(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년06월04일
(11) 등록번호 10-1153016
(24) 등록일자 2012년05월29일

(51) 국제특허분류(Int. Cl.)
G06K 19/06 (2006.01)
(21) 출원번호 10-2005-0007087
(22) 출원일자 2005년01월26일
심사청구일자 2010년01월21일
(65) 공개번호 10-2005-0093715
(43) 공개일자 2005년09월23일
(30) 우선권주장
10/802,981 2004년03월17일 미국(US)
(56) 선행기술조사문헌
US4820912 A
EP1173001 A
JP2001518414 A
JP평성11259623 A
전체 청구항 수 : 총 24 항

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
키로브시키,다르코
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이 마이크로소프트 코포레이션 내
(74) 대리인
제일특허법인

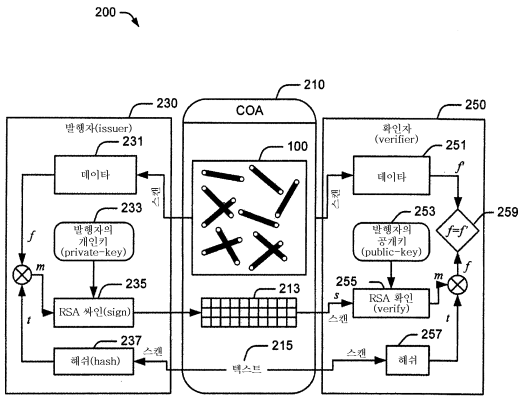
심사관 : 임은정

(54) 발명의 명칭 **랜덤하게 분포된 객체의 특징들을 인코딩하기 위한 시스템및 방법**

(57) 요 약

설명된 시스템 및 방법은 객체의 랜덤하게 분포된 특징들을 인코딩하는 것에 관한 것이다. 인증 객체의 랜덤하게 분포된 특징들이 결정된다. 랜덤하게 분포된 특징들을 나타내는 데이타는 압축되고, 서명으로 인코딩된다. 레이블(label)은 생성되고, 인증 객체 및 인코딩되는 데이타를 포함한다. 데이타는 인증 객체와 연계된 확률 밀도 함수를 결정하여 압축될 수 있다. 랜덤하게 분포된 속성들과 연계된 벡터들은, 적어도 부분적으로는, 확률 밀도 함수에 기초하여 결정된다. 벡터들은 산술 코딩 알고리즘을 사용하여 인코딩된다.

대 표 도 - 도2



특허청구의 범위

청구항 1

객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 방법으로서,

인증 객체(100)의 랜덤하게 분포된 특징들을 결정하는 단계(410);

상기 랜덤하게 분포된 특징들을 나타내는 데이타를 압축하는 단계(415);

상기 압축된 데이타를 개인키(private key)로 인코딩하는 단계(420); 및

상기 인증 객체와 상기 인코딩된 데이타를 포함하는 레이블(label)을 생성하는 단계(425)

를 포함하고,

상기 압축하는 단계는,

상기 인증 객체와 연계된 확률 밀도 함수를 결정하는 단계(505) - 상기 확률 밀도 함수는 상기 랜덤하게 분포된 특징들의 유닛이 상기 인증 객체의 특정 위치에서 발견될 확률을 나타냄 -;

상기 확률 밀도 함수에 적어도 부분적으로 기초하여 상기 랜덤하게 분포되는 특징들의 끝점들(end-points)과 연계된 포인트-투-포인트(point-to-point) 벡터들을 결정하는 단계(510);

산술적 코딩 알고리즘(arithmetic coding algorithm)을 사용하여 상기 포인트-투-포인트 벡터들을 인코딩하는 단계(515) - 상기 산술적 코딩 알고리즘을 사용하여 벡터들을 인코딩하는 단계는, 고정된 양의 데이타 내의 포인트-투-포인트 벡터들의 일부를 연결하기 위한 경로를 결정하는 단계(520)를 포함하고, 상기 경로는 상기 포인트-투-포인트 벡터들의 포인트들을 연결함 -; 및

상기 압축된 데이타로서 상기 경로를 리턴하는 단계(525)

를 포함하는 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 방법.

청구항 2

제1항에 있어서,

상기 랜덤하게 분포된 특징들은 상기 인증 객체에 랜덤하게 위치되는 파이버들(fibers; 110, 326)인 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 방법.

청구항 3

제2항에 있어서,

상기 확률 밀도 함수는 특정 지역의 파이버들이 광원(324)에 의해 조명될 확률을 나타내는 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 방법.

청구항 4

제2항에 있어서,

상기 확률 밀도 함수는, 적어도 부분적으로, 상기 파이버들의 길이에 기초하여 유도되는 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 방법.

청구항 5

제2항에 있어서,

각각의 벡터는 2개의 파이버들의 끝점들을 나타내는 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 방법.

청구항 6

제1항에 있어서,

상기 레이블은 자체-인증되도록(self-authenticated) 구성된 인증서(certificate of authenticity; 210)이고,

상기 인증 객체는 상기 인증서에 포함되는 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 방법.

청구항 7

제1항에 있어서,

상기 인코딩된 데이타는 바코드(barcode)로서 상기 레이블에 포함되는 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 방법.

청구항 8

제1항에 있어서,

문자열(string of charaters)을 포함하는 텍스트 데이타를 결정하는 단계 - 상기 텍스트 데이타는 상기 레이블에 포함됨 - ;

알고리즘에 의해 상기 텍스트 데이타를 해쉬(hash)하는 단계; 및

상기 해쉬된 텍스트 데이타를 사용하여 상기 압축된 데이타를 암호화하는 단계 - 상기 해쉬된 텍스트 데이타는 상기 압축된 데이타를 인코딩하기 전의 상기 랜덤하게 분포된 특징들을 나타내는 데이타와 병합됨 -

를 더 포함하는 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 방법.

청구항 9

제8항에 있어서,

상기 알고리즘은 암호법적으로 보안된 해쉬 알고리즘(cryptographically secure hash algorithm)인 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 방법.

청구항 10

제8항에 있어서,

상기 알고리즘은 SHA1 암호화 알고리즘인 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 방법.

청구항 11

프로세서에 의해 제1항에 기재된 방법을 수행하도록 실행가능한 명령어들을 포함하는 컴퓨터 판독가능 기록 매체.

청구항 12

인증 객체(100)의 랜덤하게 분포된 특징들(110, 326)을 결정하고, 상기 랜덤하게 분포된 특징들을 나타내는 데이타(231)를 압축하도록 구성된 발행자(issuer; 230)를 포함하는 시스템으로서,

상기 발행자는,

상기 인증 객체와 연계된 확률 밀도 함수를 결정하고 - 상기 확률 밀도 함수는 상기 랜덤하게 분포된 특징들의 유닛이 상기 인증 객체의 특정 위치에서 발견될 확률을 나타냄 -,

상기 확률 밀도 함수에 적어도 부분적으로 기초하여 상기 랜덤하게 분포된 특징들의 끝점들과 연계된 포인트-투-포인트 벡터들을 결정하고,

산술적 코딩 알고리즘을 적용함으로써 고정된 양의 데이타 내의 상기 포인트-투-포인트 벡터들의 일부를 경로로서 인코딩함으로써 상기 포인트-투-포인트 벡터들을 인코딩하고 - 상기 경로는 상기 포인트-투-포인트 벡터들의 포인트들을 연결함 -,

상기 압축된 데이타로서 상기 경로를 리턴하도록 더 구성되고,

상기 발행자는 개인키(233)에 의해 상기 압축된 데이타를 인코딩하고, 상기 인증 객체와 상기 인코딩된 데이타를 포함하는 레이블(210)을 생성하도록 더 구성되는 시스템.

청구항 13

제12항에 있어서,

상기 발행자는 상기 레이블 내에 상기 인코딩된 데이타를 갖는 바코드(213)를 포함하도록 더 구성되는 시스템.

청구항 14

제12항에 있어서,

상기 발행자는, 문자열을 포함하는 텍스트 데이타(215)를 결정하고, 알고리즘에 의해 상기 텍스트 데이타를 해쉬(237)하도록 더 구성되며,

상기 텍스트 데이타는 상기 레이블에 포함되는 시스템.

청구항 15

제14항에 있어서,

상기 발행자는, 상기 해쉬된 텍스트 데이타를 사용하여 상기 압축된 데이타를 암호화하도록 더 구성되고, 상기 해쉬된 텍스트 데이타는 상기 압축된 데이타를 인코딩하기 전에 상기 랜덤하게 분포된 특징들을 나타내는 데이타와 병합되는 시스템.

청구항 16

제12항에 있어서,

상기 레이블 내의 상기 랜덤하게 분포된 특징들을 나타내는 데이타(251)를 디코드하고, 상기 디코드된 데이타를 상기 인증 객체로부터 결정된 상기 랜덤하게 분포된 특징들의 데이타와 비교(259)함으로써 상기 레이블을 인증하도록 구성된 확인자(verifier; 250)를 더 포함하는 시스템.

청구항 17

레이블(210)을 포함하는 컴퓨터 판독가능 기록 매체로서,

상기 레이블은,

랜덤하게 분포된 특징들(110, 326)을 포함하는 인증 객체(100); 및

상기 인증 객체와 연계된 인코딩된 정보(213)를 포함하고,

상기 정보는 개인키에 의해 인코딩되고, 상기 인증 객체의 상기 랜덤하게 분포된 특징들을 나타내는 압축된 데이타를 포함하고, 상기 인코딩된 정보 내의 데이타는 상기 인증 객체와 연계된 확률 밀도 함수를 결정함으로써 압축되고, 상기 확률 밀도 함수는 상기 랜덤하게 분포된 특징들의 유닛이 상기 인증 객체의 특정 위치에서 발견될 확률을 나타내고, 상기 확률 밀도 함수에 적어도 부분적으로 기초하여 상기 랜덤하게 분포되는 특징들의 끝점들과 연계된 포인트-투-포인트 벡터들을 결정하고, 산술적 코딩 알고리즘을 사용하여 상기 포인트-투-포인트 벡터들을 인코딩(515)하고, 상기 산술적 코딩 알고리즘을 사용하여 벡터들을 인코딩하는 것은 고정된 양의 데이타 내의 상기 포인트-투-포인트 벡터들의 일부를 연결하기 위한 경로를 결정(520)하는 것을 포함하고, 상기 경로는 상기 포인트-투-포인트 벡터들의 포인트들을 연결하고, 상기 압축된 데이타로서 상기 경로를 리턴(525)하며,

상기 레이블은 상기 인코딩된 정보를 디코드한 것(a decoding of the encoded information)과 상기 인증 객체를 분석하여 얻어진 상기 랜덤하게 분포된 특징들을 나타내는 데이타(251)를 비교(259)함으로써 자체-인증되는 컴퓨터 판독가능 기록 매체.

청구항 18

제17항에 있어서,

인코딩된 정보는 바코드(213)로서 상기 레이블에 포함되는 컴퓨터 판독가능 기록 매체.

청구항 19

제17항에 있어서,

상기 레이블은

문자열을 포함하는 텍스트 데이타(215)를 더 포함하고,

상기 압축된 데이타는 상기 텍스트 데이타를 사용하여 암호화되는 컴퓨터 판독가능 기록 매체.

청구항 20

제19항에 있어서,

상기 압축된 데이타는,

알고리즘에 의해 상기 텍스트 데이타를 해쉬하고(237);

상기 해쉬된 텍스트 데이타를 사용하여 상기 압축된 데이타를 암호화함(235)으로써 암호화되며,

상기 해쉬된 텍스트 데이타는 상기 압축된 데이타를 인코딩하기 전에 상기 랜덤하게 분포된 특징들을 나타내는 데이타와 병합되는 컴퓨터 판독가능 기록 매체.

청구항 21

객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 장치로서,

인증 객체(100)의 랜덤하게 분포된 특징들을 결정하기 위한 수단(322);

상기 랜덤하게 분포된 특징들을 나타내는 데이타를 압축하기 위한 수단(230);

개인키(private key; 233)에 의해 상기 압축된 데이타를 인코딩하기 위한 수단; 및

상기 인증 객체와 상기 인코딩된 데이타를 포함하는 레이블(210)을 생성하기 위한 수단

을 포함하고,

상기 데이타를 압축하기 위한 수단은,

상기 인증 객체와 연계된 확률 밀도 함수를 결정하기 위한 수단 - 상기 확률 밀도 함수는 상기 랜덤하게 분포된 특징들의 유닛이 상기 인증 객체의 특정 위치에서 발견될 확률을 나타냄 -;

상기 확률 밀도 함수에 적어도 부분적으로 기초하여 상기 랜덤하게 분포되는 특징들의 끝점들과 연계되는 포인트-투-포인트 벡터들을 결정하기 위한 수단;

산술적 코딩 알고리즘을 사용하여 상기 포인트-투-포인트 벡터들을 인코딩하기 위한 수단 - 상기 산술적 코딩 알고리즘을 사용하여 벡터들을 인코딩하는 것은 고정된 양의 데이타 내의 포인트-투-포인트 벡터들의 일부를 연결하기 위한 경로를 결정하는 것을 포함하고, 상기 경로는 상기 포인트-투-포인트 벡터들의 포인트들을 연결함 -; 및

상기 압축된 데이타로서 상기 경로를 리턴하기 위한 수단

을 포함하는 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 장치.

