사이에 매개물로서 작용하는 프라이버시 서비스 제공자에 또는 사용자 디바이스 상의 사용자 단부에 위치할 수 있다.

[0082] 프라이버시 에이전트는 릴리즈 데이터를 서비스 제공자, 예를 들어 컴캐스트(Comcast) 또는 넷플릭스(Netflix)에 제공할 수 있으며, 이에 따라 사적 사용자(360)는 릴리즈 데이터에 기초하여 수신 서비스를 개선할 수 있는데, 예를 들어 추천 시스템은 사용자에게 그의 릴리즈된 영화 순위들에 기초하여 영화 추천들을 제공한다.

[0083] 도 4에서, 우리는 시스템 내에 복수의 프라이버시 에이전트가 존재한다는 것을 나타낸다. 상이한 변형들에서는, 도처에 프라이버시 에이전트들이 존재할 필요가 없는데, 이는 프라이버시 시스템이 작동할 요건이 아니기 때문이다. 예를 들어, 사용자 디바이스에 또는 서비스 제공자에 또는 이들 양자에 하나의 프라이버시 에이전트만이 존재할 수 있다. 도 4에서, 우리는 넷플릭스(Netflix)와 페이스북(Facebook) 양자에 대해 동일 프라이버시 에이전트 "C"가 존재한다는 것을 나타낸다. 다른 실시예에서, 페이스북 및 넷플리스에 있는 프라이버시 에이전트들은 동일할 수 있지만, 반드시 그럴 필요는 없다.

[0084] 본 명세서에서 기술되는 구현들은, 예를 들어 방법 또는 프로세스, 장치, 소프트웨어 프로그램, 데이터 스트림 또는 신호에 구현될 수 있다. 단일 형태의 구현의 맥락으로만 논의되는(예를 들어, 방법으로만 논의되는) 경우에도, 논의되는 특징들의 구현은 다른 형태들(예를 들어, 장치 또는 프로그램)로도 구현될 수 있다. 장치는 예를 들어, 적절한 하드웨어, 소프트웨어, 및 펌웨어로 구현될 수 있다. 방법들은 예를 들어, 일반적으로 예를 들어 컴퓨터, 마이크로프로세서, 집적 회로, 또는 프로그램가능 로직 디바이스를 포함하는 프로세싱 디바이스들을 지칭하는 예컨대 프로세서와 같은 장치에서 구현될 수 있다. 프로세서들은 또한 예를 들어 컴퓨터, 셀 폰, 휴대용/개인용 디지털 단말기("PDA"), 및 최종 사용자들 간의 정보의 통신을 용이하게 하는 다른 장치들과 같은 통신 장치들을 포함한다.

[0085] 본원의 원리들의 "일 실시예" 또는 "실시예" 또는 "하나의 구현" 또는 "구현"에 대한 참조뿐 아니라 그의 다른 변형들은, 실시예와 관련하여 설명되는 특정한 특징, 구조, 특성 등이 본원의 원리들의 적어도 일 실시예에 포함된다는 것을 의미한다. 따라서, 명세서 전체에 걸쳐서 다양한 곳에서 나타나는 "일 실시예에서" 또는 "실시예에서" 또는 "하나의 구현에서" 또는 "구현에서"라는 문구뿐 아니라 임의의 다른 변형들은 반드시 모두가 동일 실시예를 지칭하는 것은 아니다.

[0086] 게다가, 본원, 또는 그의 청구항들은 다양한 정보들을 "결정하는 것"을 지칭할 수 있다. 정보를 결정하는 것은 예를 들어, 정보를 추정하는 것, 정보를 계산하는 것, 정보를 예측하는 것 또는 메모리로부터의 정보를 검색하는 것 중 하나 이상을 포함할 수 있다.

