



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년10월14일
(11) 등록번호 10-1663250
(24) 등록일자 2016년09월29일

(51) 국제특허분류(Int. Cl.)
H04L 12/58 (2006.01) H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 51/046 (2013.01)
H04L 9/0838 (2013.01)
(21) 출원번호 10-2015-0095701
(22) 출원일자 2015년07월06일
심사청구일자 2015년07월06일
(30) 우선권주장
1020150071737 2015년05월22일 대한민국(KR)
(56) 선행기술조사문헌
KR101489447 B1*
KR1020150010571 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
윤지원
서울특별시 동작구 사당로20길 119, 101동 309호 (사당동, 르메이에르)
김주임
서울특별시 은평구 연서로 149, 101동 2102호 (갈현동, 동광갈현베르빌)
(74) 대리인
특허법인엠에이피에스

전체 청구항 수 : 총 13 항

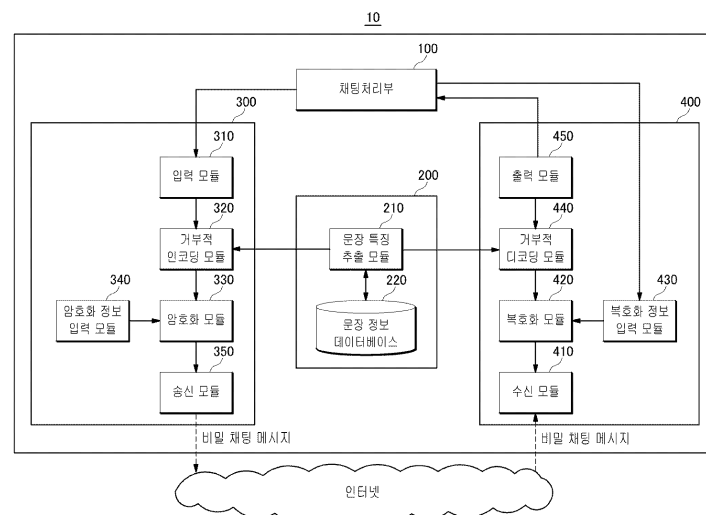
심사관 : 김대성

(54) 발명의 명칭 거부적 암호화를 이용한 비밀 채팅 장치 및 그 방법

(57) 요약

거부적 암호화를 이용한 비밀 채팅 제공 시, 둘 이상의 사용자가 참여하는 채팅창에서 채팅 메시지를 입력받고, 기설정된 데이터 집합 내 문장들에 대해 확률적 언어 모델을 적용하여 생성한 매핑 정보에 기초하여 채팅 메시지를 거부적 인코딩 처리하고, 거부적 인코딩의 결과 데이터를 암호화 키를 사용하여 암호화하고, 암호화한 채팅 메시지를 채팅창에 참여한 다른 사용자의 채팅 장치로 전송되되, 암호화한 채팅 메시지는 다른 사용자의 채팅 장치에서 확률적 언어 모델에 기반한 거부적 디코딩 및 암호화에 대응된 복호화 처리되며, 암호화 키에 대응된 진짜 복호화 키로 복호화할 경우 원래 채팅 메시지와 동일한 채팅 메시지로 복호화되고, 진짜 복호화 키가 아닌 다른 복호화 키로 복호화할 경우 원래 채팅 메시지와 상이한 채팅 메시지로 복호화된다.

대표도



이 발명을 지원한 국가연구개발사업

과제고유번호 IITP-2015-H8501-15-1003

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 대학ICT연구센터육성지원사업

연구과제명 제어시스템 보안 연구

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2015.01.01 ~ 2015.12.31

명세서

청구범위

청구항 1

거부적 암호화를 이용한 비밀 채팅 장치에 있어서,

기설정된 데이터 집합 내 문장들에 대해 확률적 언어 모델(probabilistic language model)을 적용하여 생성한 매핑 정보를 저장하는 문장 정보 처리부;

둘 이상의 사용자가 참여하는 채팅창을 생성하고, 상기 채팅창에서 입력된 채팅 메시지를 채팅 표시 영역에 디스플레이하는 채팅 처리부; 및

상기 입력된 채팅 메시지를 상기 매핑 정보에 기초하여 기설정된 거부적 인코딩을 처리하고, 상기 거부적 인코딩의 결과 데이터를 암호화 키로 암호화한 채팅 메시지를 상기 채팅창에 참여한 다른 사용자의 채팅 장치로 전송하는 메시지 송신부를 포함하며,

상기 채팅 처리부는 상기 채팅창과 별도로 상기 입력된 채팅 메시지의 암호화에 사용할 암호화 키를 입력 받는 인터페이스창을 생성하여 제 1 입력 인터페이스를 제공하고,

상기 메시지 송신부는 상기 제 1 입력 인터페이스를 통해 입력된 암호화 키를 사용하여 상기 암호화를 처리하고,

상기 암호화한 채팅 메시지는,

상기 다른 사용자의 채팅 장치에서 상기 확률적 언어 모델에 기반한 거부적 디코딩 및 상기 암호화에 대응된 복호화 처리되며, 상기 암호화 키에 대응된 진짜 복호화 키로 복호화할 경우 상기 입력된 채팅 메시지와 동일한 채팅 메시지로 복원되고, 상기 진짜 복호화 키가 아닌 다른 복호화 키로 복호화할 경우 상기 입력된 채팅 메시지와 상이한 채팅 메시지로 복원되고,

상기 다른 사용자의 채팅 장치에서는, 수신한 채팅 메시지의 복호화에 사용할 복호화 키를 입력하도록 하는 제 2 입력 인터페이스가 제공되되,

상기 다른 사용자의 채팅 장치에 사전에 약속된 상기 진짜 복호화키가 저장되어 있는 경우 상기 복호화 처리 시 상기 기저장된 진짜 복호화키가 자동으로 입력되는 거부적 암호화를 이용한 비밀 채팅 장치.

청구항 2

제 1 항에 있어서,

상기 문장 정보 처리부는,

기설정된 문장 특징 추출 알고리즘을 적용하여 상기 데이터 집합에서 문장 별 구성상 특징 요소를 추출하고,

상기 특징 요소에 대해 상기 데이터 집합 내에서의 확률을 할당하는 상기 확률적 언어 모델에 기반하여 상기 특징 요소 별 누적 분포를 산출하고,

상기 누적 분포 별로 대응된 이진 코드 정보를 매핑하여 상기 매핑 정보를 생성하는 거부적 암호화를 이용한 비밀 채팅 장치.

청구항 3

제 1 항에 있어서,

상기 메시지 송신부는,

상기 거부적 인코딩 시 평문(plain text) 형태의 상기 입력된 채팅 메시지를 상기 매핑 정보에 따라 이진 데이

터(binary data)로 변환하는 거부적 암호화를 이용한 비밀 채팅 장치.

청구항 4

제 1 항에 있어서,

다른 사용자의 채팅 장치로부터 상기 거부적 인코딩 및 상기 암호화 처리된 채팅 메시지를 수신하고, 상기 수신한 채팅 메시지를 복호화 키를 사용하여 복호화하고, 상기 복호화의 결과 데이터를 상기 매핑 정보에 기초하여 거부적 디코딩 처리하는 메시지 수신부를 더 포함하며,

상기 채팅 처리부는,

상기 거부적 디코딩 처리된 채팅 메시지를 해당 채팅창의 채팅 표시 영역에 표시하는 거부적 암호화를 이용한 비밀 채팅 장치.

청구항 5

제 4 항에 있어서,

상기 메시지 수신부는,

상기 수신한 채팅 메시지를 상기 암호화에 대응된 복호화를 통해 이진 데이터(binary data)로 복호화하고, 상기 거부적 디코딩 시 상기 이진 데이터를 상기 매핑 정보에 기초하여 평문(plain text) 형태의 채팅 메시지로 변환하는 거부적 암호화를 이용한 비밀 채팅 장치.

청구항 6

제 5 항에 있어서,

상기 복호화 키로서 상기 진짜 복호화 키가 아닌 다른 복호화 키가 사용된 경우, 상기 수신한 채팅 메시지는 상기 거부적 디코딩을 통해 평문 형태이되 상기 입력된 채팅 메시지와 의미 및 형태가 다른 가짜 채팅 메시지로 변환되는 거부적 암호화를 이용한 비밀 채팅 장치.

청구항 7

제 4 항에 있어서,

상기 채팅 처리부는,

상기 수신한 채팅 메시지의 복호화에 사용할 복호화 키를 입력받는 제 3 입력 인터페이스를 제공하며,

상기 메시지 수신부는 상기 제 3 입력 인터페이스를 통해 입력된 복호화 키를 사용하여 상기 복호화를 처리하는 거부적 암호화를 이용한 비밀 채팅 장치.

청구항 8

비밀 채팅 장치를 통한 거부적 암호화를 이용한 비밀 채팅 방법에 있어서,

개설된 채팅창에서 입력된 채팅 메시지를 수신하는 단계;

기설정된 데이터 집합 내 문장들에 대해 확률적 언어 모델(probabilistic language model)을 적용하여 생성한 매핑 정보에 기초하여, 상기 입력된 채팅 메시지를 거부적 인코딩 처리하는 단계;

상기 입력된 채팅 메시지의 암호화에 사용할 암호화 키를 입력받는 제 1 입력 인터페이스를 제공하는 단계;

상기 거부적 인코딩의 결과 데이터를 상기 제 1 입력 인터페이스를 통해 입력된 암호화 키를 사용하여 암호화하

는 단계; 및

상기 암호화한 채팅 메시지를 상기 채팅창에 참여한 다른 사용자의 채팅 장치로 전송하는 단계를 포함하며,

상기 암호화한 채팅 메시지는,

상기 다른 사용자의 채팅 장치에서 상기 확률적 언어 모델에 기반한 거부적 디코딩 및 상기 암호화에 대응된 복호화 처리되며, 상기 암호화 키에 대응된 진짜 복호화 키로 복호화할 경우 상기 입력된 채팅 메시지와 동일한 채팅 메시지로 복원되고, 상기 진짜 복호화 키가 아닌 다른 복호화 키로 복호화할 경우 상기 입력된 채팅 메시지와 상이한 채팅 메시지로 복원되며,

상기 다른 사용자의 채팅 장치에서는, 수신한 채팅 메시지의 복호화에 사용할 복호화 키를 입력하도록 하는 제 2 입력 인터페이스가 제공되며,

상기 다른 사용자의 채팅 장치에 사전에 약속된 상기 진짜 복호화키가 저장되어 있는 경우 상기 복호화 처리 시 상기 기저장된 진짜 복호화키가 자동으로 입력되는 거부적 암호화를 이용한 비밀 채팅 방법.

청구항 9

제 8 항에 있어서,

상기 입력된 채팅 메시지를 거부적 인코딩 처리하는 단계 이전에,

기설정된 문장 특징 추출 알고리즘을 적용하여 상기 데이터 집합에서 문장 별 구성상 특징 요소를 추출하는 단계;

상기 특징 요소에 대해 상기 데이터 집합 내에서의 확률을 할당하는 상기 확률적 언어 모델에 기반하여 상기 특징 요소 별 누적 분포를 산출하는 단계; 및

상기 누적 분포 별로 대응된 이진 코드 정보를 매핑하여 상기 매핑 정보를 생성하는 단계를 더 포함하는 거부적 암호화를 이용한 비밀 채팅 방법.

청구항 10

제 9 항에 있어서,

상기 입력된 채팅 메시지를 거부적 인코딩 처리하는 단계는,

평문(plain text) 형태의 상기 입력된 채팅 메시지를 상기 매핑 정보에 따라 이진 데이터(binary data)로 변환하는 거부적 암호화를 이용한 비밀 채팅 방법.