청구항 22

제21항에 있어서,

상기 랜덤하게 분포된 특징들로서 상기 인증 객체에 파이버들(110, 326)을 포함시키기 위한 수단을 더 포함하는 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 장치.

청구항 23

제21항에 있어서,

문자열을 포함하는 텍스트 데이타(215)를 결정하기 위한 수단 - 상기 텍스트 데이타는 상기 레이블에 포함됨 -;

알고리즘에 의해 상기 텍스트 데이타를 해쉬하기 위한 수단(237); 및

상기 해쉬된 텍스트 데이타를 사용하여 상기 압축된 데이타를 암호화하기 위한 수단(235) - 상기 해쉬된 텍스트 데이타는 상기 압축된 데이타를 인코딩하기 전에 상기 랜덤하게 분포된 특징들을 나타내는 데이타와 병합됨 -;

을 더 포함하는 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 장치.

청구항 24

제21항에 있어서,

인코딩된 데이타를 상기 인증 객체의 상기 랜덤하게 분포된 특징들과 연계된 데이타와 비교(259)함으로써 상기 레이블을 인증하기 위한 수단(250)을 더 포함하는 객체의 랜덤하게 분포된 특징들을 인코딩하기 위한 장치.

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0026] 본 명세서에 기재된 시스템 및 방법은 일반적으로 위조-방지 및/또는 변조-방지 레이블(label)들에 관한 것이고, 더 구체적으로, 랜덤하게 분포된 객체의 특징들을 사용하여(임베딩되거나 자연적으로 고유의) 레이블을 위조 및/또는 변조하려는 비승인된 시도를 제한하는 것에 관한 것이다.

[0027] 레이블의 위조 및 변조는 수입 손실과 고객 손실면에서 제품 마켓 경영자들과 제조자들에게 매년 수 조 달러의 비용이 들게 한다. 컴퓨터 기술의 증대로, 진품과 닮은 레이블을 생성하는 것이 더 쉬워졌다. 예를 들어, 스캐너는 진품 레이블의 고 해상도 이미지를 스캔하기 위해 사용될 수 있고, 그 다음 이 생성된 이미지는 저가의 비용으로 반복하여 재생성될 수 있다. 또한, 쿠폰들은 스캔되고, 수정되고(예를 들어, 더

고가(higher value)를 갖기 위해), 반복적으로 프린트되고, 회수될 수 있다.

[0028] 다양한 기술들이 최근에 위조 및 변조의 홍수를 막기 위해 사용되어왔다. 레이블이 보안되어온 한 가지 방식은 바코드의 사용에 의해서이다. 바코드들은 일반적으로 레이블에 프린트된 기계-판독가능 코드이다. 바코드 스캐너를 사용하여, 바코드를 갖는 레이블은 신속하게 판독되고 인증될 수 있다. 현재 바코드된 레이블의 한 가지 문제점은 동일 레이블이 다양한 항목들에 사용될 수 있다는 점이다.

[0029] 다른 현재의 해결책은 데이타베이스에 저장된 보안된 데이타에 대해 검사된 스캔된 바코드를 갖는 것이다(예를 들어, 포인트-오브-스케일(point-of-scale) 시스템). 그러나, 이 해결책은 마켓 경영자 또는 제조자로부터의 업데이트된 데이타의 병합을 필요로 한다. 그런 해결책은 복수의 개체들의 적절한 시간과 가까운 협력을 필요로 한다. 또한, 그런 해결책은 그것의 구현 유연성을 제한하고, 항상 가능한 것도 아니다.

[0030] 그러나, 이들 기술들은 공통 단점을 공유한다; 즉, 스캔된 레이블들은 주어진 객체에 대해 물리적으로 동일하다. 따라서, 합법적인 레이블을 생성하는 제조 프로세스가 매우 정교할 수 있지만, 일반적으로 위조자가 가짜 패스오프(pass-off)를 생성하기 위한 방식을 결정하기 위해 많은 시간이 소요되지 않는다. 그리고, 일단 레이블이 한 번 성공적으로 복사되면, 그것은 반복적으로 재생성될 수 있다(즉, 낮은 비용으로 복제되는 마스터 본을 구성하여). 레이블이 주어진 수의 사용 후에 데이타베이스에 블랙리스트되지만, 처음 스캔된 레이블들이 실제로 진위의 레이블들이라는 보장이 없다.

[0031] 따라서, 현재 해결책들은 비교적 복사하기 어렵고 생성하기에 비용이 드는 레이블들을 제공하는데 실패한다.

발명이 이루고자 하는 기술적 과제

[0032] 본 명세서에 기재된 시스템 및 방법은 랜덤하게 분포된 객체들의 특징들의 인코딩에 관한 것이다. 일 양태에서, 랜덤하게 분포된 인증 객체의 특징들이 결정된다. 랜덤하게 분포된 특징들을 나타내는 데이타는 압축되고 서명으로 인코딩된다. 레이블은 생성되고, 인증 객체와 인코딩된 데이타를 포함한다.

[0033] 다른 양태에서, 데이타는 인증 객체와 연계된 확률 밀도 함수를 결정하기 위해 압축된다. 랜덤하게 분포된 속성들과 연계된 벡터들은, 적어도 부분적으로, 확률 밀도 함수에 기초하여 결정된다. 벡터들은 산술적 코딩 알고리즘을 사용하여 인코딩된다.

발명의 구성 및 작용

[0034] 본 명세서에 기재된 시스템 및 방법은 레이블에서 사용되는 랜덤하게 분포된 객체들의 특징들에 대한 정보의 인코딩에 관한 것이다. 레이블들은 항목에 첨부되거나 항목 내에 병합된 임의의 유형의 식별 수단을 포함할 수 있다. 인증되도록 구성된 레이블은 본 명세서에서 인증서(certificate of authenticity)로서 언급된다. 인증서에서 사용된 랜덤하게 분포된 특징들을 갖는 객체는 본 명세서에서 인증 객체라고 언급된다. 자체-인증을 인에이블하기 위해, 인증서는 인증 객체 및 랜덤하게 분포된 특징들에 대한 정보 모두를 포함할 수 있다. 압축 방법은 인코딩될 수 있고 인증서에 포함될 수 있는 랜덤하게 분포된 특징들에 대한 정보의 양을 증가시키기 위해 사용될 수 있다. 계산의 일 예에 따라, 인증서를 위조하는 비용은 정보의 압축에의 개선에 비례하여 지수함수적으로 증가된다. 이 위조 비용의 막대한 증가는 제조하기에 비교적 저렴하지만 위조하기는 어려운 신뢰성 있는 인증서를 결과적으로 만든다.

[0035] 도 1은, 인증서와 같이, 레이블의 일부로서 사용하기 위한 인증 객체(100)의 예를 도시한다. 인증서에 효과적으로 사용되기 위해, 인증 객체(100)는 통상적으로 고유하고 복제하기 어려운 랜덤하게 분포된 특징들을 포함한다. 도 1에 도시된 인증 객체(100)의 예는 파이버(fiber)-기반의 인증서의 일부이고, 랜덤 방식으로 객체에 임베딩된 파이버(110)를 포함한다. 파이버(110)는 랜덤하게 분포된 인증 객체(100)의 특징들로서 작용한다. 파이버(110)는 임의의 방식으로 인증 객체(100)에 병합될 수 있다. 예를 들어, 파이버(100)는 인증 객체(100)에 스프레이(spray)될 수 있다. 또한 파이버(100)는 제조 프로세스 동안에 인증 객체(100)로 병합될 수 있다. 일 실시예에서, 파이버(110)는 그들의 끝점들 간에 빛을 전송시킬 수 있는 광파이버이다. 그러므로, 인증 객체(100)의 특정 지역(120)에 빛을 쬐서, 조명된 지역 내의 적어도 한 끝점을 갖는 파이버(131) 내지 파이버(133)의 끝점들이 조명된다.

[0036] 도 1에서, 인증 객체(100)는 k개의 랜덤하게 분포된 파이버들을 포함한다. 인증 객체(100)는 L x L 픽셀의 해상도에 스캔될 수 있다. 각각의 파이버는 R의 고정 길이를 갖는다. 도 1의 인증 객체(100)의 예가 파이버들을 포함하지만, 랜덤하게 분포되는 다른 특징들을 갖는 인증 객체들은 또한 유사 방식으로 인증서에 사용될

수 있슴을 이해할 것이다.

[0037] 랜덤하게 분포된 인증 객체(100)의 특징들은 인증서에 사용되어, 제품과 같은, 임의의 객체의 진위성의 증명을 보호할 수 있다. 예를 들어, 랜덤하게 분포된 인증서의 특징들에 대한 특정 복제하기 어려운 데이타는 디지탈화될 수 있고, 발행자의 개인키(private key)로 싸인될 수 있고, 그 서명은 기계-판독가능 형태로 인증서에 프린트되어 생성된 인스턴스가 진위적인지를 확인할 수 있다. 인증서의 각각의 인스턴스는 발행자가 그 진위성을 보증하기를 원하는 객체와 연계된다. 일 실시예에서, 진위성의 확인은 발행자의 공개키(public key)를 사용하여 싸인된 데이타(랜덤하게 분포된 특징들에 대한 데이타)를 발췌하여서, 그리고 그 발췌된 데이타가 인증서의 연계된 인스턴스의 데이타와 매치하는지를 확인하여 이루어진다. 보호된 객체들을 위조하기 위해, 위조자는 다음 중 한 가지를 할 필요가 있다: (i) 발행인의 공개키를 알아낸다, (ii) 이미 서명된 인증서의 인스턴스를 정확하게 복제할 수 있는 제조 프로세스를 설계한다, 또는 (iii) 인증서의 서명된 인스턴스들을 횡령한다. 그 관점으로부터, 인증서는 그것의 가치가, 성공적 위조의 제조 프로세스의 축적된 소산을 포함하여, 1개의 인증서 인스턴스를 위조하는 비용을 대략적으로 초과하지 않는 제품들을 보호하기 위해 사용될 수 있다.

[0038] 인증서 시스템의 목적은 제품들 또는 제품과 연계된 특정 정보의 진위성을 보장하기 위한 것이다. 소프트웨어와 매체(예를 들어, DVD, CD) 반해적행위(antipiracy)로부터 위조불가 쿠폰과 변조방지 하드웨어의 설계에 이르기까지의 범위에서 응용 프로그램들의 세트는 많고도 넓다. 예를 들어, 변조방지 칩의 생성은 인증서로 그것의 패키지를 코팅하는 것을 필요로 할 것이다. 각각의 사용 전에, 인증서의 무결성은 보호된 실리콘의 진위성을 보장하기 위해 확인되어야 한다.

[0039] 아래에, 파이버-기반의 인증서의 랜덤하게 분포된 특징들의 저렴하고도 효과적인 판독을 위한 하드웨어 플랫폼의 예가 기재될 것이다. 하드웨어 플랫폼들은 바코드를 포함할 것이다. 저 비용의 판독기를 위한 바코드의 용량은 약 3K 비트로 제한되므로, 개인키에 의해 싸인된 메시지는 동일 길이로 제한된다. 또한, 인증서 시스템의 목적들 중의 하나는 인증서의 특정 인스턴스를 위조하려는 위조자의 노력을 최대화시키는 것이므로, 파이버-기반의 인증서의 고유하고 랜덤하게 분포된 특징들에 대한 가능한 많은 정보를 고정-길이의 싸인된 메시지에 저장하는 것과 연계된 문제가 기재된다. 파이버-기반 인증서에 대한 분석 모델의 예가 제공될 것이다. 그 다음, 아래 논의는 또한 포인트 세트의 압축 문제를 공식화할 것이고, 인증서의 인스턴스의 파이버들의 위치들의 최적의 압축은 NP-컴플리트(NP-complete)임을 보인다. 이 문제를 휴리스틱으로(heuristically) 해결하기 위해, 종래의 압축 방법들의 압축 비율들을 크게 개선하는 알고리즘이 제공될 것이다.

[0040] II. 인증서의 발행 및 확인

[0041] 도 2는 인증서 시스템(200)의 예 및, 인증서를 발행하고 확인하기 위해 상기 시스템에 의해 채택된 과정들의 예를 도시하는 개략도이다. 인증서 시스템(200)은 인증서(210), 발행자(230), 및 확인자(250)를 포함한다. 도 2에 도시된 바와 같이, 인증서(210)는 도 1의 인증 객체(100), 바코드(213), 및 텍스트(215)를 포함할 수 있다.

[0042] 인증서에서 보호될 필요가 있는 정보는 다음을 포함한다: (a) 복제하기 어려운 랜덤하게 분포된 인증 객체(100)의 특징들의 표현 및 (b) 임의로 연계된 텍스트 데이타. 초기에, 파이버들의 위치들과 같은, 랜덤하게 분포된 인증 객체(100)의 특징들은 하드웨어 디바이스를 사용하여 스캔된다. 어떻게 이 정보가 수집되고 표현되는지에 대한 세부사항들은 도 3과 연결하여 아래 논의될 것이다.