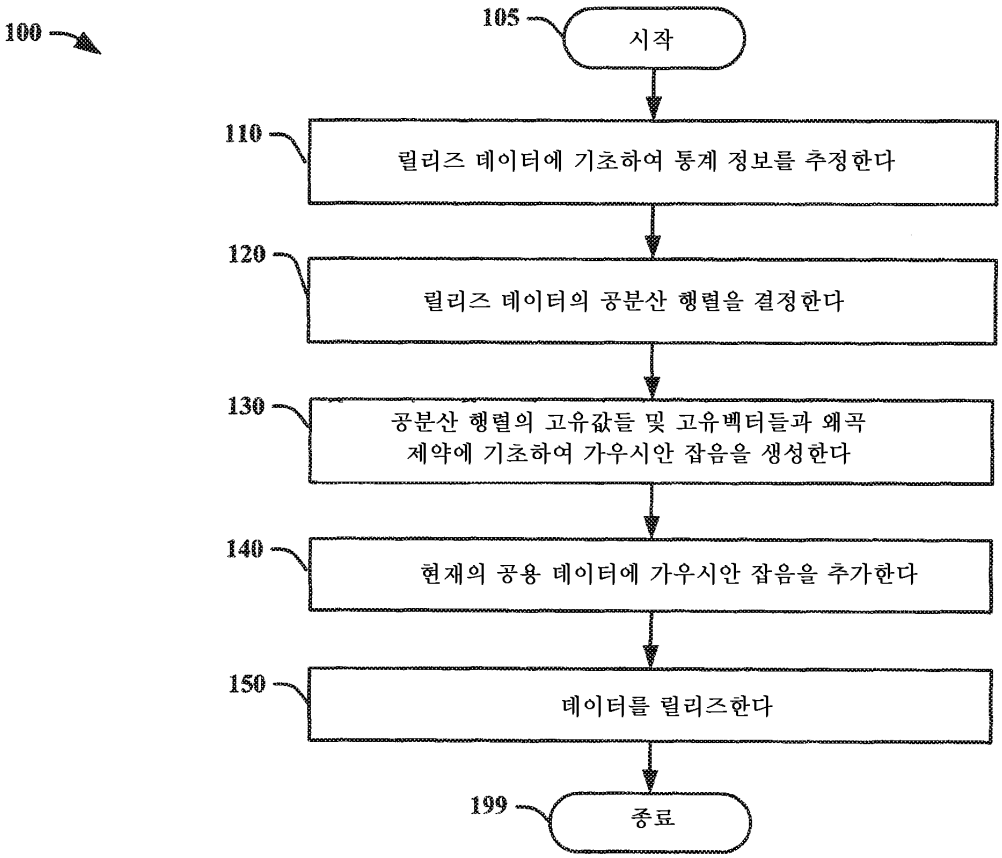
[0087] 또한, 본원, 또는 그의 청구항들은 다양한 정보들을 "액세스하는 것"을 지칭할 수 있다. 정보에 액세스하는 것은 예를 들어, 정보를 수신하는 것, (예를 들어, 메모리로부터의) 정보를 검색하는 것, 정보를 저장하는 것, 정보를 처리하는 것, 정보를 전송하는 것, 정보를 이동시키는 것, 정보를 복사하는 것, 정보를 소거하는 것, 정보를 계산하는 것, 정보를 결정하는 것, 정보를 예측하는 것, 또는 정보를 추정하는 것 중 하나 이상을 포함할 수 있다.

[0088] 게다가, 본원, 또는 그의 청구항들은 다양한 정보의 "수신"을 지칭할 수 있다. 수신은 "액세스"와 같이 광범위한 용어인 것을 의도한다. 정보의 수신은 예를 들어, 정보에 액세스하는 것 또는 (예를 들어, 메모리로부터의) 정보를 검색하는 것 중 하나 이상을 포함할 수 있다. 또한, "수신"은 통상적으로 예를 들어, 정보를 저장하는 것, 정보를 처리하는 것, 정보를 전송하는 것, 정보를 이동시키는 것, 정보를 복사하는 것, 정보를 소거하는 것, 정보를 계산하는 것, 정보를 결정하는 것, 정보를 예측하는 것 또는 정보를 추정하는 것과 같은 동작들 동안 하나의 방식 또는 다른 방식으로 수반된다.