청구항 11

삭제

청구항 12

비밀 채팅 장치를 통한 거부적 암호화를 이용한 비밀 채팅 방법에 있어서,

개설된 채팅창에 참여 중인 다른 사용자의 채팅 장치로부터 기설정된 확률적 언어 모델에 기반한 거부적 인코딩 및 기설정된 포맷으로 암호화 처리된 채팅 메시지를 수신하는 단계;

상기 수신한 채팅 메시지의 복호화에 사용할 복호화 키를 입력받는 입력 인터페이스를 제공하는 단계;

상기 수신한 채팅 메시지를 상기 입력 인터페이스를 통해 입력된 복호화 키를 사용하여 복호화하는 단계;

상기 복호화의 결과 데이터를 상기 확률적 언어 모델에 기반한 거부적 디코딩 처리하는 단계; 및

상기 거부적 디코딩의 결과인 채팅 메시지를 상기 채팅창의 채팅 표시 영역에 디스플레이하는 단계를 포함하며,

상기 수신한 채팅 메시지는,

암호화 시 사용한 암호화 키에 대응된 진짜 복호화 키로 복호화할 경우 원본 채팅 메시지와 동일한 채팅 메시지로 복원되고, 상기 진짜 복호화 키가 아닌 다른 복호화 키로 복호화할 경우 상기 원본 채팅 메시지와 상이한 채팅 메시지로 복원되고,

사전에 약속된 상기 진짜 복호화키가 기저장되어 있는 경우, 상기 복호화하는 단계는 상기 기저장된 진짜 복호화키를 자동으로 입력하여 복호화를 처리하는 거부적 암호화를 이용한 비밀 채팅 방법.

청구항 13

제 12 항에 있어서,

상기 거부적 디코딩 처리하는 단계 이전에,

기설정된 데이터 집합 내 문장들에 대해 기설정된 문장 특징 추출 알고리즘을 적용하여 문장 별 구성상 특징 요소를 추출하는 단계;

상기 특징 요소에 대해 상기 데이터 집합 내에서의 확률을 할당하는 상기 확률적 언어 모델에 기반하여 상기 특징 요소 별 누적 분포를 산출하는 단계; 및

상기 누적 분포 별로 대응된 이진 코드 정보를 매핑하여 매핑 정보를 생성하는 단계를 더 포함하는 거부적 암호화를 이용한 비밀 채팅 방법.

청구항 14

제 13 항에 있어서,

상기 거부적 디코딩 처리하는 단계는,

상기 수신한 채팅 메시지를 상기 복호화 처리한 결과인 이진 데이터(binary data)를 상기 매핑 정보에 따라 평문(plain text) 형태의 채팅 메시지로 변환하는 거부적 암호화를 이용한 비밀 채팅 방법.

청구항 15

삭제

발명의 설명

기술 분야

[0001] 본 발명은 채팅 시스템 및 방법에 관한 것으로, 보다 상세하게는 거부적 암호화(deniable encryption) 기법을 적용하여 비밀 채팅 메시지를 통신하는 비밀 채팅 장치 및 그 방법에 관한 것이다.

배경 기술

[0002] 일반적으로 암호화 시스템을 통한 송신자와 수신자 간에 암호화된 메시지 송수신 시, 불가피한 상황으로 제 3 자에게 메시지의 암호화 키가 공개될 수 있다. 이러한 경우, 제 3 자에게 가짜 키를 제공하여 원래의 메시지가 아닌 가짜 메시지가 복호화되도록 함으로써 메시지의 비밀성을 보장할 수 있다. 이처럼 진짜 키로 메시지를 복호화할 경우 진짜 메시지가 복호화되나, 가짜 키로 메시지를 복호화할 경우 진짜 메시지와는 다른 가짜 메시지가 복호화되도록 하는 기술을 거부적 암호화(deniable encryption)라고 한다.

[0003] 이와 관련하여, Ari Juels가 2014년 발표한 논문(제목: “Honey Encryption: Security Beyond the Brute-Force Bound”)에는 잘못된 비밀 키를 입력하더라도 정상적인 평문인 것처럼 보이게하는 인코딩 및 디코딩 기법이 개시되어 있다. 그러나, 이러한 종래의 거부적 암호화 기법은 비트(bit)나 정수(integer)에만 한정적으로 적용되는 것이다. 또한, 종래의 거부적 암호화 기법은 너무 많은 연산과 비효율적인 성능으로 인해 실제로는 널리 이

용되지 않고 있다. 따라서 효율적이면서 실생활에 이용 가능한 거부적 암호화 시스템이 필요하다.

[0004] 한편, 종래의 채팅 시스템은 메시지의 비밀성을 보장하기 위하여, 단순히 송신자가 메시지를 암호화하여 수신자에게 전송하면 수신자가 이를 복호화하여 평문의 형태로 읽어들이는 형태를 제공하였다.

[0005] 이와 관련하여, 대한민국 공개 특허 제 10-2001-0016233 호(발명의 명칭: 암호화 채팅시스템)에서는, 서버 사이드 암호화 채팅 시스템에서 채팅 방의 키를 네트워크로 안전하게 교환하는 방법으로서, 서버가 채팅방 구성원의 공개키로 채팅방의 암호화 키를 암호화하여 클라이언트에게 네트워크를 통해 전송하여, 채팅에 참가하고 있는 사용자가 암호화된 채팅방의 키를 수신하여 자신의 개인키로 암호화된 채팅방 키를 복호화하는 방법을 개시하고 있다.

[0006] 이러한 종래 기술에 따르면, 메시지를 복호화하는 과정에서 잘못된 비밀 정보를 사용하게 되면 결과값으로 말이 되지 않는 평문이 출력될 수 있다. 이 경우, 비정상적 수신자는 자신이 사용한 비밀 정보가 잘못된 것임을 인지할 수 있게 되고, 비밀 정보를 사용하여 진짜 평문을 얻을 때까지 반복적으로 복호화를 시도할 수 있다는 문제점이 있다. 더불어, 앞서 설명한 바와 같이 종래의 거부적 암호화 기술과 관련된 인코딩 및 디코딩 방식들은 실생활에 적용 가능한 형태의 구현 방법을 제시하지는 못하고 있다. 따라서, 대중적인 온라인 서비스인 채팅 시스템에 거부적 암호화 기법을 적용하여 사용자에게 새로운 형태의 안전한 온라인 통신 서비스를 제공할 수 있는 방법이 필요하다.

발명의 내용

해결하려는 과제

[0007] 본 발명의 실시예는 채팅 시 송신자가 수신자에게 전달한 채팅 메시지에 거부적 인코딩 및 디코딩 기법을 적용하여, 수신한 채팅 메시지에 대해 잘못된 비밀 정보로 복호화한 경우에도 말이 되는 문장을 얻을 수 있도록 하는 거부적 암호화를 이용한 비밀 채팅 장치 및 방법을 제공하고자 한다.

[0008] 다만, 본 실시예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제로 한정되지 않으며, 또 다른 기술적 과제들이 존재할 수 있다.

과제의 해결 수단

[0009] 상기와 같은 기술적 과제를 달성하기 위한 본 발명의 일 측면에 따른, 거부적 암호화를 이용한 비밀 채팅 장치는, 기설정된 데이터 집합 내 문장들에 대해 확률적 언어 모델(probabilistic language model)을 적용하여 매핑 정보를 생성하고, 상기 생성한 매핑 정보를 저장하는 문장 정보 처리부; 둘 이상의 사용자가 참여하는 채팅창을 생성하고, 상기 채팅창에서 입력된 채팅 메시지를 채팅 표시 영역에 디스플레이하는 채팅 처리부; 및 상기 입력된 채팅 메시지를 상기 매핑 정보에 기초하여 기설정된 거부적 인코딩을 처리하고, 상기 거부적 인코딩의 결과 데이터를 암호화 키로 암호화한 채팅 메시지를 상기 채팅창에 참여한 다른 사용자의 채팅 장치로 전송하는 메시지 송신부를 포함한다. 이때, 상기 암호화한 채팅 메시지는, 상기 다른 사용자의 채팅 장치에서 상기 확률적 언어 모델에 기반한 거부적 디코딩 및 상기 암호화에 대응된 복호화 처리되며, 상기 암호화 키에 대응된 진짜 복호화 키로 복호화할 경우 상기 입력된 채팅 메시지와 동일한 채팅 메시지로 복원되고, 상기 진짜 복호화 키가 아닌 다른 복호화 키로 복호화할 경우 상기 입력된 채팅 메시지와 상이한 채팅 메시지로 복원된다.

[0010] 그리고 본 발명의 다른 측면에 따른, 비밀 채팅 장치를 통한 거부적 암호화를 이용한 비밀 채팅 방법은, 개설된 채팅창에서 입력된 채팅 메시지를 수신하는 단계; 기설정된 데이터 집합 내 문장들에 대해 확률적 언어 모델(probabilistic language model)을 적용하여 생성한 매핑 정보에 기초하여 상기 입력된 채팅 메시지를 거부적 인코딩 처리하는 단계; 상기 거부적 인코딩의 결과 데이터를 암호화 키를 사용하여 암호화하는 단계; 및 상기 암호화한 채팅 메시지를 상기 채팅창에 참여한 다른 사용자의 채팅 장치로 전송하는 단계를 포함한다. 이때, 상기 암호화한 채팅 메시지는, 상기 다른 사용자의 채팅 장치에서 상기 확률적 언어 모델에 기반한 거부적 디코딩 및 상기 암호화에 대응된 복호화 처리되며, 상기 암호화 키에 대응된 진짜 복호화 키로 복호화할 경우 상기 입력된 채팅 메시지와 동일한 채팅 메시지로 복원되고, 상기 진짜 복호화 키가 아닌 다른 복호화 키로 복호화할 경우 상기 입력된 채팅 메시지와 상이한 채팅 메시지로 복원된다.

[0011] 또한, 본 발명의 또 다른 측면에 따른, 비밀 채팅 장치를 통한 거부적 암호화를 이용한 비밀 채팅 방법은, 개설된 채팅창에 참여 중인 다른 사용자의 채팅 장치로부터 기설정된 확률적 언어 모델에 기반한 거부적 인코딩 및 기설정된 포맷으로 암호화 처리된 채팅 메시지를 수신하는 단계; 상기 수신한 채팅 메시지를 복호화 키를 사용

하여 복호화하는 단계; 상기 복호화의 결과 데이터를 상기 확률적 언어 모델에 기반한 거부적 디코딩 처리하는 단계; 및 상기 거부적 디코딩의 결과인 채팅 메시지를 상기 채팅창의 채팅 표시 영역에 디스플레이하는 단계를 포함한다. 이때, 상기 수신한 채팅 메시지는, 상기 암호화 시 사용한 암호화 키에 대응된 진짜 복호화 키로 복호화할 경우 원본 채팅 메시지와 동일한 채팅 메시지로 복원되고, 상기 진짜 복호화 키가 아닌 다른 복호화 키로 복호화할 경우 상기 원본 채팅 메시지와 상이한 채팅 메시지로 복원된다.

발명의 효과

[0012] 전술한 본 발명의 과제 해결 수단에 의하면, 비밀 채팅 장치의 사용자 측에서 자신의 비밀 정보(즉, 채팅 메시지)를 추측하여 복호화하려는 제 3 자의 시도를 방지할 수 있다. 즉, 암호화 키에 대응된 진짜 복호화 키가 아닌 다른 복호화 키로 비밀 채팅 메시지를 복호화할 경우, 평문 형태이되 원본 채팅 메시지와는 의미 또는 형태가 상이한 채팅 메시지가 복원된다. 이에 따라, 비정상적 수신자인 제 3 자에게 비밀 채팅 메시지가 노출되어 제 3 자가 채팅 메시지의 내용을 확인하더라도 원본과 다른 내용을 확인하도록 함으로써 비밀을 유지할 수 있다. 또한, 진짜 복호화 키로 복원된 채팅 메시지 또한 의미있어 보이는 평문 형태를 갖도록 복호화함으로써, 진짜 채팅 메시지가 원본과 다른 내용인 것을 판별하기 어렵게 하여 제 3 자의 복호화 재시도를 방지할 수 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 일 실시예에 따른 비밀 채팅 장치의 구성을 나타낸 블록도이다.