[0043] 논의를 위해서, 결과적 정보 f 가 n_F 비트의 랜덤 문자열임을 가정한다. 파라미터 n_F 은 고정되고, $n_F = k * n_{RSA}, k \in N$ 와 같고, 여기서, n_{RSA} 는 RSA 공개키(예를 들어, $n_{RSA} = 1024$)의 길이이고, k 은 $k \in [1,3]$ 로 일반적으로 세트된다. 주어진 고정된 n_F 에서, 랜덤하게 분포된 인증 객체(100)의 특징들을 나타내는 데이타(231)의 다이제스트 f 는 임의의 2개의 구별되는 인증서 인스턴스들 간의 거리를 통계적으로 최대화할 수 있다. 이 목적은 확인 단계 동안 음의 오류 및 양의 오류를 최소화하는 확률로 직접적으로 변환된다.

[0044] 텍스트 데이타 t 는 응용 프로그램에 종속하는 임의의 문자열(예를 들어, 만료일, 제조자 보증서)이다. 텍스트 데이타는 도 2에 도시된 바와 같이 인증서(210)에 프린트된 텍스트(215)로부터 유도된다.

[0045] 텍스트 데이타는, SHA1과 같은, 암호법으로 보안된 해쉬 알고리즘(237)을 사용하여 해쉬될 수 있다. 해쉬 함

수의 출력은 n_T 비트를 갖는 메시지 t로서 표현된다. 발행자(230)는 RSA에 의해 싸인될 수 있는 메시지 m을 생성한다. 예를 들어, 메시지 f와 t은 m의 각각의 비트가 f과 t로부터의 모든 비트에 종속됨을 보장하는 반전가능한 연산자 $\dot{\otimes}$를 사용하여 길이 $n_M = n_F$의 메시지 m으로 병합된다. 이 단계는 데이타(231)와 텍스트(215)에서 조작되어 특정 메시지 m을 생성할 필요가 있는 비트 수를 최대화할 수 있다. 그런 연산자의 예는 키로서 t 또는 t로부터의 비트들의 특정 서브세트를 사용한 f의 대칭 암호화 $m = t \dot{\otimes} f \equiv E_t(f)$이다. 메시지 m는 발행자(230)의 개인키(233)를 사용하여 RSA 서명(235)으로 싸인된다. m의 각각의 n_{RSA} 비트는 분리되어 싸인된다. 결과적 서명 s는 $n_S = n_M = n_F$비트를 갖는다. 이 메시지는 인증서(210)에 바코드(213)로서(PDF417 표준을 따르는 바코드와 같은) 인코딩되고 프린트된다.

[0046] 인증서(210)의 확인은 몇 개의 단계들과 연관된다. 확인자(250)는 초기에 프린트된 콤포넌트들, 텍스트(215) 및 바코드(213),을 스캔한다. 바코드(213)는 원래 프린트된 서명 s로 디코딩된다. 텍스트(215)는 메시지 t를 생성하기 위해 스캔되고 해쉬된다. 텍스트를 프린트하기 위해 사용된 폰트가 확인자(250)에게 공지되고 개선된 OCR을 위해 최적화되기 때문에 일반적 광학 문자 인식(OCR)은 이 작업이 필요하지 않음을 주목한다. 성공적인 인증서 확인을 위해, 텍스트(215)와 바코드(213)는 오류없이 판독될 필요가 있다; 이것은 현대 스캐닝 기술로 쉽게 성취될 수 있는 작업이다.

[0047] 확인자(250)는 발행자의 공개키(253)를 사용하여 s에 RSA 서명 확인(255)를 수행하고, 싸인된 메시지 m을 획득한다. 그 다음, 확인자(250)는 $f = m(\dot{\otimes})^{-1}t$를 계산할 수 있다. $\dot{\otimes}$으로서 암호화를 사용하는 예에서, 이것은 암호해독 $f = E_t^{-1}(m)$을 통해 성취된다. 다음, 확인자(250)는 랜덤하게 분포된 인증 객체(251)의 특징들을 나타내는 데이타(251)를 스캔하고, 그들의 표현 f'을 생성한다. 확인자(250)는 f'을 발췌된 f에 비교한다. 확인자(250)는 데이타의 2개 세트, 인증서에 첨가된 데이타 및 인증서의 서명을 생성하기 위해 사용되는 데이타, 간의 상관관계를 정량화할 필요가 있다. 결정 블록(259)에서, 2개의 데이타 세트들의 유사성의 레벨이 특정 임계치를 초과하면, 확인자(250)는 인증서(210)가 인증되었고 그 반대도 성립함을 공고한다.

[0048] 도 3a는 인증서와 연계된 랜덤하게 분포된 인증 객체(310)의 특징들을 캡춰링하는 스캐닝 시스템(300)의 예의 개략도이다. 스캐닝 시스템(300)은 광학 센서(322)와 광원(324)을 포함한다. 광학 센서(322)는 인증 객체(310)를 스캔하기 위해 구성되고, 특정 해상도의 CCD(Charged Coupled Device) 매트릭스를 포함할 수 있다. 일 실시예에서, 광학 센서(322)는 128 X 128 픽셀의 해상도를 갖는다. 광원(324)은 인증 객체(310)의 지역을 조명하기 위해 특정 파장의 빛을 제공하도록 구성된다. 광원(324)은, 예를 들어, 발광 다이오드(LED)를 포함할 수 있다. 도 3a에 도시된 바와 같이, 인증 객체(310)의 파이버(326)의 한쪽 끝이 광원(324)에 의해 조명된다. 빛은 파이버(326)의 다른쪽 끝으로 전송되고, 광학 센서(322)에 의해 감지된다.

[0049] 도 3b는 도 3a의 인증 객체(310)의 윗면도이다. 동작에서, 스캐닝 시스템(300)은, 영역(311) 내지 영역(314)과 같은, 영역들로 인증 객체(310)를 분리한다. 도 3b에 도시된 바와 같이, 스캐닝 시스템(300)의 광원(324)은 지역(311) 내지 지역(313)이 광원(324)으로부터 격리된 동안 지역(314)으로 빛을 쬔다. 지역(314)을 조명하여, 인증 객체(310)의 지역(311) 내지 지역(313)의 끝점들의 위치가 광학 센서(322)에 의해 결정될 수 있다. 그러므로, 랜덤하게 분포된 인증 객체(310)의 특징들의 판독은 4개의 다른 포인트 세트를 포함하는 4개의 디지탈 이미지를 포함한다. 각각의 포인트 세트는 특정 지역과 연계되고, 그 지역을 조명하여 결정된다.

[0050] 나노기술과 같은 기술의 발달은 전자 디바이스가 인증서로부터의 랜덤하게 분포된 특징들을 디코딩하도록 할 수 있고, 이들 특징들에 대응하는 빛 패턴을 생성할 수 있슴을 이해할 수 있다. 그런 디바이스는 인증서를 위조할 수도 있다. 일 실시예에서, 스캐닝 시스템(300)은 광원(324)에 의해 사용되는 빛의 파장(즉, 칼라)을 변화시켜서 위조하는 이 방법을 막기 위해 구성될 수 있다. 예를 들어, 빛의 파장은 인증 객체가 스캐닝 시스템(300)에 의해 스캔되는 랜덤하게 선택되는 각각의 시간일 수 있다. 광학 센서(322)는 인증 객체에서 파이버에 의해 방사되는 빛의 파장을 검출하고, 그 파장이 광원(324)에 의해 방사되는 빛의 파장에 대응하는지를 판정하기 위해 구성될 수 있다. 방사되고 검출된 빛의 파장들이 매치하지 않으면, 인증서는 위조일 가능성이 있다.

[0051] 도 4는 인증서를 생성하기 위해 사용될 수 있는 프로세스(400)의 예의 흐름도이다. 블록(405)에서, 인증서의 인증 객체는 스캔된다. 인증 객체는 도 3a에서 스캐닝 시스템(300)을 사용하여 스캔될 수 있다.

[0052] 블록(410)에서, 랜덤하게 분포된 인증 객체의 특징들을 나타내는 데이타가 결정된다. 파이버-기반 인증 객체에서, 도 3b에 도시된 끝점들과 같이, 데이타는 조명된 파이버들의 끝점들의 위치들을 포함할 수 있다.

[0053] 블록(415)에서, 데이타는 인증서의 보안 레벨을 향상시키기 위해 압축한다. 데이타 압축은 도 5와 연결하여 상세히 논의될 것이다. 간략하게 기재하면, 경로는 인증 객체에서 랜덤하게 분포된 특징들을 나타내는 데이타의 일부를 압축하기 위해 결정될 것이다.

[0054] 블록(420)에서, 압축 데이타가 인코딩된다. 예를 들어, 압축된 데이타는 도 2의 개인키를 사용하여 싸인될 수 있다. 블록(425)에서, 인코딩된 데이타는 인증서에 병합된다. 예를 들어, 인코딩된 데이타는, 도 2의 바코드(213)와 같은, 바코드로서 인증서에 프린트될 수 있다.

[0055] 도 5는 랜덤하게 분포된 인증 객체의 특징들을 나타내는 데이타를 압축하기 위해 사용할 수 있는 프로세스(500)의 예의 흐름도이다. 논의를 목적으로, 프로세스(500)는 파이버-기반의 인증서의 콘텍스트로 설명될 것이다. 그러나, 프로세스(500)는 임의의 유형의 인증서에 적용될 수 있을 것이다.

[0056] 블록(505)에서, 인증 객체와 연계된 확률 밀도 함수가 결정된다. 확률 밀도 함수는 섹션 III-A에서 기재될 것이다. 확률 밀도 함수의 예는 수학식 11에 표현된다. 확률 밀도 함수의 예의 그래프 표현은 도 8에 도시된다. 간략하게 기재된 확률 밀도 함수는 랜덤하게 분포된 속성들의 유닛이 인증 객체의 특정 위치에서 발견되는 확률을 나타낸다. 파이버-기반의 인증서의 콘텍스트에서, 확률 밀도 함수는 인증 객체의 지역의 특정 포인트가 조명되는 확률을 나타낼 수 있다. 확률 밀도 함수는 또한 전체 파이버들 중 얼마나 많이 특정 지역에서 조명될 것인지를 계산하기 위해 사용될 수 있다.

[0057] 블록(510)에서, 랜덤하게 분포된 속성들과 연계된 벡터들이 결정된다. 파이버-기반 인증서의 콘텍스트에서, 포인트-투-포인트(point-to-point) 벡터들이 사용되고, 섹션 IV-A에서 논의될 것이다. 특히, 수학식 16은 포인트-투-포인트 벡터들을 계산하기 위해 사용되어 파이버-기반 인증서의 랜덤하게 분포된 속성들을 나타낼 수 있다.

[0058] 블록(515)에서, 벡터들은 산술적 코딩 알고리즘을 사용하여 인코딩될 수 있다. 산술적 인코딩 알고리즘은 섹션 IV-A에서 논의될 것이다. 알고리즘의 예는 표 2에서 도시된다.

[0059] 블록(520)에서, 고정된 양의 데이타 내에 벡터들의 일부를 압축하는 경로가 결정된다. 경로를 계산하는 방법이 섹션 IV-B에서 논의된다. 경로의 예는 수학식 20을 사용하여 계산될 수 있다. 블록(525)에서, 랜덤하게 분포된 속성들의 일부를 나타내는 압축 데이타의 경로가 리턴된다.

[0060] III. 인증서 모델

[0061] 이 섹션에서, 파이버-기반 인증서의 분석적 모델이 논의된다. 인증서 S 의 2개의 특징들이 모델링된다. 인증서의 특정 지역 S_i 이 조명되면, $S-S_i$ 의 특정 포인트가 조명되는 확률 밀도 함수가 계산된다. 또한, K 파이버들이 S 에 있으면, $S-S_i$ 에 조명되는 파이버들의 기대되는 수가 또한 계산된다.

[0062] A. 조명된 파이버 끝점들의 분포

[0063] 인증 객체(L,R,K)는 객체에 대해 랜덤하게 뿌려진 고정 길이 $R \le L/2$ 의 K 파이버들과 L 유닛의 에지를 갖는 스퀘어(square)로서 모델링된다. 변동 파이버 길이 또는 임의의 형상 인증 객체와 같은, 다른 모델 변이본들이 이 모델로부터 유도될 수 있다. 인증 객체는 도 1에 도시된 바와 같이 2D 직교좌표계의 양의 사분면(quadrant)에 위치된다. 추가로, 인증 객체는 4개의 동일 스퀘어들 $S=\{S_1,S_2,S_3,S_4\}$ 로 분리된다. 그들의 각각은 도 3a와 3b와 연결하여 위에 기재된 바와 같이 3D 파이버 구조를 기록하기 위해 사용된다. 그 다음, 파이버는 포인트들 간의 거리가 $\|A-B\|=R$ 가 되도록, 포인트들 $A,B \subset S$ 의 순서쌍 $f=\{A,B\}$ 으로서 표현된다.