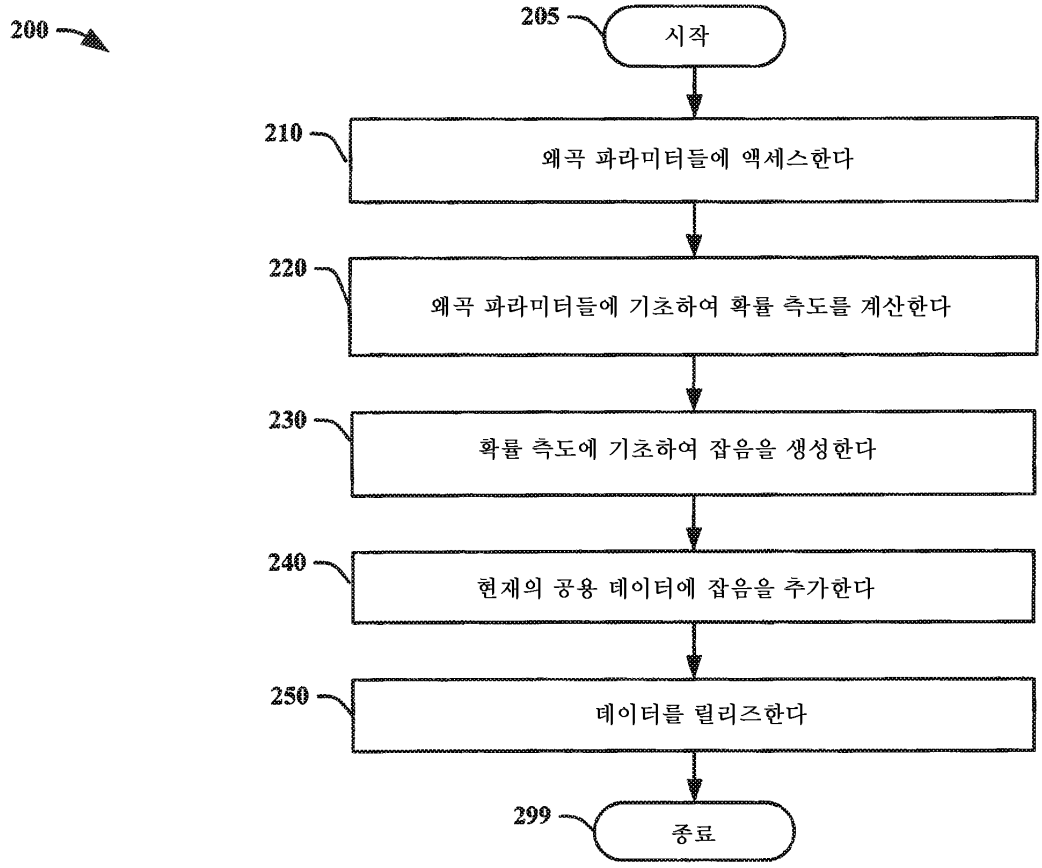
[0089] 통상의 기술자에게 명백할 것인 바와 같이, 구현들은 예를 들어 저장 또는 전송될 수 있는 정보를 전달하도록 포맷팅되는 다양한 신호들을 생성할 수 있다. 정보는, 예를 들어 방법을 수행하기 위한 명령어들, 또는 설명되는 구현들 중 하나에 의해 생성되는 데이터를 포함할 수 있다. 예를 들어, 신호는 설명되는 실시예의 비트스트림을 전달하도록 포맷팅될 수 있다. 그러한 신호는, (예를 들어, 스펙트럼의 무선 주파수 부분을 이용하여) 예를 들어, 전자기파로서, 또는 기저대역 신호로서 포맷팅될 수 있다. 포맷팅은, 예를 들어 데이터 스트림을 인코딩하고, 인코딩된 데이터 스트림으로 반송파를 변조하는 것을 포함할 수 있다. 신호가 전달하는 정보는, 예를 들어 아날로그 또는 디지털 정보일 수 있다. 신호는 알려진 바와 같이, 각종 상이한 유선 또는 무선 링크들을 통해 전송될 수 있다. 신호는 프로세서 판독가능 매체 상에 저장될 수 있다.