도 2는 본 발명의 일 실시예에 따른 비밀 채팅 메시지의 암호화를 통한 비밀 채팅 방법을 설명하기 위한 순서도이다.

도 3은 본 발명의 일 실시예에 따른 비밀 채팅 메시지의 복호화를 통한 비밀 채팅 방법을 설명하기 위한 순서도이다.

도 4a 내지 도 4c는 본 발명의 일 실시예에 따른 비밀 채팅 장치를 통해 제공되는 채팅창의 일례들을 나타낸 도면이다.

도 5는 본 발명의 일 실시예에 따른 거부적 인코딩 및 디코딩에 사용되는 확률적 언어 모델 기반의 문장 정보 데이터베이스의 일례를 나타낸 도면이다.

도 6은 본 발명의 일 실시예에 따른 확률적 언어 모델 기반의 문장 정보 데이터베이스의 다른 예를 나타낸 도면이다.

도 7은 본 발명의 일 실시예에 따른 거부적 디코딩 결과의 일례를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0014] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0015] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0016] 아래에서는 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 첨부된 도면을 참조하여 본 발명의 실시예를 상세히 설명한다.

[0017] 도 1은 본 발명의 일 실시예에 따른 비밀 채팅 장치의 구성을 나타낸 블록도이다.

[0018] 도 1에 도시한 본 발명의 일 실시예에 따른 비밀 채팅 장치(10)는, 채팅에 참여 중인 사용자 간에 거부적 암호화 기법을 적용하여 암호화된 채팅 메시지(이하, "비밀 채팅 메시지"라고 지칭함)를 송수신한다. 본 발명에 적용되는 거부적 암호화 기법은 정확한 비밀 정보(즉, 암호화 키에 대응된 진짜 복호화 키)를 사용하지 않을 경우, 일반적인 평문(plain text) 형태의 메시지 출력은 가능하나 원래의 비밀 메시지와는 다른 의미를 갖는 내용(또는 형태)의 진짜 채팅 메시지가 출력되도록 하는 암호화 기법이다.

[0019] 이때, 비밀 채팅 장치(10)는 채팅 서비스 서버(미도시)를 포함하는 채팅 시스템(미도시)의 일 구성으로 포함될

수 있으며, 채팅 시스템(미도시)의 각 구성요소들은 네트워크를 통해 서로 연결될 수 있다. 참고로, 본 발명에 적용될 수 있는 네트워크는 단말들 및 서버들과 같은 각각의 노드 상호 간에 정보 교환이 가능한 연결 구조를 의미하는 것으로, 이러한 네트워크(network)의 일 예에는 3GPP(3rd Generation Partnership Project) 네트워크, LTE(Long Term Evolution) 네트워크, WIMAX(World Interoperability for Microwave Access) 네트워크, 인터넷(Internet), LAN(Local Area Network), Wireless LAN(Wireless Local Area Network), WAN(Wide Area Network), PAN(Personal Area Network), 블루투스(Bluetooth) 네트워크, 위성 방송 네트워크, 아날로그 방송 네트워크, DMB(Digital Multimedia Broadcasting) 네트워크 등이 포함되나 이에 한정되지는 않는다.

[0020] 또한, 비밀 채팅 장치(10)는 채팅 시스템(미도시)에 접속할 수 있는 사용자 단말기일 수 있으며, 예를 들어 휴대성과 이동성이 보장되는 무선 통신 장치, 즉 PCS(Personal Communication System), GSM(Global System for Mobile communications), PDC(Personal Digital Cellular), PHS(Personal Handyphone System), PDA(Personal Digital Assistant), IMT(International Mobile Telecommunication)-2000, CDMA(Code Division Multiple Access)-2000, W-CDMA(W-Code Division Multiple Access), Wibro(Wireless Broadband Internet) 단말 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다. 특히, 비밀 채팅 장치(10)는 휴대용 단말기에 인터넷 통신과 정보 검색 등 컴퓨터 지원 기능을 추가한 지능형 단말기로서, 사용자가 원하는 다수의 응용 프로그램(즉, 애플리케이션)을 설치하여 실행할 수 있는 스마트 폰(smart phone)일 수 있다. 이외에도 비밀 채팅 장치(10)는 PC 등과 같이 채팅 서비스 서버(미도시)와 유/무선 통신을 통해 접속할 수 있는 사용자 단말일 수도 있다.

[0021] 이하의 설명에서 비밀 채팅 장치(10)가 다른 비밀 채팅 장치로 비밀 채팅 메시지를 전송하거나 다른 비밀 채팅 장치로부터 비밀 채팅 메시지를 수신하는 것은, 비밀 채팅 장치 간에 비밀 채팅 메시지가 직접 송수신되는 경우 또는 비밀 채팅 장치(10)가 채팅 서비스 서버(미도시)로 비밀 채팅 메시지를 전송하여 목적지(즉, 상대 비밀 채팅 장치)로 전달하는 경우를 모두 포함할 수 있다.

[0022] 한편, 본 발명의 일 실시예에 따른 비밀 채팅 장치(10)의 적어도 하나의 구성은 채팅 서비스 서버(미도시) 또는 채팅 프로그램이 탑재된 사용자 단말(미도시)과 연동된 별도의 비밀 채팅 서비스 서버로서 구성될 수 있다. 이 처럼, 비밀 채팅 장치(10)가 서버로서 구현될 경우, 비밀 채팅 장치(10)는 사용자 단말(미도시)로부터 채팅 메시지가 수신되면 거부적 암호화 기법을 적용하여 해당 채팅 메시지를 암호화/복호화하고, 암호화/복호화된 채팅 메시지를 채팅 서비스 서버(미도시)를 통해 또는 상대 사용자 단말(미도시)로 전송할 수 있다. 예를 들어, 아래에서 설명할 문장 정보 처리부(200), 메시지 송신부(300) 및 메시지 수신부(400) 중 적어도 하나의 구성이 서버(즉, 비밀 채팅 서비스 서버) 형태로써 구현될 수 있다. 이러한 비밀 채팅 서비스 서버는 사용자 단말(미도시)로부터 채팅 메시지 및 목적지 정보를 획득하고, 채팅 메시지를 거부적 암호화 기법을 적용한 암호화 또는 복호화 처리하여 목적지로 제공할 수 있다.

[0023] 구체적으로, 도 1에 도시한 바와 같이, 본 발명의 일 실시예에 따른 비밀 채팅 장치(10)는, 채팅 처리부(100), 문장 정보 처리부(200), 메시지 송신부(300) 및 메시지 수신부(400)를 포함한다.

[0024] 이때, 비밀 채팅 장치(10)의 메시지 송신부(300) 및 메시지 수신부(400)는 하나의 장치에 함께 구현되거나, 각각 별도의 장치(즉, 송신 장치 및 수신 장치)로 구성될 수도 있다. 또한, 문장 정보 처리부(200)는 메시지 송/수신부(300, 400)과 함께 하나의 장치 내에 구현되거나, 별도의 장치로 각각 구성될 수 있다.

[0025] 채팅 처리부(100)는 둘 이상의 사용자가 참여하는 채팅창을 생성하고, 채팅창에서 입력된 채팅 메시지를 채팅 표시 영역에 디스플레이한다. 참고로, 채팅 처리부(100)는 비밀 채팅 장치(10)를 통한 채팅이 요청되면 직접 채팅창을 생성하여 개설할 수 있으며, 연동된 채팅 서비스 서버(미도시)에 접속하여 채팅 서비스 서버가 생성한 채팅창을 비밀 채팅 장치(10) 상에서 활성화되도록 개설할 수도 있다. 이때, 채팅 처리부(100)는 터치 패드, 키보드 등의 입력 장치를 통해 사용자가 입력한 채팅 메시지를 수신하며, 입력된 채팅 메시지를 디스플레이함과 동시에 메시지 송신부(300)로 전달한다.

[0026] 또한, 채팅 처리부(100)는 채팅창에 참여 중인 다른 사용자의 채팅 장치(즉, 다른 비밀 채팅 장치)로부터 수신된 채팅 메시지를 채팅창에 디스플레이한다. 이때, 다른 사용자의 채팅 장치로부터 수신된 채팅 메시지는 거부적 암호화를 적용하여 암호화된 채팅 메시지이다. 이에 따라, 채팅 처리부(100)는 암호화된 채팅 메시지를 메시지 수신부(400)가 거부적 디코딩 및 복호화 처리한 결과인 채팅 메시지를 수신하여 채팅창에 디스플레이한다.

[0027] 한편, 채팅 처리부(100)는 채팅창에서 입력된 채팅 메시지를 암호화하는데 사용될 암호화 키 또는 다른 사용자의 채팅 장치로부터 수신된 채팅 메시지를 복호화하는데 사용될 복호화 키를 입력받는 인터페이스를 제공한다.

이때, 채팅 처리부(100)는 채팅창 내 채팅 표시 영역과 구분된 영역에 암호화 키 또는 복호화 키를 입력할 수 있는 입력 인터페이스를 출력할 수 있다. 또한, 채팅 처리부(100)는 채팅창과 별도로 암호화 키 또는 복호화 키를 입력할 수 있도록 하는 입력 인터페이스창을 생성하여, 비밀 채팅 장치(10)의 화면 상에 디스플레이 하는 것도 가능하다.

[0028] 이상, 본 발명의 일 실시예에서는 채팅 처리부(100)가 제공하는 인터페이스를 통해 사용자(즉, 송신자와 수신자)가 암호화 키 또는 복호화 키를 직접 입력하는 것을 설명하였다. 그런데 본 발명의 다른 실시예에 따른 비밀 채팅 장치(10)는 정상적인 사용자 간에 비밀 채팅 메시지에 적용할 암호화 키 및 복호화 키를 제공하는 구성을 더 포함할 수 있다. 즉, 사용자가 상기 인터페이스를 통해 암호화 키 또는 복호화 키를 직접 입력하지 않더라도, 비밀 채팅 장치(10)가 비밀 채팅 시 사전에 설정된 암호화 키 및 복호화 키를 자동으로 적용하는 것도 가능하다. 이때, 비밀 채팅 장치(10)는 암호화 키 및 암호화 키에 대응되는 복호화 키(즉, 진짜 복호화 키)를 사전에 약속된 정상 사용자 간에 각각 저장하고 있을 수 있다. 또한, 송신자의 비밀 채팅 장치(10)가 사전에 설정되거나 새롭게 생성된 암호화 키에 대응된 복호화 키의 정보를 정상 수신자(즉, 사전에 약속된 수신자)의 비밀 채팅 장치로 전송하여, 상대의 비밀 채팅 장치에서 사용 및 저장되도록 할 수 있다. 즉, 진짜 채팅 메시지를 송수신할 사용자들 간에는 진짜 비밀 키(암호화 키 및 복호화 키)가 미리 약속되어 있어, 채팅 시 자동으로 거부적 암호화 및 복호화에 적용될 수 있다. 이처럼, 비밀 채팅 장치(10)가 채팅 처리 시 자동으로 진짜 비밀 키를 적용하여 암호화 및 복호화를 처리함으로써, 채팅 메시지가 발생될 때마다 매번 채팅 처리부(100)가 제공한 인터페이스를 통해 사용자가 직접 비밀 키를 입력할 필요가 없어 편리하며 신속하게 비밀 채팅을 제공할 수 있다. 반면, 비정상적으로 비밀 채팅 메시지를 획득한 사용자의 채팅 장치에는 사전에 약속된 진짜 비밀 키 정보가 없으며, 비밀 채팅 메시지를 복호화하기 위해서는 채팅 처리부(100)가 제공하는 인터페이스를 통해 사용자가 임의로 입력하는 가짜 복호화 키를 사용하게 된다. 또한, 송신자가 비밀 채팅 메시지를 원본 그대로 제공하고 싶어하지 않는 수신자, 즉 사전에 송신자가 진짜 비밀 키를 제공하도록 설정되지 않은 수신자의 비밀 채팅 장치(10)는, 송신자의 비밀 채팅 장치로부터 가짜 복호화 키의 정보를 수신할 수 있으며, 이러한 가짜 복호화 키를 복호화에 자동으로 적용할 수 있다. 이러한 경우 수신자의 비밀 채팅 장치(10) 또한 가짜 복호화 키를 사용함으로써 원본 채팅 메시지와는 상이한 채팅 메시지가 제공된다.