[0064] 정의 1. 조명된 파이버 끝점들의 분포

[0065] 스퀘어 S_i 중의 한 개가 조명되면, 임의의 영역 $P \subset S-S_i$ 가 파이버 $f=\{A,B\}$ 의 한 조명된 끝점 A 를 포함

하고 다른 끝점 B는 조명된 지역 S_i에 위치되는 사실을 조건으로 하는 확률 $\xi(i,P)$를 통해 임의의 포인트 $Q(x,y)\subset S-S_i$에 대해 확률 밀도 함수 (pdf) $\varphi(i,Q(x,y))$가 정의된다. 더 공식적으로는, 임의의 $P\subset S-S_i$에 대해 다음이 성립한다:

수학식 6

$$\xi(i,P)=\Pr[A\subset P\mid f=\{A,B\}\subset S,B\subset S_i]$$

$$=\iint_{Q(x,y)\subset P}\varphi(i,Q(x,y))\mathrm{d}x\mathrm{d}y.$$

[0066]

[0067] 인증 객체로의 파이버 $f=\{A,B\}$의 흩뿌림은 다음의 2개의 독립적 이벤트들로 구성됨을 가정한다: (i) 제1 끝점 A는 인증 객체에 위치하고, (ii) 제2 끝점 B은 인증 객체에 닿는다. A는 COA()의 임의의 장소에 위치할 수 있고, B의 위치는 A의 위치에 종속된다. 끝점 B는 반경이 R인 A 주위에 중심이 있고, 인증 객체 내에 포함되는 원의 둘레의 일부에 위치해야 한다. 이 서브섹션의 나머지 부분에서, 함수 $\varphi(i,Q(x,y))$는 이벤트(i) 내지 이벤트(ii)의 분석에 기초하여 분석적으로 계산된다. 단순성을 위해, 단지 $\varphi(1,Q(x,y))$이 지역 S_1가 조명될 때의 경우에 대해 계산된다. $\varphi(1,Q(x,y))$는 2개의 단계들에서 계산된다.

[0068] 정의2. 둘레 포함

[0069] 첫번째로, 주어진 포인트 $A\subset S$에서, 전체 인증 객체 S에 의해 포함되는 반경 R를 갖는 A에 중심이 있는 원의 둘레(원호)의 일부의 길이를 측정하는 둘레 포함 함수 $\varrho(A)$가 정의된다. 인증 객체에 4개의 상이한 지역들(도 6에서 P1으로부터 P6로 표시됨)이 있고, 여기서 $\varrho(A)$가 일정하게 계산된다.

[0070] 도 6은 인증 객체(600)의 예의 4개의 상이한 영역들에 대응하는 영역(P1) 내지 영역(P4)의 그래프 표현이다. 특정 영역 PX의 각각의 포인트에 대해, 둘레 포함 함수는 아래 기재되는 바와 같이 수학식 7 내지 수학식 10을 사용하는 그 영역에 대해 구별되는 폐쇄 분석 형식(closed analytical form)을 사용하여 계산된다.

[0071] 영역 P1. 이것은 인증 객체의 중심 영역이고, 여기서 임의의 포인트 $Q\subset \mathrm{P1}$에 대해, Q에 중심이 있는 반경 R의 원은 인증 객체의 임의의 에지와도 교차하지 않는다. 그 영역은 다음에 의해 제한된다: $R\le x\le L-R$, $R\le y\le L-R$.

수학식 7

[0072] $$\varrho(Q(x,y))=2R\pi.$$

[0073] 영역 P2. 4개의 상이한 P2 영역들이 있고, 여기서 임의의 포인트 $Q\subset \mathrm{P2}$에 중심이 있고 반경이 R인 원은 인증 객체의 정확히 1개의 에지와 2번 교차한다. 단순성을 위해, 다음의 경우만을 고려한다: $R\le x\le L-R,\ 0\le y<R$. 다른 3개의 지역들의 수학식들은 대칭적으로 계산될 수 있다.

수학식 8

[0074] $$\varrho(Q(x,y))=R\left[\pi+2\arcsin\left(\frac{y}{R}\right)\right]$$

[0075] 영역 P3. 4개의 상이한 P3 영역들이 있고, 여기서 임의의 포인트 $Q\subset \mathrm{P3}$에 중심이 있고 반경이 R인 원은 인증 객체의 2개의 상이한 에지들과 2번 교차한다. 다음의 경우만을 고려한다: $0\le x<R$,

$0 \le y < R,\ x^2 + y^2 \ge R^2$

수학식 9

[0076] $$\varrho(Q(x,y)) = 2R\left[\pi - \arccos\left(\frac{x}{R}\right) - \arccos\left(\frac{y}{R}\right)\right]$$

[0077] 영역 P4. 4개의 상이한 P4 지역들이 있고, 여기서 임의의 포인트 $Q \subset \mathrm{P4}$ 에 중심이 있고 반경이 R 인 원은 COA의 2개의 에지들과 1번 교차한다. 다음의 경우만을 고려한다: $x^2 + y^2 < R^2$.

수학식 10

[0078] $$\varrho(Q(x,y)) = R\left[\frac{\pi}{2} + \arcsin\left(\frac{x}{R}\right) + \arcsin\left(\frac{y}{R}\right)\right]$$

[0079] 모든 수학식 8 내지 수학식 10에서, $\{0, \pi/2\}$ 내의 함수 $\arcsin(\cdot)$ 과 $\arccos(\cdot)$ 의 리턴 값들만이 고려된다.

[0080] 제2 단계에서, B 가 S_i 에 의해 포함되고 지름이 R 이고 $Q(x,y)$ 에 중심이 있는 원 $C(Q,R)$ 의 부분(들)에 위치하기만 하면, 파이버 $f = \{A, B\}$ 의 조명된 끝점 A 가 위치 $A = Q(x,y)$ 에 있는 사실에 기초하여 실제 $\varphi(1, Q(x,y))$ 가 계산된다.

[0081] 정리 3. $\varrho(Q(x,y))$ 로부터의 $\varphi(i, Q(x,y))$ 의 종속성

[0082] 함수 $\varrho(Q(x,y))$ 를 사용하여, pdf $\varphi(i, Q(x,y))$ 는 다음 적분을 사용하여 계산된다:

수학식 11

[0083] $$\varphi(i, Q(x,y)) = \int_{C(Q,R) \subset S_i} \frac{\alpha R \mathrm{d}\vartheta}{\varrho(Q(x + R\cos\vartheta, y + R\sin\vartheta))}$$

[0084] 여기서, ϑ 은 $C(Q,R) \subset S_i$ 의 둘레를 브라우징하고, α 는 다음을 성립하도록 하는 상수이다:

수학식 12

[0085] $$\iint_{Q(x,y) \subset S - S_i} \varphi(i, Q(x,y)) \mathrm{d}x\mathrm{d}y = 1$$

[0086] 포인트 $Q \subset S - S_i$ 는 $B \subset S_i$ 이 되도록 단지 파이버 $f = \{Q, B\}$ 때문에만 조명될 수 있다. 이것은 B 가 S_i 에 의해 포함된 원 $C(Q,R)$ 의 둘레의 어떤 부분에 위치됨을 내포한다. 주어진 파이버 $f = \{A, B\}$ 에 대해, A 가 길이 $\mathrm{d}l \subset S$ 의 특정한 미세하게 작은 원호에 위치하는 확률은 $\mathrm{d}l / \varrho(B)$ 과 같다.

[0087] 그러므로:

수학식 13

[0088] $$\varphi(i, Q) = \mathrm{area}(S - S_i)^{-1} \int_{C(Q,R) \subset S_i} \frac{4R\mathrm{d}l\mathrm{d}\vartheta}{\varrho(B(Q,R,\vartheta) \subset C)\mathrm{d}l}$$

[0089] 여기서, 함수 $\mathrm{area}(S - S_i)$ 은 $S - S_i$ 하의 면적을 계산한다. 그러므로, 포인트 $Q \subset S - S_i$ 에의 pdf $\varphi(1, Q(x,y))$ 는

$C(Q,R) \subset S_1$에 대해 $\varrho(\cdot)$의 값의 인버스(inverse)의 적분에 비례한다.

[0090] 도 7은 도 11에서 정량화된 적분으로의 솔루션으로서 구분되는 분석 공식을 갖는 인증 객체(700)의 예에 19개의 상이한 지역들의 그래프 표현이다. 단순성을 위해, $\varphi(1,Q(x,y))$는 간단한 수치 계산을 사용하여 근사치로 해결된다. 그 결과는 도 8에 도시된다.

[0091] 도 8은 단위 포인트들에서 샘플링된 파라미터 $L=64$와 파라미터 $R=28$를 갖는 스퀘어 인증 객체에 대한 확률 밀도 함수의 예의 그래프이다. 도 8은 파이버의 한 끝점이 특정의 작은 영역 $P \subset S-S_1$에 위치할 확률은 $S-S_1$ 내의 P의 특정 위치에 종속하여 크게 달라짐을 도시한다. $S-S_i$에서의 $\varphi(i,Q(x,y))$의 분산에 대한 정보를 사용하여, 포인트-서브세트 압축 알고리즘들은, 섹션 IV에서 표현된 바와 같이, 크게 개선될 수 있다. 전체 영역 $S-S_i$에 대해 $\varphi(i,Q(x,y))=const.$이도록 인증 객체를 제조하는 것은 사소한 작업이 아니고, 아마도 원래의 인증 객체를 위조하는 것만큼 어려울 것이다.

표 1

Area	Bounds	$\psi(1,Q(x,y))$
T0	$0 \le x \le L/2-R,\ 0 \le y \le L/2-R$	0
T1	$x^2+(y-L/2)^2 < R^2,\ 0 \le x \le L/2-R,$ $L/2-R < y \le L/2$	$R\left[\arcsin\left(\frac{x}{R}\right)+\arccos\left(\frac{L/2-y}{R}\right)\right]$
T2	$x^2+(y-L/2)^2 \ge R^2,\ 0 \le x \le L/2-R,$ $L/2-R < y \le L/2$	$2R\arccos\left(\frac{L/2-y}{R}\right)$
T3	$x^2+(y-L/2)^2 \ge R^2,$ $(x-L/2)^2+y^2 \ge R^2,$ $(x-L/2)^2+(y-L/2)^2 \ge R^2$	$2R\left[\arccos\left(\frac{L/2-y}{R}\right)+\arccos\left(\frac{L/2-x}{R}\right)\right]$
T4	$x^2+(y-L/2)^2 < R^2,$ $(x-L/2)^2+y^2 < R^2,$ $(x-L/2)^2+(y-L/2)^2 \ge R^2$	$R\left[\arcsin\left(\frac{x}{R}\right)+\arcsin\left(\frac{y}{R}\right)\right]$ $R\left[\arccos\left(\frac{L/2-y}{R}\right)+\arccos\left(\frac{L/2-x}{R}\right)\right]+$
T5	$x^2+(y-L/2)^2 < R^2,$ $(x-L/2)^2+y^2 < R^2,$ $(x-L/2)^2+(y-L/2)^2 < R^2$	$R\left[\frac{\pi}{2}+\arcsin\left(\frac{x}{R}\right)+\arcsin\left(\frac{y}{R}\right)\right]$
T6	$x^2+(y-L/2)^2 < R^2,$ $(x-L/2)^2+y^2 \ge R^2,$	$R\left[\arcsin\left(\frac{x}{R}\right)+\arccos\left(\frac{L/2-y}{R}\right)\right]+$ $2R\arccos\left(\frac{L/2-x}{R}\right)$
	$(x-L/2)^2+(y-L/2)^2 \ge R^2,$ $L/2-R < x \le L/2$	
T7	$x^2+(y-L/2)^2 < R^2,$ $(x-L/2)^2+y^2 \ge R^2,$ $(x-L/2)^2+(y-L/2)^2 < R^2$	$R\left[\frac{\pi}{2}+\arcsin\left(\frac{x}{R}\right)+\arccos\left(\frac{L/2-x}{R}\right)\right]$
T8	$x^2+(y-L/2)^2 \ge R^2,$ $(x-L/2)^2+y^2 \ge R^2,$ $(x-L/2)^2+(y-L/2)^2 < R^2$	$R\left[\frac{\pi}{2}+\arccos\left(\frac{L/2-y}{R}\right)+\arccos\left(\frac{L/2-x}{R}\right)\right]$

[0092]

[0093] B. 파이버 끝점들의 조명 비

[0094] 정의 3. 파이버 끝점들의 조명 비.

[0095] 인증 객체(L,R,K)와 그것의 조명된 지역 S_i에 대해, 끝점들 중의 1개가 $B \subset S-S_i$에 있고 다른 끝점이 $A \subset S_i$에 있는 사실을 조건으로 하여 파이버 $f=\{A,B\}$가 위치되는 확률로서 조명 비율 λ가 정의된다.

수학식 14

[0096] $$\lambda = \Pr[B \subset S-S_i \mid f=\{A,B\}, A \subset S_i]$$

[0097] 정의 4. 조명가능한 원호.

[0098] 임의의 포인트 $A \subset S_i$ 에 대해, $S-S_i$ 에 의해 포함된 $C(A,R)$ 의 둘레의 부분의 길이를 측정하는 함수 $\psi(i,A(x,y))$ 가 정의된다.