도면

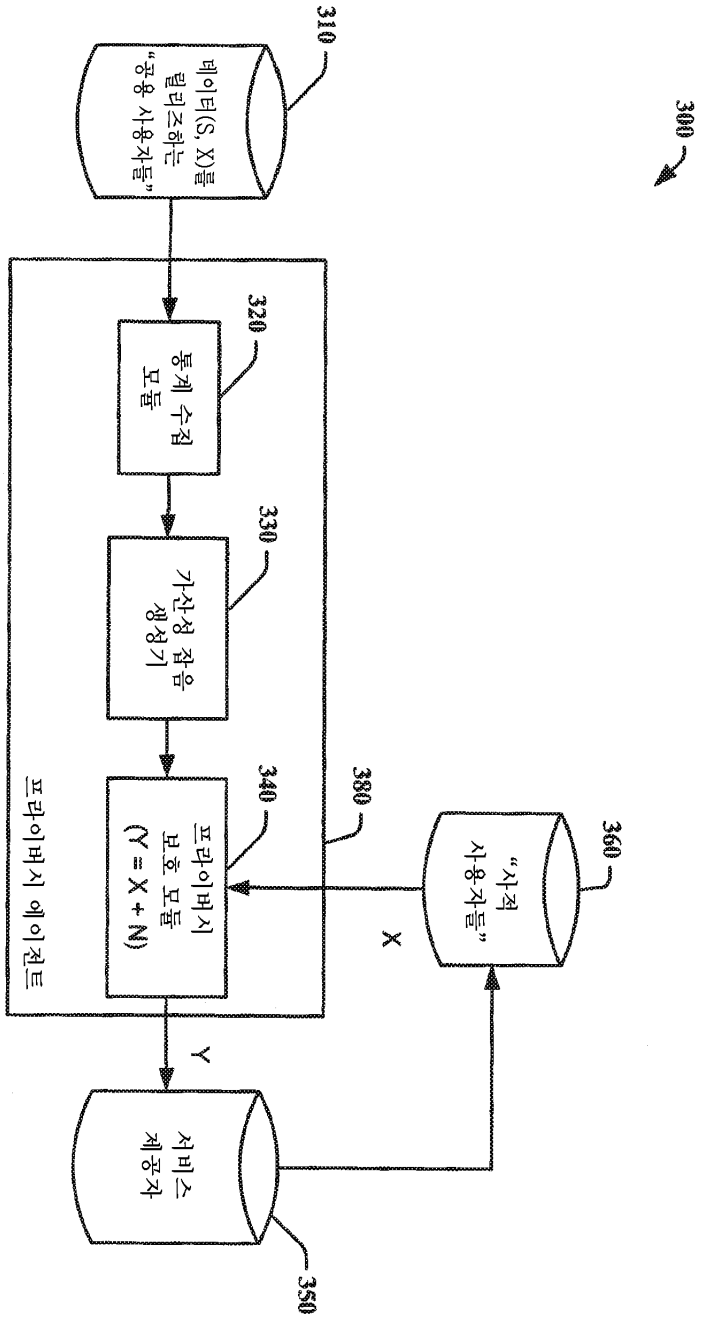
도면1


100
105
시작
110
릴리즈 데이터에 기초하여 통계 정보를 추정한다
120
릴리즈 데이터의 공분산 행렬을 결정한다
130
공분산 행렬의 고유값들 및 고유벡터들과 왜곡 제약에 기초하여 가우시안 잡음을 생성한다
140
현재의 공용 데이터에 가우시안 잡음을 추가한다
150
데이터를 릴리즈한다
199
종료