[0029] 문장 정보 처리부(200)는 기설정된 데이터 집합 내 문장들에 대해 확률적 언어 모델(probabilistic language model)을 적용하여 매핑 정보를 생성한다. 그리고 문장 정보 처리부(200)는 생성한 매핑 정보를 저장하여 메시지 송신부(300) 및 메시지 수신부(400)로 제공한다.

[0030] 도 1에 도시한 바와 같이, 문장 정보 처리부(200)는 문장 특징 추출 모듈(210) 및 문장 정보 데이터베이스(220)를 포함한다.

[0031] 문장 특징 추출 모듈(210)은 기설정된 문장 특징 추출 알고리즘을 적용하여 기설정된 데이터 집합에서 문장 별 구성상 특징 요소를 추출한다. 본 발명의 일 실시예에 적용되는 데이터 집합은, 존재할 수 있거나 사용 가능한 형태의 임의의 문장들을 수집한 데이터의 집합을 의미한다. 문장 특징 추출 모듈(210)은 수집된 데이터의 집합(즉, 대량의 문장들)을 문장 정보 데이터베이스(220)에 저장한 후, 데이터 집합 내 문장들의 구성상 특징 요소를 추출하여 이를 다시 문장 정보 데이터베이스(220)에 저장한다.

[0032] 그리고 문장 특징 추출 모듈(210)은 문장의 구성상 특징 요소에 대해 데이터 집합 내에서의 확률을 할당하는 확률적 언어 모델에 기반하여 특징 요소 별 누적 분포를 산출한다. 문장 특징 추출 모듈(210)은 누적 분포 별로 대응된 이진 코드(binary code) 정보를 매핑하여 매핑 정보를 생성하고, 생성된 매핑 정보를 문장 정보 데이터베이스(220)에 저장한다.

[0033] 문장 정보 데이터베이스(220)는 수집된 문장 그 자체 및 문장 별 구성상 특징 요소를 저장하는 저장 매체이다. 그리고 문장 정보 데이터베이스(220)는 문장 특징 추출 모듈(210)을 통해 생성된 매핑 정보가 저장되며, 하기에 설명할 메시지 송신부(300) 및 메시지 수신부(400)로 매핑 정보를 제공한다. 이처럼 메시지 송신부(300) 및 메시지 수신부(400)로 제공되는 매핑 정보는, 거부적 암호화를 위한 거부적 인코딩 및 거부적 디코딩의 기준으로 사용된다.

[0034] 메시지 송신부(300)는 채팅 처리부(100)를 통해 채팅창에서 입력된 채팅 메시지를 수신하고, 수신된 채팅 메시지(즉, 원본 채팅 메시지)를 거부적 인코딩 및 암호화 처리하여 비밀 채팅 메시지로 변환하고, 변환된 비밀 채팅 메시지를 다른 사용자의 채팅 장치(즉, 비밀 채팅 장치)로 전송한다. 이때, 메시지 송신부(300)를 통해 전송되는 비밀 채팅 메시지는 암호화된 채팅 메시지로서, 다른 사용자의 채팅 장치에서 확률적 언어 모델에 기반한 거부적 디코딩 및 복호화 처리된다. 이때, 다른 사용자의 채팅 장치에서, 메시지 송신부(300)가 사용한 암호화

호화 키에 대응된 진짜 복호화 키로 비밀 채팅 메시지를 복호화할 경우, 비밀 채팅 메시지는 원본 채팅 메시지와 동일한 채팅 메시지로 복호화된다. 반면, 다른 사용자의 채팅 장치에서, 진짜 복호화 키가 아닌 다른 복호화 키로 복호화할 경우 비밀 채팅 메시지는 원본 채팅 메시지와 상이한 채팅 메시지로 복호화된다.

- [0035] 구체적으로, 도 1에 도시한 바와 같이, 메시지 송신부(300)는 입력 모듈(310), 거부적 인코딩 모듈(320), 암호화 모듈(330), 암호화 정보 입력 모듈(340) 및 송신 모듈(350)을 포함한다.
- [0036] 입력 모듈(310)은 채팅 처리부(100)로부터 채팅창에서 입력된 채팅 메시지(이하, “원본 채팅 메시지”라고 지칭함)를 전달받는다. 그리고 입력 모듈(310)은 전달된 원본 채팅 메시지를 거부적 인코딩 모듈(320)에 입력 가능한 형태로 변경하여 전달한다.
- [0037] 거부적 인코딩 모듈(320)은 수신된 원본 채팅 메시지를 문장 정보 데이터베이스(220)에 저장된 매핑 정보에 기반하여 거부적 인코딩 처리한 후, 암호화 모듈(330)로 전달한다. 이때, 거부적 인코딩 모듈(320)은 평문(plain text) 형태의 원본 채팅 메시지를 매핑 정보에 따라 이진 데이터(binary data)로 변환한다. 이러한 거부적 인코딩 방법에 대해서는 아래 도 5 내지 7을 참조하여 상세히 설명하도록 한다.
- [0038] 암호화 모듈(330)은 거부적 인코딩의 결과 데이터를 기설정된 암호화 키를 사용하여 기설정된 포맷의 암호화를 처리한 후 송신 모듈(350)로 전달한다. 이때, 암호화 모듈(330)은 암호화 정보 입력 모듈(340)로부터 암호화 키를 제공받아 암호화에 사용한다. 참고로, 암호화 모듈(330)이 처리하는 암호화의 포맷은 RSA, AES, DES 등과 같은 암호 알고리즘을 사용할 수 있으며, 이에 한정되지 않는다.
- [0039] 암호화 정보 입력 모듈(340)은 설정된 암호화 키를 암호화 모듈(330)로 제공한다. 이때, 암호화 정보 입력 모듈(340)은 채팅 처리부(100)가 제공한 인터페이스를 통해 입력된 암호화 키를 수신하여 암호화 모듈(330)로 전달할 수 있다.
- [0040] 또한, 암호화 정보 입력 모듈(340)은 사전에 상대 비밀 채팅 장치와 약속되어 저장되어 있던 암호화 키를 암호화 모듈(330)로 전달할 수도 있다. 이때, 암호화 정보 입력 모듈(340)은 비밀 채팅 메시지를 전송할 대상인 적어도 하나의 비밀 채팅 장치의 정보 및 각 비밀 채팅 장치 별로 암호화 키를 매칭하여 저장해둘 수 있다. 이에 따라, 암호화 정보 입력 모듈(340)은 암호화 모듈(330)에서 암호화 처리하는 채팅 메시지의 목적지 정보를 확인하고, 목적지 정보에 따른 비밀 채팅 장치의 정보에 매칭된 암호화 키를 암호화 모듈(330)로 제공할 수 있다.
- [0041] 또한, 암호화 정보 입력 모듈(340)은 암호화 키 별로 대응된 복호화 키(진짜 복호화 키)의 정보를 송신 모듈(350)로 제공하여, 사전에 약속된 수신자의 비밀 채팅 장치로 전송할 수 있다. 이때, 암호화 정보 입력 모듈(340)은 진짜 복호화 키를 제공하도록 약속된 수신자의 비밀 채팅 장치의 정보 및 가짜 복호화 키를 제공할 수신자의 비밀 채팅 장치의 정보를 구분하여 관리할 수 있다. 참고로, 가짜 복호화 키는 특정 값으로 한정되지 않으며 진짜 복호화 키와 포맷은 동일하되 랜덤한 값을 갖도록 설정된다. 즉, 암호화 정보 입력 모듈(340)은 사전에 진짜 복호화 키를 제공하도록 약속되지 않은 수신자에 대해서는 랜덤 값을 갖는 가짜 복호화 키를 생성하여 제공할 수 있다.
- [0042] 송신 모듈(350)은 거부적 인코딩 및 암호화 처리된 비밀 채팅 메시지를 기설정된 목적지(즉, 채팅창 내 다른 사용자의 채팅 장치)로 전송한다.
- [0043] 또한, 송신 모듈(350)은 암호화 정보 입력 모듈(340)로부터 전달된 복호화 키를 목적지로 전송할 수 있다. 이때, 상대 비밀 채팅 장치로 전송할 복호화 키는 해당 비밀 채팅 장치에 따라 진짜 복호화 키 또는 가짜 복호화 키일 수 있다.
- [0044] 이하 도 2를 참조하여, 메시지 송신부(300)를 통해 채팅 메시지를 거부적 인코딩 및 암호화 처리하여 비밀 채팅을 제공하는 방법에 대해서 상세히 설명하도록 한다.
- [0045] 도 2는 본 발명의 일 실시예에 따른 비밀 채팅 메시지의 암호화를 통한 비밀 채팅 방법을 설명하기 위한 순서도이다.
- [0046] 먼저, 둘 이상의 사용자가 참여하는 채팅창을 개설하고(S210), 해당 채팅창에서 입력된 채팅 메시지(즉, 원본 채팅 메시지)를 수신한다(S220).
- [0047] 그런 다음, 기설정된 데이터 집합 내 문장들에 대해 확률적 언어 모델을 적용하여 생성한 매핑 정보에 기초하여 원본 채팅 메시지를 거부적 인코딩 처리한다(S230).
- [0048] 이때, 원본 채팅 메시지는 평문 형태이며, 원본 채팅 메시지를 기설정된 매핑 정보에 따라 이진 데이터로 변환

하는 거부적 인코딩을 처리할 수 있다.