[0099] 도 9는 영역(T0) 내지 영역(T8)의 그래프 표현이고, 여기서 $\psi(i,Q(x,y))$ 는 명백한 폐쇄 분석 형식들을 사용하여 계산된다. $\psi(i,Q(x,y))$ 는 섹션 III-A로부터 이벤트(i) 내지 이벤트(ii)의 분석에 기초하여 분석적으로 계산된다. 섹션 III-A에 유사하게, 지역 S_i 이 조명될 때의 경우에만 계산된다. COA에 9개의 상이한 지역들(도 9에 T0에서 T8로 표시됨)이 있고, 여기서 $\psi(1,Q)$ 는 일정하게 계산된다. S_i 내의 Q 의 위치에 종속하는 $\psi(1,Q)$ 에 대한 폐쇄 분석 형식들은 표 1에 주어진다:

[0100] 정리 4. $\psi(1,Q(x,y))$, $\rho(Q(x,y))$, 및 λ 의 종속성

[0101] 정의 3에 정의된 조명 비는 다음과 같이 계산될 수 있다:

수학식 15

[0102] $$\lambda = \int_{Q(x,y)\subset S_i} \frac{\psi(i,Q(x,y))}{\rho(Q(x,y))} dxdy.$$

[0103] 반경 R 를 갖고 포인트 $A \subset S$ 에 중심이 있는 원은 $C(A,R)$ 로서 표현된다. 각각이 포인트 $Q \subset S_i$ 에 대해, 파이버 $f=\{Q,B\}$ 의 다른 끝점 B 가 $S-S_i$ 내에 위치하는 확률은 $S-S_i$ 과 S 각각에 의해 포함되는 $C(Q,R)$ 의 둘레의 부분들의 길이들의 비율과 같다. S_i 내의 모든 포인트들에 대한 이 비율을 적분하여, 수학식 15가 얻어진다.

[0104] 주어진 인증 객체(L,R,K)에서, 수학식 15와 표 1로부터의 $\psi(1,Q)$ 에 대한 폐쇄 형식(closed forms)을 수치적으로 근사하여 계산되는 λ 를 사용하여, S_i 이 $\lambda K/2$ 로서 조명될 때 $S-S_i$ 내의 조명된 포인트들의 기대 수가 계산될 수 있다. 예를 들어, 인증 객체(64,28,100)에 대해, 결과는 $\lambda \approx 0.74$ 이고, 이것은 평균적으로 S_i 의 경우에 조명된 끝점들의 수가 대략 $0.74 \cdot 50 = 37$ 임을 의미한다.

[0105] IV. COA의 포인트-서브세트의 압축

[0106] 인증서 시스템의 목적은 특정한 인증 객체의 인스턴스를 제조하는(즉, 위조) 작업이 가능한 어렵도록 하는 것이다. 이 목적은 인증 객체의 가능한 많은 파이버들의 위치들을 기록하는 요구로서 정량화된다. 압축 알고리즘의 예에서, 인증 객체의 지역들의 수는 4와 같다. 그러므로, 각각의 지역 S_i 에 대해, 싸인된 메시지 m 의 비트들의 1/4인 $n_M/4$ 는 일단 빛이 S_i 에 조명되면 $S-S_i$ 에 조명된 가능한 많은 파이버 끝점들을 저장하기 위해 전용된다. 일반적으로, 모든 조명된 포인트들이 저장될 필요가 있는 것은 아님을 주목한다. 단지 $n_M/4$ 비트들을 사용하여 인코딩될 수 있는 이들 포인트들의 가장 큰 서브세트만이 저장될 필요가 있다.

[0107] 이 섹션에서, 인증 객체의 2개의 조명된 포인트들 간의 거리를 인코딩하기 위해 구성되는 메카니즘이 설명된다. 메카니즘은 산술적 인코딩에 기초된다. 다음, 일정 수의 비트들을 사용하여 가능한 많은 수의 파이버 끝점들을 압축하는 문제가 공식화된다. 최종적으로, 논의는 이 문제가 NP-컴플리트(NP-complete)임을 보일 것이고, 서브-최적화 솔루션으로서 구성적 휴리스틱이 제공된다.

[0108] A. 포인트-투-포인트 벡터들의 인코딩

[0109] 이 서브섹션에서, 어떻게 그것의 시작과 끝 포인트에 의해 정의된 벡터가 비트들의 최소-근접(near-minimal) 수를 사용하여 인코딩되는지가 기재된다. 추가 제한점은 고려되는 영역의 포인트들은 주어진 pdf에 따라 발생한다는 것이다.

[0110] 1) 산술 코딩:

[0111] 산술 코더(AC)는 임의의 길이의 입력 스트림을 $[0,1)$ 내의 1개의 유리수로 변환한다. AC의 주요 장점은 그것이 엔트로피에 임의로 근접하게 압축할 수 있다는 점이다. 아래 논의는 부호 출현의 비공지된 pdf로 알파벳이 주어지면 어떻게 단어 "abc"가 인코딩되는지를 보여준다.

[0112] 도 10은 부호 출현의 비공지된 pdf로 알파벳 $L=\{a,b\}$ 이 주어지면 어떻게 산술 코더가 문자열 "abc"를 인코딩하는지의 예의 그래픽 표현이다. 그 예는 도 10에 도시된다. 초기에, AC의 범위는 $[0,1)$ 로 리세트(reset)되고, L 의 각각의 부호는 출현의 동일 확률, $\Pr[a]=\Pr[b]=1/2$,이 주어진다. 그러므로, AC는 그것의 범위를 각각 "b"와 "a"를 나타내는 2개의 서브범위 $[0,0.5)$ 와 $[0.5,1)$ 로 분리한다. 부호 a 는 이 부호에 대응하는 범위, 즉 $[0.5,1)$,로 AC의 범위를 제한하여 인코딩된다. 추가로, AC는 부호 "a"의 출현에 대한 카운터를 갱신하고, $\Pr[a]=2/3$ 과 $\Pr[b]=1/3$ 를 재계산한다. 다음 번 반복에서, 갱신된 $\Pr[a],\Pr[b]$ 에 따라, AC는 각각이 "b"와 "a"를 나타내는 $[0.5,0.6667)$ 과 $[0.6667,1)$ 로 그것이 범위를 분리시킨다. "b"가 다음에 도착할 때, AC는 대응하는 $[0.5,0.6667)$ 으로 그것의 범위를 축소시키고, $\Pr[a]=\Pr[b]=2/4$ 를 갱신시키고, 새 범위를 각각이 "b"와 "a"를 나타내는 $[0.5,0.5833)$ 와 $[0.5833,0.6667)$ 로 분리시킨다. 최종 부호가 "a"이므로, AC는 출력으로서 $[0.5833,0.6667)$ 내에 임의의 수를 선택하여 이 부호를 인코딩한다. 가장 적은 수의 비트들(이 예에서의 숫자들)로 인코딩되는 수를 선택하여, 0.6, AC는 그것의 최종 출력을 생성한다. 디코더는 압축된 메시지의 헤더에서 명백하게 또는 특수 "파일끝(end-of-file)" 부호를 통해 메시지 길이를 안다.

[0113] AC는 그것의 범위가 높고 낮은 한계의 첫번째 숫자가 동일하게 될 때의 포인트까지 그것의 동작 범위를 축소시킨다. 그 다음, 그 첫번째 숫자는 전송될 수 있다. 재정규화(renormalization)라고 불리우는 이 프로세스는 제한된 정확성 산술 단위의 임의의 길이의 파일들의 압축을 인에이블시킨다. 클래식 AC의 성능 개선은 산술 계산의 미리 계산된 근사치들을 사용하고 나눗셈과 곱셈을 쉬프팅(shifting)과 덧셈으로 대체하는 것에 중점을 둔다.

[0114] AC는 소스의 엔트로피, $H(s)=-\sum_{s_i}\Pr[s_i]\log_2(\Pr[s_i])$,와 같은 비트들의 수를 사용하여 인입 부호들 $s=s_1,s_2,\ldots$ 의 시퀀스를 인코딩한다. 그러므로, 독립적으로 동일하게 분포된(independent and identically distributed) 부호들의 반-무한의(semi-infinite) 스트림에 대해, 무한 정확성 산술(infinite precision arithmetic)의 컴퓨터 상에서, AC는 최적의 엔트로피 코더이다.

[0115] 2. 최소거리 포인-투-포인트 벡터의 산술 인코딩

[0116] 주어진 인증 객체(L,R,K)에서, 빛은 그것의 사분면들, S_i , 중의 하나에 조명됨이 가정된다. 다음, 인증 객체는 $L\times L$ 단위 스퀘어들 $U=u(i,j),i=1\ldots L,j=1\ldots L$ 의 그리드로 분할되고, 여기서 각각의 $u(i,j)$ 는 $x\in\{i-1,i],y\in\{j-1,j]$ 내의 스퀘어 영역을 커버한다. 단위 영역들은 인증 객체의 디지탈 스캔의 픽셀들을 모델링한다. 스캔의 해상도는 $L\times L$ 과 같다. 다음, 단위 $u(x,y)$ 의 주요 포인트는 좌표 (x,y) 를 갖는 포인트 Q_u 로서 정의된다.

[0117] 정리 5. 단위 조명 확률

[0118] $S-S_i$ 에 정확히 1개의 끝점을 갖는 κ 파이버들이 있다고 가정하면, 임의의 단위 영역 $u(x,y)\subset S-S_i$ 이 적어도 1개의 조명된 파이버 끝점을 포함하는 확률은 다음과 같다:

수학식 16

[0119]
$$\tau(u)=\Pr[(\exists f=\{A,B\}\in F)A\subset u,B\subset S_i]$$
$$=1-[1-\xi(i,u)]^{\kappa}.$$

[0120] 및

$$\tau(u) = \Pr[(\exists f = \{A, B\} \in F) A \subset u, B \subset S_i] = 1 - \Pr[(\neg \exists c \in F) A \subset u, B \subset S_i] = 1 - (1 - \Pr[A \subset u, B \subset S_i \mid f = \{A, B\}])^{\kappa}$$

[0121]

[0122] 수학식 7로부터, 수학식 16이 귀결된다. 섹션 III-B에서, κ 에 대한 기대값, $E[\kappa] = \lambda K/2$, 이 계산된다.

[0123] 문제 1. COA에 대한 듀얼(dual) 벡터 인코딩.

[0124] 단위 $u \subset S - S_i$ 가 조명된 파이버 끝점을 포함한다는 사실들을 조건으로, 목적은 가능한 적은 수의 비트들을 사용하여 단위 u 에 관련된 2개의 다른 조명된 단위들 v_1 와 v_2 의 위치들을 인코딩하는 것이다. 추가 제한점은, $S - S_i$ 의 모든 조명된 단위들 간에, v_1 과 v_2 의 주요 포인트들, Q_1 과 Q_2 각각은 u 의 주요 포인트, Q_u , 로부터 2개의 최단 유클리드 거리들에 위치된다는 점이다. 단위들의 세트 $V, |V| > 1$ 가 u 에 대해 동일 거리 상에 있으면 조명의 최고의 확률 $\text{argmax}_{v \subset V}(\tau(v))$ 를 갖는 것이 먼저 인코딩된다.

[0125] <알고리즘 A1>

표 2

Set U as a list of all unit areas in $S - S_i - u$.
List of all marked units, $M(u)$, is set to $M(u) = \varnothing$.
do
  Find all unit areas $V = \text{argmin}_{v \subset U} \| Q_v - Q_u \|$.
  do
    Find unit area $w = \text{argmax}_{v \in V} \xi(1, v)$.
    Set AC range for w to $\gamma(w,u)$ (see Eqns.17,18).
    Set of nodes ordered before w is $M_w(u) = M(u)$.
    $M(u) = M(u) \cup w$, $V = V - w$, $U = U - w$.
  while $V \neq \varnothing$
while $U \neq \varnothing$

[0126]

[0127] 단위-대-단위(unit-to-unit) 벡터의 인코딩은 알고리즘 A1을 사용하여 각각의 인코딩 부호에 대해 인코딩 간격에 대응하는 범위를 할당하는 - 즉, 각각의 단위 $v \subset S - S_i$ 는 소스 단위 u 와는 상이함- AC를 사용하여 성취된다. 각각의 단위 v 에 대해, 알고리즘 A1은 v 가 소스 단위 u 에 대해 2개의 가장 근접한 조명된 단위들 중의 하나인 확률과 동일한 범위를 할당한다. 이 확률은 $p(v|u)$ 로서 표현된다. $\kappa \gg 1$ 단위들이 $S - S_i$ 에 조명되는 것이 기대될 때의 경우에, $p(v|u)$ 가 다음과 같이 계산될 수 있다:

수학식 17

$$p(v|u)=\tau(v)\prod_{w\subset M_v(u)}[1-\tau(w)]+$$

$$\sum_{w\subset M_v(u)}\tau(v)\tau(w)\prod_{z\subset M_v(u),z\neq w}[1-\tau(z)]$$

[0128]

[0129] 여기서, 단위들의 세트 $M_v(u)$는 알고리즘 A1으로서 계산된다. 각각의 단위 v에 대해, 알고리즘 A1은 AC에 의해 사용되는 범위 $\gamma(v,u)$를 할당하여 u가 이미 인코딩된 사실을 조건으로 하는 v를 인코딩한다. 이 범위는 다음과 같다:

수학식 18

$$\gamma(v,u)=\frac{p(v|u)}{\sum_{w\subset S-S_i}p(w|u)}$$

[0130]

[0131] 그러므로, 부호들의 시퀀스가 다음의 소스 엔트로피와 근사하게 같은 비트들의 수를 사용하여 인코딩되기 때문에, 2개의 가장 근접하게 조명된 단위들은 최적에 근사하는(즉, 인코딩은 무한 정확성 산술적 프로세서 상에서 최적화됨) 구성에 의해 인코딩된다:

수학식 19

$$H(u)=-\sum_{v\subset S-S_i}\gamma(v,u)\log_2[\gamma(v,u)]$$

[0132]

[0133] 듀얼 벡터 인코딩은 프리미티브(primitive)로서 사용되어 섹션 IV-B에서 제공된 전체 압축 알고리즘에서의 포인트들의 서브세트를 인코딩한다. 인코딩 알고리즘이 섹션 IV-A.2에서 제공된 가정들의 세트에 대해 최적에 근접하지만, 제한점들의 동일 세트는 전체 압축 목적에 대해 유효하지 않으므로, A1을 통한 범위 할당으로 산술 코딩을 사용하는 고유의 최적화가 섹션 IV-B에서 논의된다.