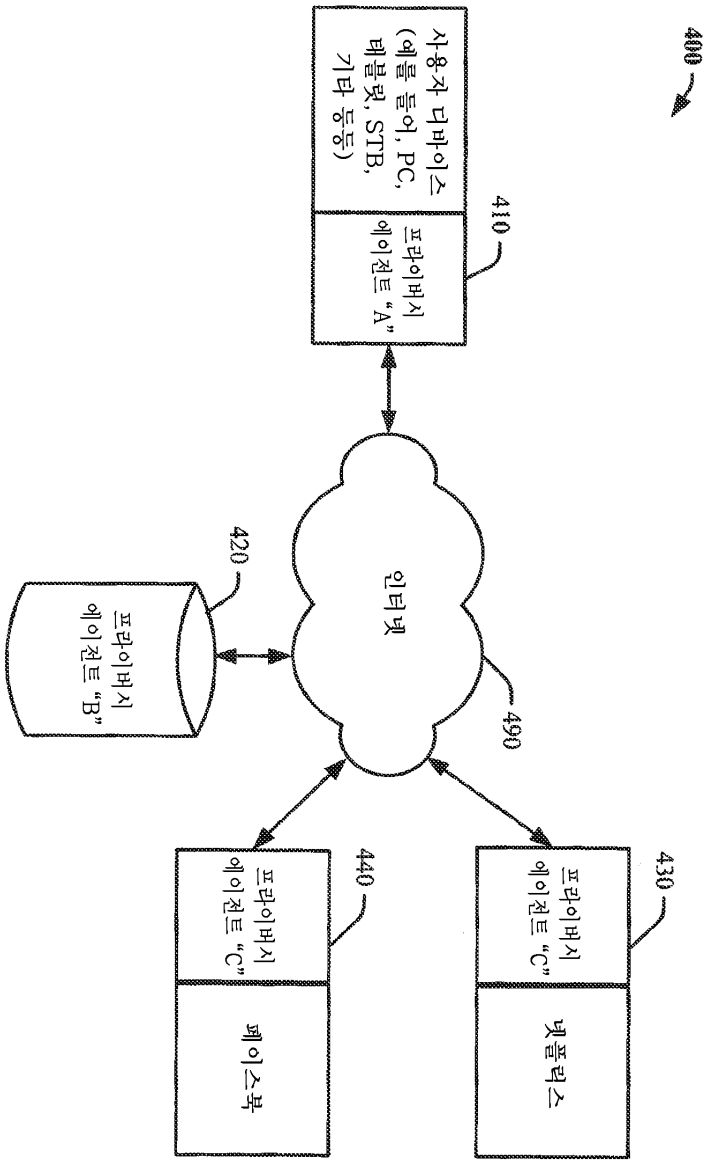
도면2


200
205
시작
210
왜곡 파라미터들에 액세스한다
220
왜곡 파라미터들에 기초하여 확률 측도를 계산한다
230
확률 측도에 기초하여 잡음을 생성한다
240
현재의 공용 데이터에 잡음을 추가한다
250
데이터를 릴리즈한다
299
종료

도면3


300
310
데이터(S, X)를 릴리즈하는 "공용 사용자들"
320
통계 수집 모듈
330
가산성 잡음 생성기
340
프라이버시 보호 모듈 (Y = X + N)
380
프라이버시 에이전트
360
"사적 사용자들"
X
Y
350
서비스 제공자

도면4


400
사용자 디바이스
(예를 들어, PC,
태블릿, STB,
기타 등등)
프라이버시
에이전트 "A"
410
인터넷
490
420
프라이버시
에이전트 "B"
프라이버시
에이전트 "C"
440
페이스북
프라이버시
에이전트 "C"
430
넷플릭스