- [0049] 참고로, 상기 단계 (S230) 이전에, 기설정된 문장 특징 추출 알고리즘을 적용하여 데이터 집합에서 문장 별 구성상 특징 요소를 추출하는 단계, 특징 요소에 대해 데이터 집합 내에서의 확률을 할당하는 확률적 언어 모델에 기반하여 특징 요소 별 누적 분포를 산출하는 단계, 및 누적 분포 별로 대응된 이진 코드 정보를 매핑하여 매핑 정보를 생성하는 단계를 수행할 수 있다. 이를 통해 생성된 매핑 정보는 저장되어, 추후 채팅 메시지를 거부적 인코딩하는데 사용하거나, 수신된 채팅 메시지를 거부적 디코딩하는데 사용된다.
- [0050] 그런 다음, 거부적 인코딩의 결과 데이터를 암호화 키를 사용하여 암호화한다(S240).
- [0051] 상기 단계 (S240) 이전에, 원본 채팅 메시지의 암호화에 사용할 암호화 키를 입력받는 인터페이스를 제공한 후, 인터페이스를 통해 사용자가 입력한 암호화 키를 상기 암호화 키로 사용할 수 있다.
- [0052] 그런 후, 암호화한 채팅 메시지를 채팅창에 참여한 다른 사용자의 채팅 장치로 전송한다(S250).
- [0053] 다시 도 1로 돌아가서, 메시지 수신부(400)는 다른 사용자의 채팅 장치로부터 거부적 인코딩 및 암호화 처리된 비밀 채팅 메시지를 수신하고, 수신된 비밀 채팅 메시지를 복호화 및 거부적 디코딩 처리한다. 그리고 메시지 수신부(400)는 거부적 디코딩 처리된 채팅 메시지를 채팅 처리부(100)로 전달하여 채팅창에 디스플레이 되도록 한다.
- [0054] 구체적으로, 도 1에 도시한 바와 같이, 메시지 수신부(400)는 수신 모듈(410), 복호화 모듈(420), 복호화 정보 입력 모듈(430), 거부적 디코딩 모듈(440) 및 출력 모듈(450)을 포함한다.
- [0055] 수신 모듈(410)은 다른 사용자의 채팅 장치(즉, 비밀 채팅 장치)로부터 비밀 채팅 메시지를 수신하여 복호화 모듈(420)로 전달한다. 이때, 수신된 비밀 채팅 메시지는 다른 사용자의 채팅 장치에서 거부적 인코딩 및 암호화 처리된 채팅 메시지로서, 상대 비밀 채팅 장치에서 설정된 암호화 키로 암호화되어 있다.
- [0056] 복호화 모듈(420)은 수신된 비밀 채팅 메시지를 기설정된 복호화 키를 사용하여 복호화한 후 거부적 디코딩 모듈(440)로 전달한다. 이때, 복호화 모듈(420)은 복호화 정보 입력 모듈(430)로부터 복호화 키를 제공받아 복호화에 사용한다. 또한, 복호화 모듈(420)은 비밀 채팅 메시지가 암호화된 포맷과 대응된 복호화 방식을 사용하여, 비밀 채팅 메시지를 이진 데이터로 복호화한다.
- [0057] 복호화 정보 입력 모듈(430)은 설정된 복호화 키를 복호화 모듈(420)로 제공한다. 이때, 복호화 정보 입력 모듈(430)은 채팅 처리부(100)가 제공한 인터페이스를 통해 입력된 복호화 키를 수신하여 복호화 모듈(420)로 전달할 수 있다.
- [0058] 또한, 복호화 정보 입력 모듈(430)은 상대 비밀 채팅 장치(즉, 비밀 채팅 메시지를 전송한 채팅 장치)로부터 수신된 복호화 키를 복호화 모듈(420)로 전달할 수 있다. 이때, 복호화 정보 입력 모듈(430)은 사전에 약속된 다른 비밀 채팅 장치로부터 복호화 키를 수신하여 해당 비밀 채팅 장치의 정보와 매칭하여 저장해둘 수 있다. 이에 따라, 복호화 정보 입력 모듈(430)은 복호화 모듈(420)에서 복호화 처리하는 채팅 메시지의 발신지 정보를 확인하고, 발신지 정보에 따른 비밀 채팅 장치의 정보에 매칭된 복호화 키를 복호화 모듈(420)로 제공할 수 있다. 참고로, 복호화 정보 입력 모듈(430)에 저장된 복호화 키는 송신자의 비밀 채팅 장치에서 설정한 바에 따라 암호화 키에 대응되는 진짜 복호화 키이거나, 임의의 값을 갖는 가짜 복호화 키일 수 있다.
- [0059] 거부적 디코딩 모듈(440)은 복호화의 결과 데이터를 문장 정보 데이터베이스(220)에 저장된 매핑 정보에 기반하여 거부적 디코딩 처리한 후, 채팅 처리부(100)로 전달한다. 이때, 거부적 디코딩 모듈(440)은 복호화된 이진 데이터를 매핑 정보에 따라 평문 형태의 채팅 메시지로 변환한다. 본 발명의 일 실시예에서, 복호화 키로서 암호화 키에 대응된 진짜 복호화 키가 아닌 다른 복호화 키가 사용된 경우, 비밀 채팅 메시지는 거부적 디코딩을 통해 평문 형태이되 원본 채팅 메시지와 의미가 다른 가짜 채팅 메시지로 변환된다.
- [0060] 이하 도 3을 참조하여, 메시지 수신부(400)를 통해 비밀 채팅 메시지를 거부적 디코딩 및 복호화 처리하여 비밀 채팅을 제공하는 방법에 대해서 상세히 설명하도록 한다.
- [0061] 도 3은 본 발명의 일 실시예에 따른 비밀 채팅 메시지의 복호화를 통한 비밀 채팅 방법을 설명하기 위한 순서도이다.
- [0062] 먼저, 둘 이상의 사용자가 참여하는 채팅창을 개설하고(S310), 채팅창에 참여 중인 다른 사용자의 채팅 장치로부터 기설정된 확률적 언어 모델에 기반한 거부적 인코딩 및 기설정된 포맷으로 암호화 처리된 채팅 메시지(즉, 비밀 채팅 메시지)를 수신한다(S320).

- [0063] 그런 다음, 수신된 비밀 채팅 메시지를 설정된 복호화 키를 사용하여 복호화한다(S330).
- [0064] 이때, 복호화된 비밀 채팅 메시지는 이진 데이터로 복호화된다. 또한, 수신된 비밀 채팅 메시지를 복호화하기 이전에, 복호화에 사용할 복호화 키를 입력받는 인터페이스를 제공한 후, 인터페이스를 통해 입력된 복호화 키를 사용하여 복호화를 처리할 수 있다.
- [0065] 그런 후, 복호화의 결과 데이터를 확률적 언어 모델에 기반한 거부적 디코딩 처리한다(S340).
- [0066] 이때, 복호화된 이진 데이터를 매핑 정보에 따라 평문 형태의 채팅 메시지로 변환한다. 상기 단계 (S330)에서, 진짜 복호화 키로 복호화된 채팅 메시지를 거부적 디코딩할 경우 원본 채팅 메시지와 동일한 채팅 메시지가 복호되고, 진짜 복호화 키가 아닌 다른 복호화 키로 복호화된 채팅 메시지를 거부적 디코딩한 경우 원본 채팅 메시지와 상이한 채팅 메시지가 복호된다.
- [0067] 또한, 상기 단계 (S340)에서 거부적 디코딩을 처리하기 이전에, 기설정된 데이터 집합 내 문장들에 대해 기설정된 문장 특징 추출 알고리즘을 적용하여 문장 별 구성상 특징 요소를 추출하는 단계, 특징 요소에 대해 비밀 채팅 메시지를 암호화하는데 사용한 확률적 언어 모델과 동일한 확률적 언어 모델에 기반하여 특징 요소 별 누적 분포를 산출하는 단계, 및 누적 분포 별로 대응된 이진 코드 정보를 매핑하여 매핑 정보를 생성하는 단계를 더 포함할 수 있다.
- [0068] 그런 후, 거부적 디코딩의 결과인 채팅 메시지를 채팅창의 채팅 표시 영역에 디스플레이한다(S350).
- [0069] 이하, 도 4를 참조하여 이상에서 설명한 거부적 암호화를 이용한 비밀 채팅 방법의 예를 상세히 설명하도록 한다.
- [0070] 도 4는 본 발명의 일 실시예에 따른 비밀 채팅 장치를 통해 제공되는 채팅창의 일례들을 나타낸 도면이다.
- [0071] 구체적으로, 도 4a, 4b, 4c는 각각 비밀 채팅 장치(10)를 통해 구현된 채팅창을 나타내었다. 이때, 도 4a는 송신자(도 4a에서는 “alice”로 나타냄)의 비밀 채팅 장치(10)를 통해 구현된 채팅창 화면을 나타내었다. 그리고, 도 4b는 도 4a에서 나타낸 송신자가 전송한 채팅 메시지를 수신하는 제 1 수신자(도 4b에서는 “bob”으로 나타냄)의 비밀 채팅 장치(10)를 통해 구현된 채팅창 화면으로서, 송신자와 같은 비밀 키(즉, 암호화 키에 대응된 진짜 복호화 키)를 입력한 경우의 채팅 화면을 나타내었다. 또한, 도 4c는 도 4a에서 나타낸 송신자가 전송한 채팅 메시지를 수신하는 제 2 수신자(도 4c에서는 “eve”로 나타냄)의 비밀 채팅 장치(10)를 통해 구현된 채팅창 화면으로서, 송신자와 다른 비밀 키(즉, 암호화 키에 대응되지 않은 가짜 복호화 키)를 입력한 경우의 채팅 화면을 나타내었다.
- [0072] 도 4a, 4b, 4c에 도시한 바와 같이, 송신자와 수신자들은 각각 통신 상대방의 IP주소와 Port번호 등의 ‘목적지 정보’를 입력하고, 자신의 식별 정보인 ‘ID’와 사용할 비밀 키인 ‘Password’를 입력할 수 있다. 이때, 입력한 ‘Password’는 암호 알고리즘에 사용되는 비밀 키로서, 채팅 메시지의 암호화 또는 복호화에 사용하는 암호화 키 또는 복호화 키이다. 채팅 처리부(100)는 이러한 ‘목적지 정보’, 사용자의 ‘ID’ 및 비밀 키로서의 ‘Password’를 각각 입력할 수 있는 인터페이스를 제공한다.
- [0073] 구체적으로, 도 4a에서와 같이, 송신자(alice)가 채팅 표시 영역 하단의 입력창을 통해 전송하고자 하는 메시지를 입력하면, 비밀 채팅 장치(10)는 입력된 채팅 메시지를 거부적 인코딩 처리 및 암호화 키(즉, “realkey”)로 암호화 처리하여 수신자(bob 또는 eve)측으로 전송한다.
- [0074] 이때, 도 4b에서와 같이, 제 1 수신자(bob)의 비밀 채팅 장치(10)는 송신자(alice) 측으로부터 수신된 데이터(즉, 비밀 채팅 메시지)를 진짜 복호화 키(즉, 도 4b에서의 “realkey”)로 복호화하고, 복호화된 데이터를 거부적 디코딩 처리하여 채팅 메시지를 복원한다. 이때, 제 1 수신자(bob)의 비밀 채팅 장치(10)에서 사용된 복호화 키는 송신자의 암호화 키에 대응되므로 진짜 채팅 메시지가 채팅창의 표시 영역에 디스플레이된다.
- [0075] 반면, 도 4c에서와 같이, 제 2 수신자(eve)의 비밀 채팅 장치(10)는 송신자(alice) 측으로부터 수신된 데이터(즉, 비밀 채팅 메시지)를 가짜 복호화 키(즉, 도 4c에서의 “thisisfakekey”)로 복호화하고, 복호화된 데이터를 거부적 디코딩 처리하여 채팅 메시지를 복원한다. 이때, 제 2 수신자(eve)의 비밀 채팅 장치(10)에서 사용된 복호화 키는 송신자의 암호화 키에 대응되지 않는 가짜 복호화 키이므로, 원본 채팅 메시지와 상이한 가짜 채팅 메시지가 채팅창의 표시 영역에 디스플레이된다. 도 4c에 도시한 바와 같이, 제 2 수신자(eve)의 채팅창에 디스플레이되는 가짜 채팅 메시지는 말이 되는 평문 형태로 디스플레이되나, 실제로도 도 4a에서 나타낸 송신자가 전송한 채팅 메시지와는 상이한 의미(내용) 또는 형태를 갖는다. 즉, 수신자는 이러한 가짜 채팅 메

시지를 확인하더라도 말이 되보이는 평문 형태를 확인하게 됨으로써 복호화에 성공했다고 인식할 수 있다.