[0134] B. 포인트 서브세트의 압축

[0135] 고정된 수의 비트들을 사용하여 가능한 많은 조명된 단위 영역들의 위치들을 압축하는 최적화 문제가 모델링된다. 다음의 가중된 에지들을 갖는 방향성 컴플리트 그래프(directed complete graph)를 고려한다. 각각의 조명된 단위 $u\subset S-S_i$에 대해, 노드 n_u가 생성된다. 노드 n_u로부터 노드 n_v로의 방향성 에지 $e(u,v)$는, 수학식 19에서와 같이 $\omega(e(u,v))=-\log_2[\gamma(v,u)]$으로 u가 이미 인코딩되었다는 사실을 조건으로 하여, v를 가리키는 벡터를 인코딩하는 코드워드(codeword)의 최적의 길이로 가중된다. 이 그래프를 $G(N,E,\Omega)$로 표현하고, 여기서 N, E, 및 Ω은 노드들의 세트, 방향성 에지들, 및 대응하는 가중치들을 각각 나타낸다고 하자.

[0136] 문제 2. 포인트 서브세트의 압축(CPS)

[0137] 인스턴스: 음이 아닌 꼭지점 함수 $\Omega:E\rightarrow R$, 양의 정수 $l_{min}\in Z^+$, 양의 실수 $\Lambda\in R^+$를 갖는 방향성, 컴플리트, 및 가중된 그래프 $G(N,E)$.

[0138] 문제: 경로를 따라 가중치들의 합이 다음과 같도록, 노드들을 통한 경로를 갖는 노드들 $N^*\subset N$, $l>l_{min}$, 의 서브세트, 즉, 순열 $<n^*_{\pi(1)},\ldots,n^*_{\pi(l)}>$, 가 있는가?:

수학식 20

[0139] $$\sum_{i=1}^{l-1} \omega(e(n^*_{\pi(i)}, n^*_{\pi(i+1)})) < \Lambda$$

[0140] 문제 2는 고정된 저장량을(즉, Λ) 사용하여 인증 객체의 가능한 많은 (즉, l) 파이버 끝점들을 압축하는 최적화 문제를 모델링한다. ATSP(ASYMMETRIC TRAVELING SALESMAN PROBLEM)가 Λ에 대한 이진탐색을 통해 $\mathbf{CPS}$, $\mathbf{ATSP} \leq^{p}_{m} \mathbf{CPS}$으로 축소될 수 있음이 보여질 수 있으므로, 이 문제는 NP-컴플리트이다. 이 섹션의 나머지 부분에서, 이 문제를 해결하기 위한 효과적인 구성 휴리스틱 A2가 제공된다. 휴리스틱에 대한 제1의 설계 요구사항은 각각의 인증서가 제조 라인에서 분리되어 싸인되어야 하므로 신속한 실행시간의 성능이다.

[0141] 첫번째로, N의 2개의 노드들 간의 거리 측정은 모든 노드들에 대해 삼각 부등식을 따르지 않는다. 직관적으로, 섹션 IV-A으로부터의 인코딩 과정은 특정 단위가 2개의 가장 근접한 조명된 포인트들 중의 하나인 확률에 비례하는 비트들의 수를 사용하여 $S-S_i$에 벡터들을 인코딩한다. 그러므로, 소스 코드로부터 더 먼 단위들은, 솔루션 루트(route)에서 이들 노드들로의 단축경로들을 매우 바람직하지 않게 만드는, 매우 발생할 확률이 낮은 매우 더 긴 코드워드들로 인코딩된다.

[0142] 공리 2. 거리 측정 ω는 보편적으로 삼각 부등식을 따르지 않는다:

[0143] $$\omega(e(u,v)) + \omega(e(v,w) \geq \omega(u,w)$$

[0144] 단순성을 위해, $(\forall u \subset S-S_i)\, t = \tau(u) = \text{const.}$을 가정하고, u, v, 및 w는 $S-S_i$에 동일 라인을 따라 위치된다. 유클리드 거리 $\|u-v\|$, $\|v-w\|$, 및 $\|u-w\|$는 각각 a, b, 및 $a+b$이다. 삼각 부등식은 $f(u,v,w) = \log_2[\gamma(w,u)] - \log_2[\gamma(v,u)] - \log_2[\gamma(w,v)] \geq 0$를 내포한다. 수학식 17과 수학식 18로부터, 다음이 계산될 수 있다:

수학식 21

[0145] $$f(a,b,t) = 2ab\pi \log_2(1-t) + \log_2 \frac{t}{1-t} - \\ -\log_2 \frac{(1-t)^2 + (a^2+b^2)\pi t(1-t) + a^4 b^4 \pi^2 t^2}{1+\left[(a+b)^2\pi - 1\right]t}$$

[0146] 그리고, $ab\pi t \gg 1$에 대해, 삼각 부등식은 성립하지 않음을, 즉, $f(a,b,t) < 0$, 보인다.

[0147] 삼각 부등식이 성립하는 ATSP에 대한 최상의 근사 알고리즘은 최적치보다 기껏해야 $\log(|N|)$ 배 저조한 솔루션들을 생성한다. 다른 경우에서, 필자들이 아는 한에서는, 삼각 부등식이 성립하지 않는 ATSP 변이본들에 대한 근사 알고리즘들은 개발되지 않았다. 일반 경우에, 거리 메트릭 함수(distance metric function) ω가 임의적 일 때, ATSP 문제는 NPO-컴플리트이다, 즉, $P = NP$가 아닌 한 좋은 근사 알고리즘이 없다. 다른 한편, 삼각 부등식의 스케일된 버젼 $\mu(\omega(e(u,v)) + \omega(e(v,w))) \geq \omega(u,w), \mu > 1$을 만족시키는 TSP의 변이본들에 대한 근사 알고리즘들은 최악의 경우의 결과에 최적 솔루션보다 $(3\mu+1)\mu/2$ 배 저조하게 해결될 수 있다. 거리 메트릭 ω는 이 제한사항을 따르지 않고, 그러므로, 문제 2에 대한 휴리스틱은 최악의 경우의 보장이 없이 개발된다. 추가로, 최악의 경우의 보장보다는, 평균적으로 가능한 좋은 휴리스틱의 성능을 목표로 한다. 만족하게 압축될 수 없는 인증 객체 인스턴스는 버려질 수 있다. 이 이벤트의 확률은 1억 분의 1보다 작아야 한다.

[0148] <알고리즘 A2>

표 3

CONSTRUCTIVE PHASE

Set of edges $E' = \{\text{argmin}_e(\omega(a,b),\omega(b,a)) \mid (\forall a,b) \subset N\}$.

Set of subpaths P is selected as a set of shortest K edges in E' s.t. $\sum_{i=1}^{K} \omega(e_i) \le \Lambda$ sorted by ω.

Denote the weight of the shortest edge in E as $\omega_{\min}$.

for each path $p_i \subset P, i = 1..K-1$

for each path $p_j \subset P, j = i+1..K$

if p_i and p_j have a common source-destination node

Concatenate p_i and p_j as $p_i = p_i \mid p_j$.

Remove p_j from P.

Denote source and destination nodes of a path $p_i \subset P$ as s_i and d_i respectively.

for each path $p_i \subset P, i = 1..K$

Find all shortest paths $q(i,j)$ from s_i to any $d_j, j \neq i$.

while $|P| <$ maxP

$(p_i, p_j) = \text{argmin}_{q(i,j)} \sum_{e \subset \{p_i \mid q(i,j) \mid p_j\}} \frac{\omega(e)}{\|p_i \mid q(i,j) \mid p_j\|}$.

Concatenate $p_i = p_i \mid q(i,j) \mid p_j$ and remove p_j from P.

Find exhaustively a concatenation $p_h = p_1 \mid ... \mid p_{\text{maxP}}$ s.t.

$M(p_h)\{\sum_{e \subset p_h} \omega(e) < \Lambda$ and $|p_h|$ is maximal$\}$.

reroute(p_h)

reroute(p_h)

$p_{\text{best}} = p_h$

[0149]

for each edge $e(s_i, d_i) \subset p_h, i = 1,...,|p_h| - 1$

for each node pair $(d_i, s_j) \subset p_h, j = i+2,...,|p_h| - 1$.

Find shortest path $q(i,j)$ via nodes in $N - p_h$.

if path $e_1,...,e_i \mid q(i,j) \mid e_j,...,e_{|p_h|}$ has a better metric $M(p_h)$ then p_{best}

then $p_{\text{best}} = p_h$.

GREEDY ITERATIVE IMPROVEMENT

repeat I times

Contract p_h so that $\sum_{e \subset p_h} \omega(e) \le \rho\Lambda$, where ρ is a contraction factor, randomly chosen from $\rho \in \{0.4, 0.8\}$.

Denote nodes n_0 and n_l as the first and last node in p_h.

while $\sum_{e \subset p_h} \omega(e) \le \Lambda$

Among edges that have n_0 or n_l as destination or source respectively, find edge e with minimal weight.

Concatenate e to p_h.

rereoute(p_h)

[0150]

[0151] 섹션 IV-A로부터 거리 메트릭 ω를 사용하는 배경의 논리적 근거는 좋은 솔루션은 2개의 가장 근접한 이웃 노드들을 통해 그것의 루트에서 각각의 노드를 트래버스하는 것을 성공한다는 가정에 기초된다. 그러므로, 문제 2의 범위에서, 사용된 메트릭은 발견된 최상의 솔루션이 이 특성을 만족시키기만 하면 최적이다. 최종 솔루션이 이 특성을 갖지 않으면, 1개의 벡터를 인코딩하는 최적화는 솔루션에서 에지들의 가중치들의 분포에 종속된다.

[0152] 개발된 휴리스틱 A2는 다음의 2개의 단계들을 갖는다: 구성적 및 반복적 개선 페이즈. 구성 페이즈는 초기 솔루션을 빌드하는 그리디 휴리스틱(greedy heuristic)을 따른다. 초기에, A2는 지배적인 에지들의 세트 $\dot{E}'$를 식별한다. 노드들 u와 v간의 각각의 에지들의 쌍 $e(u,v)$, $e(v,u)$에 대해, A2는 2개 중의 더 짧은 것만을 선택하고, $\dot{E}'$에 그것을 저장한다. 다음, 초기 서브경로들의 세트 P는 $\dot{E}'$의 에지들을 정렬하고, 에지들의 가중치들의 합이 Λ에 가능한 근사한 처음 K 최단 에지들을 선택하여 생성된다. 경로 p_i에서의 첫번째와 최종 노드는 각각 s_i와 d_i으로 표현된다. 다음 단계에서, A2는 P로부터의 서브경로들을 그들의 가중치들의 증가 순서에 따라 반복적으로 결합시킨다: 임의의 포인트에서, 공통 소스-목적지(source-destination) 노드 $d_i = s_j$를 갖는 최단 서브경로들의 쌍 p_i, p_j는 모든 가능한 연결들이 확립될 때까지 결합된다. $|P|=1$일 때의, 거의 불가능한 경우에 최적의 솔루션이 발견되고, 탐색이 중지된다. 그렇지 않으면, 모든 단일-에지 서브경로들은 P로부터 삭제된다. 그 다음, 딕스트라 알고리즘(Dijkstra's algorithm)을 사용하여, A2는 P의 각각의 서브경로 p_i의 각각의 목적지 테일(destination tail) d_i과 모든 다른 서브경로들의 소스 테일들(source tails), $s_j, i=1...|P|, i \neq j$, 간에 모든 최단 경로들을 발견한다. 최단 경로들은 P에 있지 않은 노드들을 통해 라우트(route)된다. 최단 경로는 s_i와 d_j 간에 $q(i,j)$로서 표현된다. 다른 그리디(greedy) 단계에서, A2는 모든 결합들 $p_i|q(i,j)|p_j$을 그들의 가중치/노드 카운트 비율에 따라 정렬시킨다. 이 메트릭의 증가 순서에 따라, A2는 나머지 경로들의 총 수가 $|P|=\max P$일 때까지(보통 $\max P = 9$) $N-P$에서 노드들을 통해 P에 서브경로들을 결합시키기를 계속한다. 나머지 경로들은 최적의 메트릭, 최대 카디낼러티(maximal cardinality)와 Λ보다 작은 가중치들의 합, 으로 경로 p_h를 발견하는 이그젝트 알고리즘(exact algorithm)을 사용하여 결합된다. 최종 단계에서, 라우팅 과정은 P에서 모든 노드들을 브라우징하고, 딕스트라 알고리즘을 사용하여 E에 남아있는 노드들을 통해 P의 다른 노드들로의 최단 경로들을 발견하려고 한다. 동일 과정은 또한 p_h에 존재하는 것보다 더 나은 엔딩 테일(ending tail)을 발견하려고 한다. 각각의 리라우트(reroute)에 대해, A2는 그 새로운 리라우트가 현재의 최상의 경로 p_h보다 더 나은 메트릭을 갖는지를 검사한다.