- [0076] 이하, 도 5 내지 도 7을 참조하여 본 발명의 일 실시예에 따른 거부적 인코딩 및 디코딩에 사용할 확률적 언어 모델 기반한 매핑 정보를 생성하는 방식 및 생성한 매핑 정보를 문장 정보 데이터베이스에 저장하는 방법에 대해서 상세히 설명하도록 한다.
- [0077] 본 발명의 일 실시예에 따른 비밀 채팅 장치(10)는 평문의 특징을 이용하여 거부적 인코딩 및 디코딩에 거부 능력(deniability)을 부여한다.
- [0078] 구체적으로, 거부적 인코딩 시 진짜 평문(즉, 원본 채팅 메시지)을 이진 데이터로 변환한다. 이때, 변환 기준으로서 ASCII 코드 테이블과 같은 기존의 방식이 아닌, 확률적 언어 모델을 적용한다. 확률적 언어 모델은 일련의 문자열에 확률을 할당하는 확률 모델로서, 예를 들어, 영어 단어 또는 문장에서 특정 알파벳(예, "e")이 나올 확률, 단어의 첫번째 글자에 특정 알파벳이 나올 확률, 영어 문장에서 특정 단어(예, "the")가 나올 확률, 또는 제1 특정 단어(예, "the") 다음에 연이어 제2 특정 단어(예, "love")라는 단어가 나올 확률 등을 모델링한 것이다. 또한, 거부적 디코딩 시, 거부적 인코딩에서 사용한 것과 같은 확률적 언어 모델을 이용하여 이진 데이터(즉, 비밀 채팅 메시지)를 채팅 메시지로 변환한다. 앞서 설명한 확률 모델에서 일련의 문자열에 포함된 각 글자 별로 확률을 할당하는 조건의 예는 모두 문장의 구성상 특징 요소로서 사용될 수 있다. 참고로, 일련의 문자열에 확률을 할당하는 조건의 예는 단어 또는 문장 등의 문자열 내 특정 글자가 나올 조건, 문자열 내 특정 글자들이 연이어 나올 조건, 단어의 첫번째 글자로서 특정 글자가 나올 조건, 문장 내 특정 단어가 나올 조건, 문장 내 특정 단어에 연이어 또 다른 특정 글자가 나올 조건 등을 의미하며, 이에 한정되지 않는다.
- [0079] 도 5는 본 발명의 일 실시예에 따른 거부적 인코딩 및 디코딩에 사용되는 확률적 언어 모델 기반의 문장 정보 데이터베이스의 일례를 나타낸 도면이다.
- [0080] 이때, 도 5에서는 문장에서의 첫 번째 글자에 대한 통계적 언어 모델을 도시하고 있다.
- [0081] 구체적으로, 도 5는 영어 문장에서 각 글자(즉, 'a, b, ..., z') 별로 첫 번째 글자가 될 확률 $p(X_1)$, 및 문장에서 첫 번째 글자가 될 글자(즉, 'a, b, ..., z') 별 확률의 누적 분포와, 이러한 글자별 확률의 누적 분포를 인코딩할 경우 각 요소가 L 비트 길이의 이진 코드로 표현되는 결과 값이 저장된 $2L \times 1$ 크기의 래티스 공간을 도시하였다. 즉, 래티스 공간의 각 요소는 각 문자의 누적 분포에 대응되는 이진 코드를 나타낸다.
- [0082] 이와 같은 통계적 언어 모델에서 사용되는 문장은 영어 문장에 한정되지 않으며, 첫 번째 글자인지 조건을 판단할 글자 또한 영어 알파벳으로 한정되지 않는다. 즉, 글자 조건은 영어 알파벳(a, b, ..., z)뿐 아니라 숫자 또는 문장 부호 등 특수 문자일 수도 있다. 또한, 상기 래티스 공간은 실제적인 물리 공간은 아니며, 평문의 각 문자가 래티스 공간에 저장된 값 중 하나의 요소로 대응(mapping)되어 거부적 인코딩된다.
- [0083] 본 발명의 일 실시예에 따른 거부적 암호화 방식에서는, 확률적 언어 모델을 다음과 같이 활용할 수 있다.
- [0084] 먼저, 도 5에 도시되어 있는 누적 분포에서 첫 번째 글자로서의 t의 위치를 찾는다. 그리고, 도 5의 래티스 공간에서 t의 누적 분포 위치에 대응하는 L 비트 길이의 이진 코드 집합을 찾는다. 도시되어 있는 바와 같이, 래티스 공간 내 글자 t의 누적 분포에 대응하는 후보가 다수 개 존재할 경우 첫 번째 후보를 선택할 수 있다.
- [0085] 예를 들어, 평문 "the school"을 암호화하려고 할 때, 도 5에서 t가 문장의 첫번째 글자일 조건의 확률 누적 분포는 72.749% ~ 89.420% 구간에 있다. 이때, 도 5의 래티스 공간에서 72.749% ~ 89.420% 구간의 위치에 대응하는 요소는 음영이 있는 구간이다. 이처럼, 대응된 후보가 다수 개 존재하므로 첫 번째 후보를 선택할 수 있다. 즉, 첫 번째 후보의 이진 데이터 값을 10...11라고 가정할 경우, 글자 t는 10...11로 인코딩된다.
- [0086] 이러한 과정을 거쳐 평문 "the school"의 각 글자 별로 사전에 설정된 조건(즉, 구성적 특징 요소) 별로 매핑된 이진 데이터를 적용함으로써 거부적 인코딩을 수행할 수 있다. 아래 도 6을 참조하여 또 다른 확률적 언어 모델에 기반하여 생성된 매핑 정보를 이용하여 평문의 다른 글자에 적용되는 거부적 인코딩에 대해서 설명하도록 한다.
- [0087] 도 6은 본 발명의 일 실시예에 따른 확률적 언어 모델 기반의 문장 정보 데이터베이스의 다른 예를 나타낸 도면이다.
- [0088] 이때, 도 6에서는 일련의 문자열 내에서 임의의 순번째 글자에 대해 적용하는 통계적 언어 모델을 도시하고 있다. 참고로, 도 6에서는 조건부 확률이 고려된 확률 모델을 적용하는 것을 나타내었으며, 해당 문자열 내 다른

문자(다른 순서)들의 인코딩도 유사하게 수행될 수 있다.

- [0089] 예를 들어, “the school”이라는 문자열의 3번째 알파벳인 “e”에 대한 인코딩은 첫 번째 글자가 “t”이고 두 번째 글자가 “h”일 때 세 번째 글자가 “e”일 확률($p(X_3 = e \mid X_2 = h, X_1 = t)$)을 구하여 수행될 수 있다.
- [0090] 도 6에 도시된 바와 같이, 이 확률의 누적 분포에 대응되는 구간인 인코딩 후보가 다수 개 존재하며, 도 5에서와 마찬가지로 다수의 후보 중 첫 번째 후보인 이진 데이터 값이 해당 글자의 인코딩 값으로 설정될 수 있다.
- [0091] 한편, 본 발명의 일 실시예에 따른 거부적 디코딩 과정은 앞서 설명한 인코딩 과정을 역으로 수행하여 처리될 수 있다.
- [0092] 구체적으로, 특정 문자열을 앞서 설명한 확률적 언어 모델에 기반한 거부적 인코딩 및 암호화 키로 암호화 처리된 경우, 해당 문자열의 복원 시 암호화된 문자열을 복호화 키로 복호화한 결과 데이터를 거부적 인코딩시 사용한 것과 동일한 확률적 언어 모델에 기반하여 거부적 디코딩한다. 참고로 이하의 설명에서는 설명의 편의상 이진 데이터 값을 16진수로 표기하기로 한다.
- [0093] 예를 들어, “crypto”라는 단어를 위에서 설명한 확률적 언어 모델에 기반하여 거부적 인코딩한 값을 ‘35 21 2B 62 44 A2’라고 가정한다. 또한, 이러한 거부적 인코딩의 결과 값을 암호화 키로 암호화한 결과를 ‘73 C3 39 13 F2 37’이라고 가정한다.
- [0094] 이때, 암호화된 문자열인 ‘73 C3 39 13 F2 37’의 복원 시, 암호화 키에 대응된 진짜 복호화 키로 복호화한 경우 원래의 거부적 인코딩의 결과 값인 ‘35 21 2B 62 44 A2’ 값을 획득할 수 있다. 그런 다음, ‘35 21 2B 62 44 A2’ 값 별로 대응하는 확률 모델(예를 들어, 앞서 도 5 및 도 6에서 설명한 확률 모델들)의 래티스 공간에 저장된 이진 데이터 값 중 해당하는 값에 매핑된 누적 분포 값을 확인한다. 그리고, 확인된 누적 분포 값을 갖는 글자를 추출함으로써 거부적 디코딩을 처리할 수 있다. 이에 따른 결과로서 “crypto”라는 원래 문자열을 복원할 수 있다. 참고로, ‘35 21 2B 62 44 A2’ 중에서 값 별로 대응하는 확률 모델은 거부적 암호화에 적용한 확률 모델과 대응되며, 하나 이상의 값이 동일한 확률 모델을 사용하는 것도 가능하다.
- [0095] 반면, 암호화된 문자열인 ‘73 C3 39 13 F2 37’의 복원 시, 암호화 키에 대응된 복호화 키가 아닌 가짜 복호화 키로 복호화한 경우 원래의 이진 데이터 값이 아닌 전혀 다른 값(예를 들어, ‘78 3F 22 56 1F 30’)을 획득할 수 있다. 이러한 경우에도 복호화의 결과 값인 ‘78 3F 22 56 1F 30’ 별로 대응하는 확률 모델의 래티스 공간에 저장된 이진 데이터 값 중 해당하는 값에 매핑된 누적 분포 값을 확인한다. 그리고, 확인된 누적 분포 값을 갖는 글자를 추출하여 거부적 디코딩을 처리한다. 이때, 가짜 복호화 키로 복호화된 값들이 원래의 이진 데이터 값과 상이하므로 거부적 디코딩의 결과로서 복원된 문자열 또한 원본 문자열(즉, “crypto”)과 상이한 문자열(예를 들어, “school”)이 복원된다. 이때, 가짜 복호화 키로 복호화된 값들도 앞서 거부적 인코딩에 적용한 확률 모델과 대응된 확률 모델을 이용하여 거부적 디코딩을 처리할 수 있다.
- [0096] 본 발명의 일 실시예에 따른 메시지 송신부(300) 및 메시지 수신부(400)는 이상에서 설명한 방식으로 확률적 언어 모델에 기반한 거부적 인코딩 및 거부적 디코딩을 처리하고, 이를 이용한 암호화 및 복호화를 처리할 수 있다.
- [0097] 이처럼, 본 발명의 일 실시예에 따른 거부적 암호화 방식을 적용하면 가짜 채팅 메시지도 유의미하거나 유의미해 보이는 평문이 생성될 수 있다. 즉, 종래의 암호화 기법에서는 주어진 암호문을 가짜 키를 사용하여 복호화하면 전혀 의미가 없는 이진 코드가 생성된다. 예를 들어, ASCII 코드를 사용할 경우, “the school”을 암호화한 암호문을 가짜 복호화 키로 복호화하면 가짜 채팅 메시지로써 “@8hk*s”과 같이 전혀 의미 없는 문자열이 복원된다. 그러나, 본 발명의 일 실시예에 따르면 가짜 채팅 메시지도 “an apple”과 같이 의미있는 문자열(즉, 평문 형태)로 복원될 수 있다.
- [0098] 또한, 이상에서 설명한 확률적 언어 모델에 기반한 데이터 집합 내 문자의 누적 분포 및 이에 대응되는 이진 코드 정보(즉, 매핑 정보)는 문자 정보 데이터베이스(220)에 저장되며, 매핑 정보는 공개 정보이다. 따라서 송신자 및 수신자 모두가 해당 정보에 접근할 수 있다. 또한, 송신자가 비밀 채팅 메시지를 전송하도록 설정한 수신자 뿐만 아니라 제 3 자도 해당 매핑 정보에 접근할 수 있다. 이때, 제 3 자는 암호화된 비밀 채팅 메시지를 임의의 복호화 키로 복호화를 시도하게 되며, 이러한 비정상적인 복호화를 통해 얻게 되는 채팅 메시지 또한 거부적 디코딩을 통해 의미있어 보이는 평문으로 복원될 수 있다.
- [0099] 한편, 앞서 도 5 및 도 6을 통해 설명한 바와 같이, 본 발명의 일 실시예에서 기설정된 데이터 집합 내 문장(또는 문자열)에서 구성적 특징 요소 별 누적 분포는 데이터 집합에 대한 학습(training) 과정을 통해 얻을 수 있

다. 즉, 본 발명의 일 실시예에 따른 문자 정보 데이터베이스(220)에는 주어진 데이터 집합에서의 누적 분포 학습을 통해 추출된 구성적 특징 요소 별 누적 분포 및 이에 각각 대응되는 이진 코드 정보가 저장된다.

[0100] 이는, 다양한 데이터 집합을 사용하여 특화된 데이터베이스를 사용할 수 있음을 의미한다. 예를 들어, 어떤 사용자가 데이터 집합으로서 성경을 통해 언어 모델을 구축한다면, 데이터베이스는 성경의 누적 분포를 가지게 될 것이다. 이에 비해, 데이터 집합으로서 경제 뉴스를 통해 언어 모델을 구축했을 경우, 성경을 통해 구축한 언어 모델의 누적 분포와 상당히 차이가 있는 누적 분포를 가지게 될 것이다. 예를 들어, 성경에서는 "사랑"이라는 단어의 빈도가 높지만, 경제 뉴스에서는 "계좌"라는 성경에는 나오지 않을 법한 단어의 빈도가 높을 것이다. 이러한 특성을 활용하여, 본 발명의 일 실시예에 따른 비밀 채팅 장치(10)는 원하는 스타일의 가짜 채팅 메시지를 생성할 수 있다. 즉, 거부적 인코딩 및 디코딩에 사용될 확률적 언어 모델을 생성하는데 적용한 데이터 집합의 종류 및 내용에 따라 가짜 채팅 메시지의 내용 및 형태가 영향을 받을 수 있다. 아래 도 7을 참조하여 데이터 집합의 종류에 따라 거부적 디코딩을 통한 복호화의 결과에 대해서 설명하도록 한다.

[0101] 도 7은 본 발명의 일 실시예에 따른 거부적 디코딩 결과의 일례를 나타낸 도면이다.

[0102] 도 7에서 첫번째 열은 확률적 언어 모델에 기반한 매핑 정보를 생성하는데 사용된 데이터 집합(자료)의 종류를 나타내었다. 예를 들어, 데이터 집합은 NASA 문서, 소설인 ‘로미오와 줄리엣’, 암호학 문서, 성경, 클래식 음악 문서가 사용되었다.

[0103] 도 7의 두번째 열은 거부적 인코딩 및 암호화 키로 암호화된 문자열을 진짜 복호화 키로 복호화하여 거부적 디코딩한 결과를 도시하고 있다. 즉, 암호문(즉, 비밀 채팅 메시지)의 복호화에 진짜 복호화 키(K1)가 사용되었을 때 복원되는 진짜 평문을 나타내었다.

[0104] 도 7의 세번째 열 및 네번째 열은 암호문을 임의로 선택된 가짜 복호화 키(K2 또는 K3)가 사용되었을 경우 거부적 디코딩 및 복호화를 통해 복원된 평문을 나타내었다. 도 7의 세번째 및 네번째 열에 도시한 바와 같이, 확률 모델에 모델링에 적용한 데이터의 집합 별로 각각 진짜 평문과는 전혀 다른 내용 및 형태이지만 의미있어 보이는 가짜 평문이 생성된다. 이때, 가짜 복호화 키로 복원된 각 평문들은 확률 모델의 훈련(학습)에 사용된 자료(즉, 데이터 집합)에 따라 의미 및 형태가 해당 자료의 특성과 연관됨을 알 수 있다. 예를 들어, 확률 모델의 훈련 자료로서 암호학 문서를 사용했을 때는 암호학 문서에 나올 법한 구 또는 절(즉, “the secret key signatu” 및 “the probabilistic tech”)이 복원되었다. 또한, 확률 모델의 훈련 자료로서 클래식 음악 문서를 사용했을 때는 음악 문서에 나올 법한 구 또는 절(즉, “sym orchphil. Classic” 및 “beethovenl.v. symcom”)이 복원되었다.

[0105] 한편, 이상 도 1 내지 도 7을 통해 설명한 비밀 채팅 장치(10)는, 확률적 언어 모델에 기반한 거부적 인코딩 및 디코딩을 통해 비밀 채팅 메시지를 암호화 및 복호화하는 비밀 채팅 절차를 수행하는 애플리케이션이 저장된 메모리와, 이러한 애플리케이션을 실행하여 각 절차를 처리하는 프로세서를 포함할 수 있다. 즉, 비밀 채팅 장치(10)의 프로세서가 상기 애플리케이션을 실행함에 따라 거부적 암호화를 통한 비밀 채팅을 사용자에게 제공할 수 있다.

[0106] 이상에서 설명한 본 발명의 일 실시예에 따른 거부적 암호화를 이용한 비밀 채팅 방법은 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0107] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0108] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미

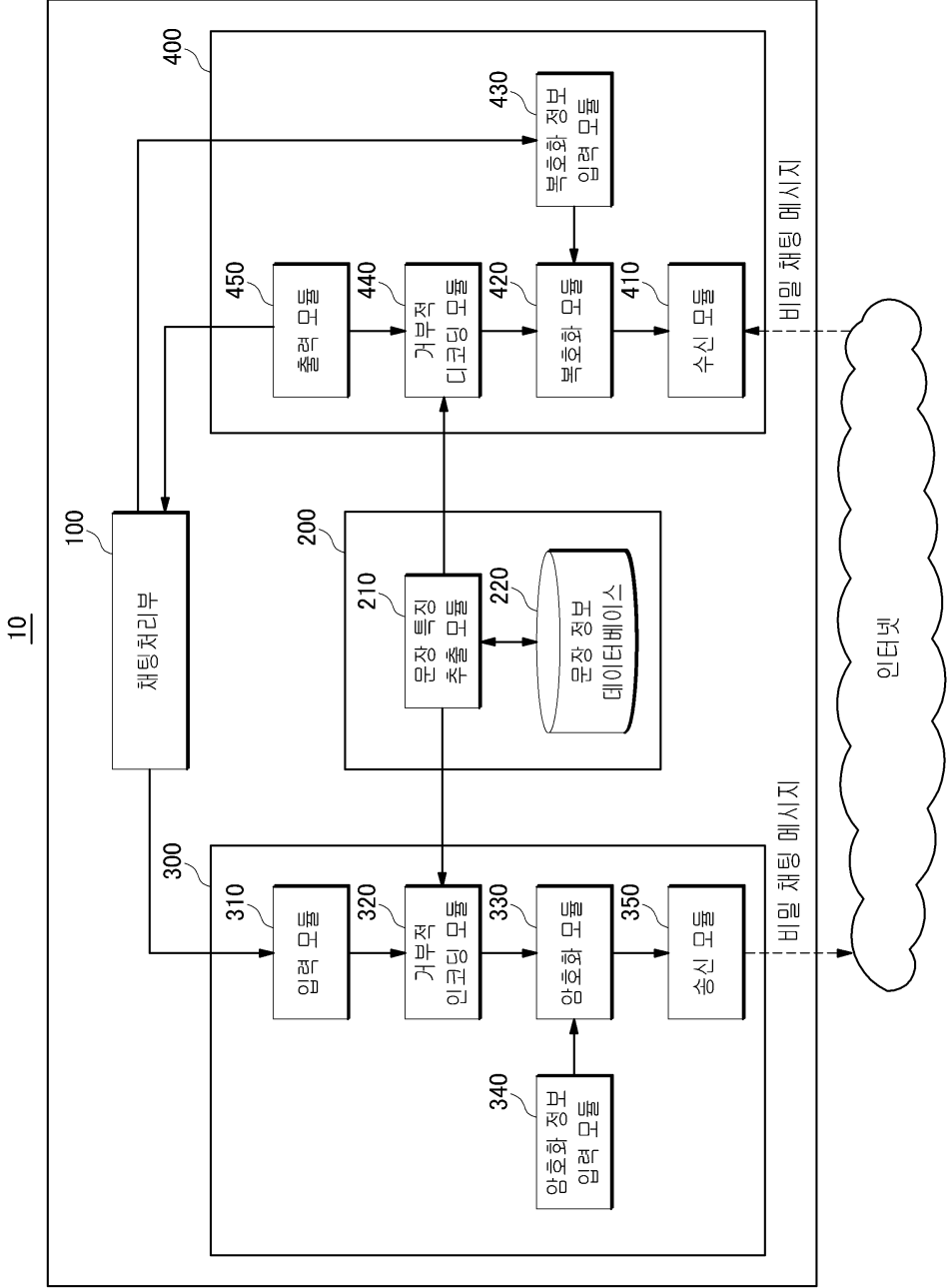
및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

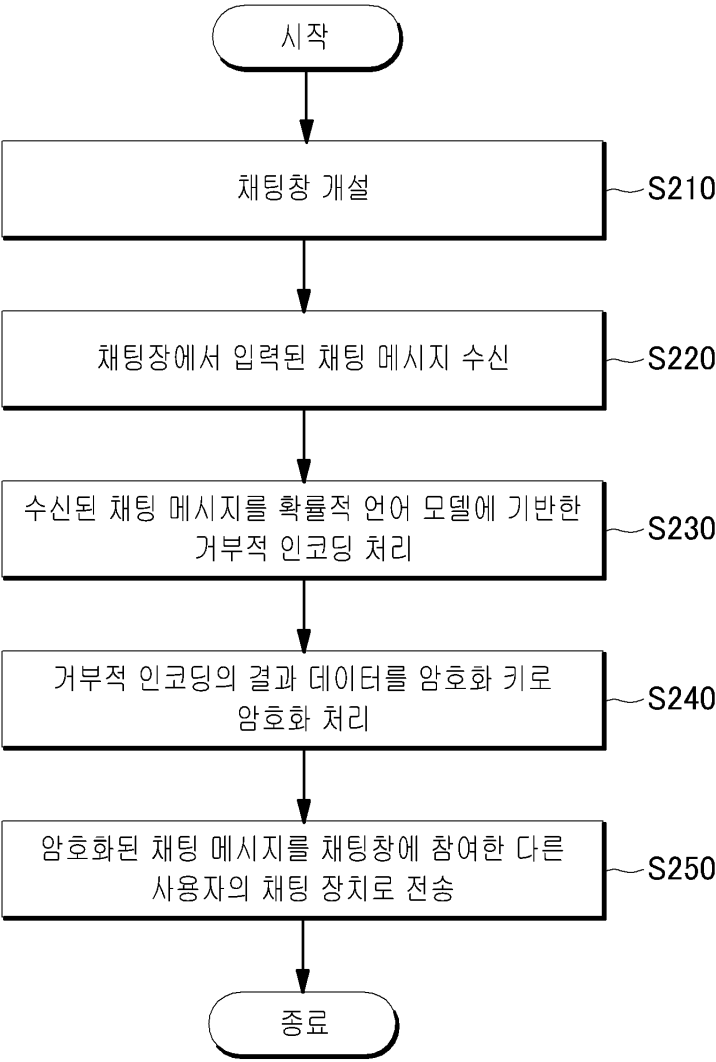
- 10: 비밀 채팅 장치
- 100: 채팅 처리부
- 200: 문장 정보 처리부
- 300: 메시지 송신부
- 400: 메시지 수신부