[0153] 도 11은 $\kappa = 88$ 노드들로 도시된 인증 객체 $(512, 0.4 \cdot 512, 256)$의 인스턴스의 예이다. A2는 짙은선으로 도시된 경로를 리턴한다. 경로는 그것의 가중치들의 합이 $\Lambda = 512$보다 작도록 된다. 경로를 도큐멘트하기 위해, 포인트당 12.11 비트가 사용된다.

[0154] 반복적 개선 페이즈(iterative improvement phase)에서, 다음 루프의 몇 라운드를 반복한다. 제1 단계에서, A2는 현재 발견된 최상의 경로 p_{best}를 p_h으로 축소시켜서, $|p_h|$이 최대이고, p_h에 따른 가중치들의 합이 $\rho\Lambda$의 부분보다 더 작도록 한다. 축소 파라미터(contraction parameter) ρ는 $\rho \in \{0.4, 0.8\}$ 내의 각각의 반복에서 랜덤하게 선택된다. 노드들 n_0, n_l은 p_h에서 처음과 최종 노드로서 표현된다. p_h의 가중치들의 합이 Λ보다 작을 동안, 각각 소스와 목적지로서 n_0와 n_l을 갖는 에지들 간에, 최소 가중치를 갖는 에지 e를 발견하고, 그것을 p_h에 결합시킨다. 새로운 후보 경로 p_h가 생성될 때, 그것의 메트릭이 현재까지 생성된 최상의 경로의 메트릭보다 나으면 최상의 솔루션으로서 채택된다. 반복적 개선 루프의 최종 단계에서, A2는 전술된 리라우팅 과정을 수행한다.

[0155] 1초 내에 특정 인증 객체(L,R,K) 클래스에 대한 A2의 실행시간에 적합하기 위해, 개선 루프는 $I=\{100,10000\}$ 배 반복된다. 일반적으로, 복수의 소스 최단 경로들이 딕스트라 알고리즘을 통해 계산되므로, A2의 최악의 경우의 복잡도는 $O(|N|^3 \log|N|)$ 이다. 모든 최단의 경로들의 쌍을 계산하기 위해 플로이드-와셸 알고리즘(Floyd-Warshall algorithm)을 사용하는 구현에서, A2의 복잡도는 $O(|N|^3)$ 으로 감소될 수 있다. 그래프는 원래 컴플리트하지만, 높은 가중치들을 갖는 에지들을 제거하여, 모든 최단 경로들의 쌍에 대한 존슨 알고리즘(Johnson's algorithm)이 $O(|N|^2 \log|N|+|N||E|)$ 을 생성하는 스파스 그래프(sparse graph)가 생성된다.

[0156] V. 실험 평가

[0157] 이 섹션에서의 논의는 어떻게 인증 객체(L,R,K) 파라미터들이 알고리즘 A.2의 성능에 영향을 주는지를 보인다. 도 11은 그 문제의 단일 인스턴스, 인증 객체 $(512,0.4\cdot512,256)$, 로의 솔루션을 도시한다. $L=512$ 스캐닝 셀들로의 스캐닝 그리드이다. 도면은 인증 객체의 좌측아래 사분면이 조명될 때의 경우를 도시한다. 대응하는 조명된 파이버 끝점들을 사용하여 빌드된 그래프 $G(N,E)$ 는 중간 짙은선들로 도시된다. 그래프의 $\kappa=88$ 노드들의 각각으로부터 시작하는 처음 10개의 최단 에지들만이 도시된다. 짙은선들을 사용하는 도면에 도시된 결과적 경로는 41 노드들로 구성된다. 경로의 에지들을 따라서의 가중치들의 합은 저장 한계, $\Lambda=512$ 비트, 보다 작다. 경로는 파이버 끝점(b/feb)당 12.11 비트를 사용하여 압축된다. 압축없는 데이타 저장은 $41\cdot18=738$ 비트를 필요로 하고, 이것은 0.61의 압축비로 귀결한다. 압축비는 압축 메시지의 크기 대 원본 메시지 크기의 비율로서 정의된다.

[0158] VI. COA 시스템을 위한 설계 목적

[0159] 인증서 설계의 목적은 한계점이 있는 제조 비용 ς_m 를 사용하여 위조 비용 ς_f 를 최대화하는 것이다. 몇 개의 파라미터들은 ς_m 에 영향을 미칠 것이다. 단순성을 위해, 3개의 파라미터들이 다음과 같이 논의된다:

[0160] 파이버의 총 길이 $RK\le\Phi$,

[0161] 스캐닝 오차 ζ, 및

[0162] 바코드 저장 Λ

[0163] 시스템 성능은 싸인된 파이버 끝점들의 충분한 서브세트의 정확한 위치화에 대해 위조자가 가능한 시도 수를 제한하고(섹션 VI-A), 기대되는 위조 비용 $\varsigma_f(A2)$ 가 최대화되도록 시스템 파라미터들 $\{R,K\}$ 를 선택하여(섹션 VI-B) 최적화된다.

[0164] A. 위조 시도 수의 제한

[0165] Λ-한계의(Λ-limited) 저장에 κ 조명된 파이버 끝점들 중의 G 를 저장하는 압축 스킴 C 를 고려한다. 일반적으로, 인증서를 위조할 때, 위조자는 모든 κ 파이버를 사용하여 그들 중의 적어도 $G\zeta$ 를 정확히 그들의 대응하는 위치들에 배치하려고 할 수 있다. 인증서의 위조 비용은 크게 가능한 시도 수에 종속된다. 여기서, 확인시에 싸인된 파이버 끝점들 주위의 변칙적 파이버들의 분포를 검출하여, 위조자의 시도 수, K_T, 를 감소시키는 것을 목적으로 하는 기술이 제안된다.

[0166] <알고리즘 A3>

표 4

ISSUING A COA INSTANCE
Scan for a set N of κ points, illuminated when light is shed on S_i.
Using Λ bits, compress a subset $P \subset N$, with $G = \lvert P \rvert \leq \kappa$.
Find a subset of units $U \subset S - S_i$, such that
$(\forall u_i \in U)(\forall p_j \in P) \min(\lVert u_i - p_j \rVert) < \varepsilon_1$.
$\varepsilon_2 = \lvert N \cap U \rvert - G$, $K_T = G + \varepsilon_2$.
Sign P, ε_2 and the associated information (see Section 2).
VERIFYING A COA INSTANCE
Extract P, ε_2 from signature.
Find a subset of units $U \subset S - S_i$, such that
$(\forall u_i \in U)(\forall p_j \in P) \min(\lVert u_i - p_j \rVert) < \varepsilon_1$.
Scan for a set N' of κ' points, illuminated when light is shed on S_i.
if $\lvert N' \cap U \rvert > K_T$ **then** COA instance is invalid,
elseif $\lvert N' \cap P \rvert \geq G\zeta$ **then** COA instance is valid,
else COA instance is invalid.

[0167]

[0168] 인증서 발행자와 확인자는 각각의 인증 객체 사분면 S_i에 대해 알고리즘 A3의 그들의 부분들을 반복한다. 발행자는 초기에 인증 객체 인스터스를 스캔하고, S_i가 조명될 때 조명하는 포인트들의 세트 N에 대한 정보를 수집한다. 다음, 이용가능한 Λ 비트를 사용하여, 그것은 A2에 의해 리턴된 가장 큰 서브세트 $P \subset N$, $\lvert P \rvert = G$를 압축한다. 그 다음, 각각의 단위 $u_i \in U$와 그것의 가장 근접한 단위 $p_j \in P$ 간의 유클리드 거리가 기껏해야 ε_1이도록, A3는 서브세트 $U \subset S - S_i$을 발견한다. 단위들의 서브세트 U는 P의 ε_1-이웃을 나타낸다. 그 다음, 발행자는 U에 존재하는 N의 포인트들의 수 K_T를 카운트한다. K_T는 음의 오류들(false negatives)을 방지하기 위해 G보다 커야 하므로, 발행자는 P에 따라 발행자의 개인키를 사용하여 나중에 싸인되는 메시지 m에서의 차이 $\varepsilon_2 = K_T - G$를 저장한다(섹션 II를 참조). 발행자의 공개키를 사용하여, 확인자는 첨부된 서명으로부터 압축된 포인트 서브세트 P와 ε_2를 발췌하고, 대응하는 ε_1-이웃, 즉 U를 재생성한다. 그 다음, 확인자는 S_i이 조명될 때 조명된 파이버들의 세트 N'에 대한 인증 객체 인스턴스를 스캔한다. U과 N'의 공통 포인트들의 수가 기껏해야 $G + \varepsilon_2$이고, N'과 P의 공통 포인트들의 수가 적어도 $G\zeta$임을 검사하여 그 인스턴스의 진위성을 공고한다.

[0169] 서명에 ε_2를 저장하여, 위조자는 P의 ε_1-이웃에 파이버들을 위치시키려는 기껏해야 $K_T = G + \varepsilon_2$ 시도들을 사용하도록 부가된다. 위조자의 목적은 P로부터 적어도 $G\zeta$ 파이버 끝점들을 정확하게 위치시키는 것이므로, 위조자는 위조 과정 중에 P의 ε_1-이웃에 위치된 잘못 배치된 $G(1-\zeta) + \varepsilon_2$을 허용할 수 있다. 포인트 p_i을 타겟하는 각각의 시도는, 성공하면, p_i의 ε_1-이웃에 귀결함이 기대된다. ε_1를 증가시켜서, 확인자는 더 큰 이웃에 대해 잘못 배치될 수 있는 것들을 식별할 수 있다. 그러나, 이것은 또한 인증서 설계자가 될 수 있는 한 낮게 유지하기를 원하는 값 ε_2에 대한 기대치를 증가시킨다.

[0170] 아래, 주어진 $\varepsilon_1 = \text{const.}$를 채택하고, 그 다음 몇 개의 인증서 파라미터들의 관점에서 주 목적 $\varsigma_f(A2)$을 최대화하려는 실험적 설계 방법이 도시된다.

[0171] B. COA 시스템의 설계

[0172] 문제 3. COA 시스템을 위한 설계 목적

[0173] 주어진 압축 알고리즘 A2, 고정된 $RK \le \Phi$, ζ, ε_1, 및 Λ에서, 최대화시키는 이용가능한 파이버의 컷(cut) $\{R_*, K_*\}$을 발견한다:

수학식 22

[0174] $$\{R_*, K_*\} = \arg \max_{\{R,K|RK \le \Phi\}} \varsigma_f(A2, R, K)$$

[0175] 여기서, ς_f는 정리 2에서 정의된다. 수학식 2의 시도 수 K는 섹션 VI-A에 제공된 바와 같이 K_T와 같음을 주목한다. 수학식 2의 압축 성능 G는 A2의 효용성에 종속한다.

[0176] 도 12는 최적화된 비용 효용성에 대한 인증서의 그래프 표현이다. 가로축은 L에 관련된 파이버 길이 R를 정량화하고, 세로축은 파이버들의 수 K를 나타낸다. 바는 제한 한계 $\Lambda = 512$ 비트와 고정된 파라미터들의 세트, $\zeta = 0.9$, $\varepsilon_1 = 8$, 및 $\nu = 0.8$, 을 갖는 위조의 로그-비용(log-cost) $\log_{10}(\varsigma_f(A2, R, K))$를 도시한다. 도면은 또한 고정 길이 파이버의 모든 컷들, $RK = \Phi = 100L$, 에 대해 획득된 솔루션들의 품질을 도시한다.

[0177] 최상의 파이버 컷 $\{R_*, K_*\}$을 찾는 간단한 실험적 기술이 사용될 수 있다. 탐색 과정은 도 12를 사용하여 도시된다. 가로축과 세로축은 각각 R과 K의 값들을 나타낸다. 바는 인증서 인스턴스를 위조하는 기대되는 로그-비용, $\log_{10}(\varsigma_f(A2, RK))$, 을 나타낸다. 비용은 파라미터들의 고정 세트, $\Lambda = 512$, $\zeta = 0.9$, $\varepsilon_1 = 8$, 및 $\nu = 0.8$에 대해 그리고 R과 K에 대해 주어진다. 도 12의 다이어그램은 실험적으로 계산된다. A2는 $R = \{0.05L, 0.10L, ..., 0.45L\}$과 $K = \{80, 96, ..., 192, 256, 384, 512, 768, 1024\}$의 각각의 조합으로 랜덤하게 생성된 500 인증서(512,R,K) 인스턴스들에 적용된다. $\{R, K\}$-공간의 나머지 부분에서의 각각의 포인트에 대한 기대되는 압축 성능은 실험적 결과들을 보간하여 획득된다. 도 12에서, 최상의 파이버 컷은 $K_* \approx 900$과 $R_* \approx 0.1L$의 이웃에서 발견될 수 있다. 이 결과는, 선택된 설계 환경에 대해 크로스-형상의(cross-shaped) 인증서가 최상의 옵션이라는 사실을 가리킨다. 파이버 컷의 신중한 선택은 $RK = \Phi$에 랜덤하게 선택된 포인트에 대해 위조 비용 등급 개선의 결과를 가져옴을 주목한다. 이 예에서 사용된 실험적 원칙들은 상이한 인증서 환경들과 제조 제한점들에 대한 최적에 근사하는 파라미터 세트을 탐색하기 위해 적용될 수 있다.