도면

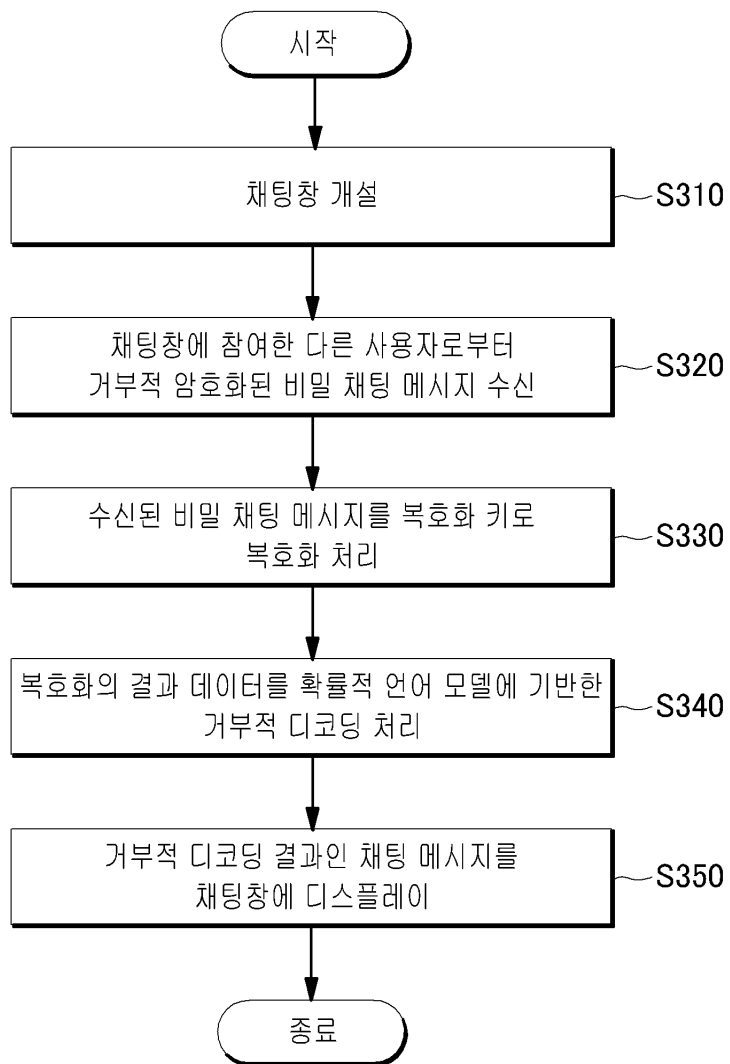
도면1



도면2



도면3



도면4a

IP Addr:	xxx.xxx.xxx.xxx
Port:	4444
UserID:	alice
Passwd:	realkey
Connect Disconnect	
<pre> press Connect button alice connected. bob connected. wer and stand so alice i am so hungry alice <u>its almost time for dinner. what do you want for dinner</u> bob <u>can i have a pork cutlet and soup</u> alice <u>sure. that sounds good</u> bob <u>all of your food is really delicious to me</u> bob <u>all of your food is really delicious to me haha</u> </pre>	

도면4b

IP Addr:	xxx.xxx.xxx.xxx
Port:	4444
UserID:	bob
Passwd:	realkey
Connect Disconnect	
<pre> press Connect button bob connected. wer and stand so alice i am so hungry alice <u>its almost time for dinner. what do you want for dinner</u> bob <u>can i have a pork cutlet and soup</u> alice <u>sure. that sounds good</u> bob <u>all of your food is really delicious to me</u> bob <u>all of your food is really delicious to me haha</u> </pre>	

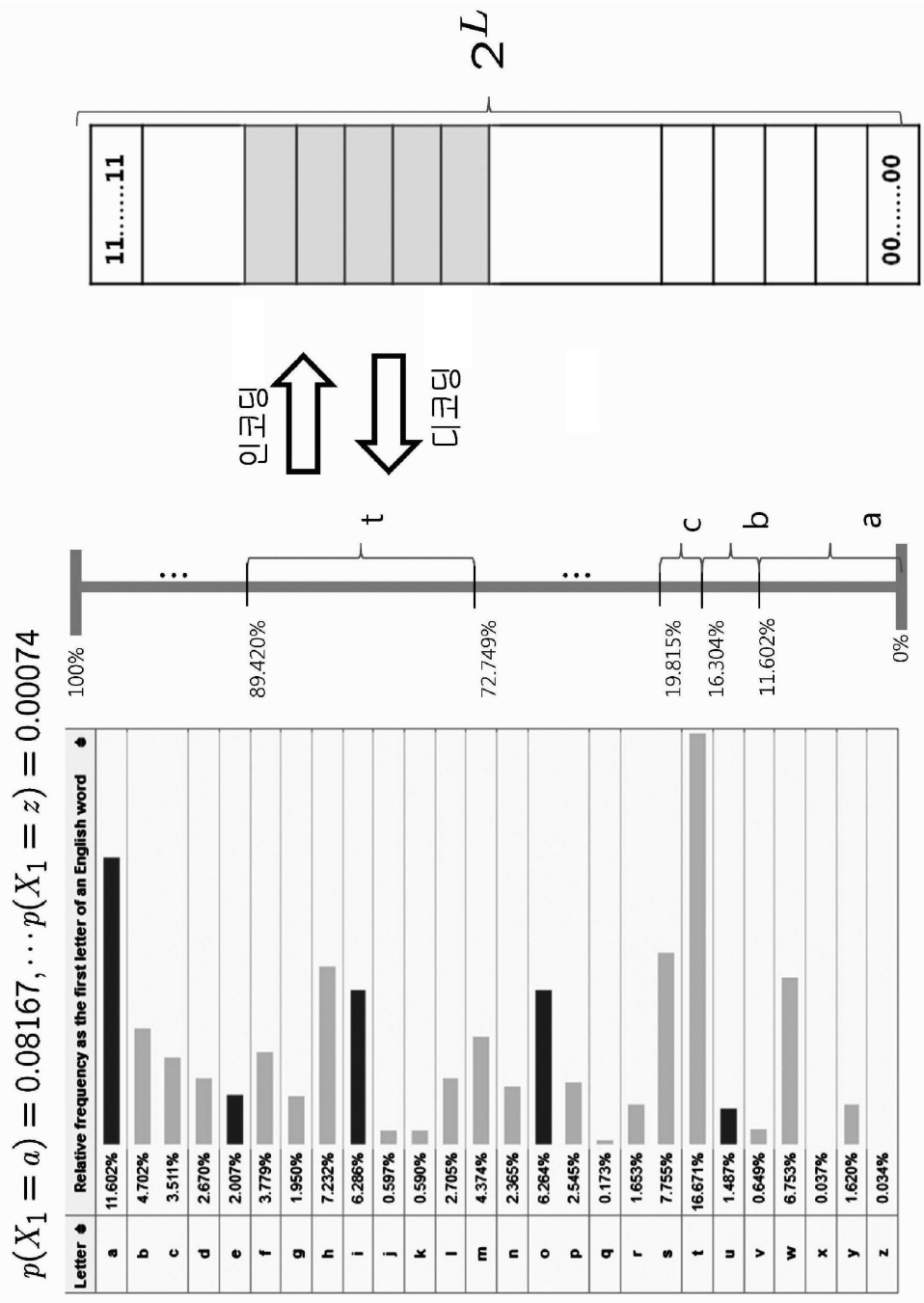
도면4c

IP Addr:	xxx.xxx.xxx.xxx
Port:	4444
UserID:	eve
Passwd:	thisisfakekey

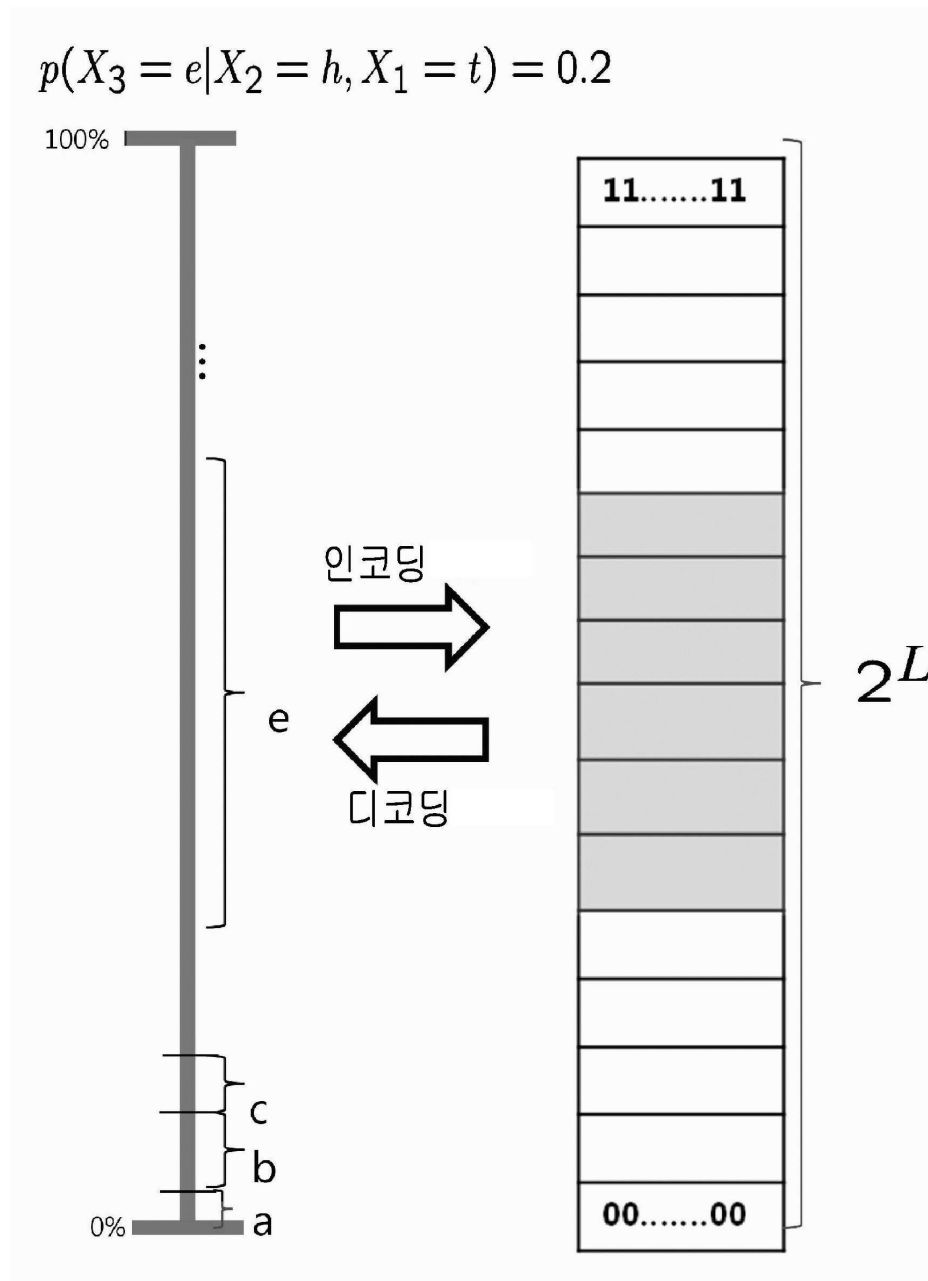
Connect Disconnect

press Connect button
 eve connected.
 act ii, scene ii, scene
 what thou will not for the come to the county such a man the lar
 and the stand the search for the lazy ti
 and the fair which the street w
 act ii, scene iii, scene iii, scene iii, scene i
 there in the gone of the strains from the prince, what i

도면5



도면6



도면7

학습 데이터	진짜 키(K1) 사용	임의로 선택된 가짜 키(K2) 사용	임의로 선택된 가짜 키(K3) 사용
NASA 문서	'deniable encryption...'	'the scout's payload ac'	'the spacecraft and the'
로미오와 줄리엣 (소설)	'deniable encryption...'	'what show the project'	'scene iii. scene iii'
암호학 문서	'deniable encryption...'	'the secret key signatu'	'the probabilistic tech'
성경	'deniable encryption...'	'and the children of th'	'and the lord was not b'
클래식 음악 문서	'deniable encryption...'	'sym orch phil. Classic'	'beethoven l.v. sym com'

【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 제11항

【변경전】

상기 암호화 시

【변경후】

암호화 시