[0178] 도 13은 설명된 시스템 및 방법이 전체적으로 또는 부분적으로 구현될 수 있는 컴퓨팅 시스템(1300)의 예를 도시한다. 컴퓨팅 시스템(1300)는 컴퓨팅 시스템의 일 예일 뿐이고, 본 발명의 사용이나 기능의 범위에 대해 임의의 제한점을 제안하려고 의도되지 않는다.

[0179] 컴퓨팅 시스템(1300)은 다수의 다른 일반 목적이나 특수 목적 컴퓨팅 시스템 환경들 또는 구성들로 구현될 수 있다. 사용하기에 적합할 수 있는 잘 공지된 컴퓨팅 시스템, 환경, 및/또는 구성들의 예들은 개인용 컴퓨터, 서버 컴퓨터, 씬 클라이언트(thin client), 씩 클라이언트(thick client), 핸드-헬드나 랩톱 디바이스, 멀티프로세서 시스템, 마이크로프로세서-기반 시스템, 셋톱 박스, 프로그램가능한 소비자 전자제품, 통신망 PC, 미니 컴퓨터, 메인프레임 컴퓨터, 게임 콘솔, 상술된 시스템이나 디바이스 중의 임의의 것을 포함하는 분산 컴퓨팅 환경 등을 포함하지만, 이에 제한되지 않는다.

[0180] 컴퓨팅 시스템(1300)의 콤포넌트들은 프로세서(1302)(예를 들어, 임의의 마이크로프로세서, 컨트롤러 등), 시스템 메모리(1304), 입력 디바이스(1306), 출력 디바이스(1308), 및 통신망 디바이스(1310)를 포함할 수 있지만, 이에 제한되지 않는다.

[0181] 컴퓨팅 시스템(1300)는 통상적으로 다양한 컴퓨터 판독가능 매체들을 포함한다. 그런 매체는 컴퓨팅 시스템(1300)에 의해 액세스가능하고 휘발성과 비휘발성 매체, 분리형과 비분리형 매체 모두를 포함하는 임의의 이용가능한 매체일 수 있다. 시스템 메모리(1304)는 랜덤 액세스 메모리(RAM)와 같은 휘발성 메모리 및/

또는 읽기용 메모리(ROM)와 같은 비휘발성 메모리의 형태로 컴퓨터 판독가능 매체를 포함한다. 스타트업 동안같은 때에 , 컴퓨팅 시스템(1300) 내의 소자들 간에 정보 전송을 돕기 위해 기본 루틴들을 포함하는 기본 입/출력 시스템(BIOS)은 시스템 메모리(1304)에 저장된다. 시스템 메모리(1304)는 통상적으로 즉시 액세스가능하고 그리고/또는 현재 프로세서(1302)에서 동작되는 데이타 및/또는 프로그램 모듈들을 포함한다.

[0182] 시스템 메모리(1304)는 또한 다른 분리형/비분리형, 휘발성/비휘발성 컴퓨터 저장 매체를 포함할 수 있다. 예로써, 하드 디스크 드라이브는 비분리형, 비휘발성 자기 매체로(부터) 읽고 쓰기 위해 포함될 수 있다. 자기 디스크 드라이브는 분리형, 비휘발성 자기 디스크(예를 들어, "플로피 디스크")로(부터) 읽고 쓰기 위해 포함될 수 있다. 광 디스크 드라이브는 CD-ROM, DVD, 또는 임의의 다른 유형의 광 매체와 같은 분리형, 비휘발성 광 디스크로(부터) 읽고 쓰기 위해 포함될 수 있다.

[0183] 디스크 드라이브들과 그들과 연계된 컴퓨터 판독가능 매체는 컴퓨터 판독가능 명령, 데이타 구조, 프로그램 모듈, 및 컴퓨팅 시스템(1300)에 대한 기타 데이타의 비휘발성 저장을 제공한다. 자기 카세트나 다른 자기 저장 디바이스, 플래쉬 메모리 카드, CD-ROM, 디지탈 다용도 디스크(DVD)나 다른 광 저장장치, 랜덤 액세스 메모리(RAM), 읽기용 메모리(ROM), 전기적으로 삭제가능한 프로그램가능한 읽기용 메모리(EEPROM) 등과 같은, 컴퓨팅 시스템(1300)에 의해 액세스가능한 데이타를 저장할 수 있는 다른 유형의 컴퓨터 판독가능 매체는 또한 컴퓨팅 시스템(1300)의 예를 구현하기 위해 사용될 수 있슴을 이해할 수 있다. 임의의 수의 프로그램 모듈들은, 예를 들어, 운영 체제(1320), 응용 프로그램(1328), 및 데이타(1332)를 포함하여 시스템 메모리(1304)에 저장될 수 있다.

[0184] 컴퓨팅 시스템(1300)는 통신 매체로서 식별된 다양한 컴퓨터 판독가능 매체를 포함할 수 있다. 통신 매체는 통상적으로 컴퓨터 판독가능 명령, 데이타 구조, 프로그램 모듈, 또는 반송파나 다른 전송 메카니즘과 같은 변조된 데이타 신호의 기타 데이타를 구현하고, 임의의 정보 전달 매체를 포함한다. "변조된 데이타 신호"라는 용어는 신호에서 정보를 인코딩하는 방식으로 한 개 이상의 그것의 특성들이 세트되거나 변경되는 신호를 일컫는다. 예를 들어, 통신 매체는 유선 통신망이나 직접 유선 연결과 같은 유선 매체 및 음향, RF, 적외선, 및 다른 무선 매체와 같은 무선 매체를 포함하지만, 이에 제한되지 않는다. 상술된 것들 중의 임의의 것의 조합들은 또한 컴퓨터 판독가능 매체의 범위 내에 포함될 수 있다.

[0185] 사용자는 키보드와 포인팅 디바이스(예를 들어, "마우스")와 같은 입력 디바이스(1306)를 통해 컴퓨팅 시스템(1300)로 커맨드와 정보를 입력할 수 있다. 다른 입력 디바이스들(1306)은 마이크로폰, 조이 스틱, 게임 패드, 컨트롤러, 위성 접시, 직렬 포트, 스캐너, 터치 스크린, 터치 패드, 키 패드 등을 포함할 수 있다. 출력 디바이스(1308)는 CRT 모니터, LCD 스크린, 스피커, 프린터 등을 포함할 수 있다.

[0186] 컴퓨티 디바이스(1300)는 구내 통신망(LAN), 광역 통신망(WAN) 등과 같은 컴퓨터 통신망에 연결하기 위한 통신망 디바이스(1310)를 포함할 수 있다.

[0187] 본 발명이 구조적 특징 및/또는 방법적 단계에 고유한 언어로 기재되었지만, 첨부된 청구범위에 정의된 본 발명은 기재된 특정 특징이나 단계에 제한될 필요는 없다. 대신, 특정 특징 및 단계는 청구된 본 발명을 구현하는 양호한 형태로서 개시된다.

발명의 효과

[0188] 개시된 시스템 및 방법은 랜덤하게 분포된 객체들의 특징들의 인코딩에 관한 것이다. 랜덤하게 분포된 인증 객체의 특징들이 결정되고, 그 특징들을 나타내는 데이타는 압축되고 서명으로 인코딩된다. 레이블은 생성되고, 인증 객체와 인코딩된 데이타를 포함한다. 데이타는 인증 객체와 연계된 확률 밀도 함수를 결정하기 위해 압축된다. 랜덤하게 분포된 속성들과 연계된 벡터들은, 적어도 부분적으로, 확률 밀도 함수에 기초하여 결정된다. 벡터들은 산술적 코딩 알고리즘을 사용하여 인코딩된다.

도면의 간단한 설명

[0001] 도 1은, 인증서와 같이, 레이블의 일부로서 사용하기 위한 인증 객체의 예를 도시한다.

[0002] 도 2는 인증서 시스템의 예와, 인증서를 발행하고 확인하기 위해 그 시스템에 의해 채택되는 과정들의 예를 도시하는 개략도이다.

[0003] 도 3a는 인증서와 연계된 랜덤하게 분포된 인증 객체의 특징들을 캡처링하는 스캐닝 시스템의 예의 개략도이

다.

[0004] 도 3b는 도 3a에 도시된 인증 객체의 윗면도이다.

[0005] 도 4는 인증서를 생성하기 위해 생성될 수 있는 프로세스의 예의 흐름도이다.

[0006] 도 5는 랜덤하게 분포된 인증 객체의 속성들을 나타내는 데이타를 압축하기 위해 사용될 수 있는 프로세스의 예의 흐름도이다.

[0007] 도 6은 인증 객체의 예에서 4개의 상이한 지역들에 대응하는 영역들의 그래프 표현이다.

[0008] 도 7은 인증 객체의 예에 19개의 상이한 지역들의 그래프 표현이다.

[0009] 도 8은 스퀴어 인증 객체에 대한 확률 밀도 함수의 예의 그래프이다.

[0010] 도 9는 인증 객체의 영역들의 그래프 표현이다.

[0011] 도 10은 어떻게 산술 코더(arithmetic coder)가 문자열 "aba"를 인코딩하는지의 예의 그래프 표현이다.

[0012] 도 11은 노드들로 도시된 인증 객체의 인스턴스의 예이다.

[0013] 도 12는 비용의 효용성을 최적화하기 위해 설계된 인증서의 그래프 표현이다.

[0014] 도 13은 기재된 시스템 및 방법이 전체적으로 또는 부분적으로 구현될 수 있는 컴퓨팅 디바이스의 예를 도시한다.

[0015] <주요 도면 부호 설명>

[0016] 230 발행자

[0017] 231, 251 데이타

[0018] 233 발행자의 개인키(private key)

[0019] 235 RSA 싸인(sign)

[0020] 237 해쉬(hash)

[0021] 215 텍스트

[0022] 250 확인자(verifier)

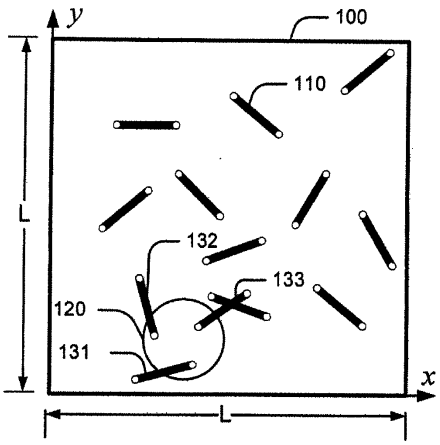
[0023] 253 발행자의 공개키(public key)

[0024] 255 RSA 확인(verify)

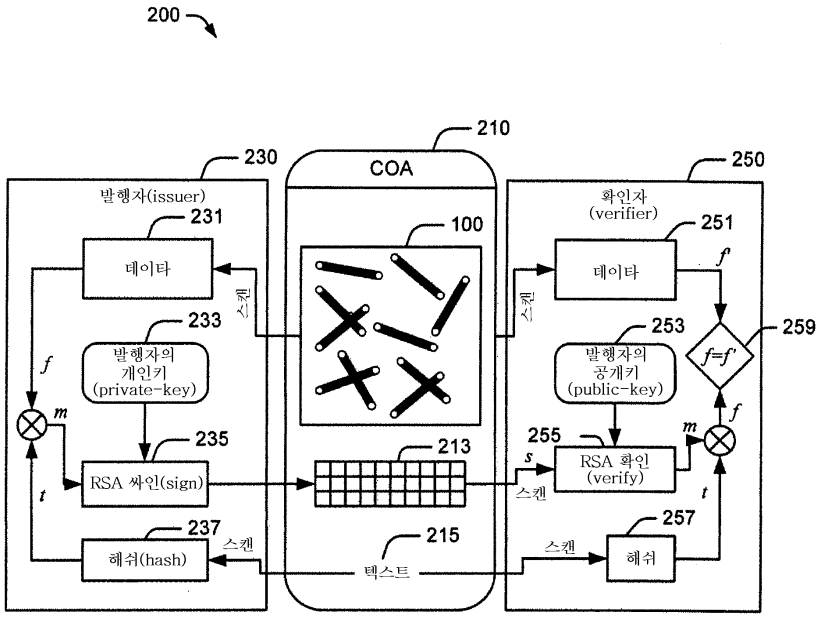
[0025] 257 해쉬

도면

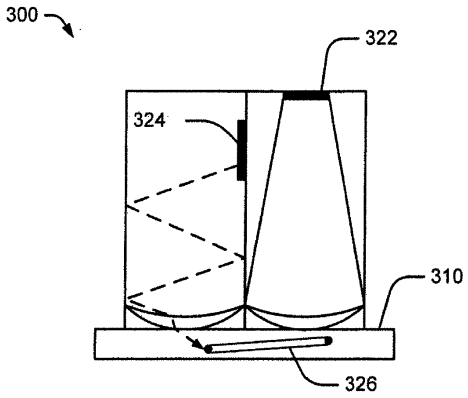
도면1


y
100
110
L
132
133
120
131
x
L

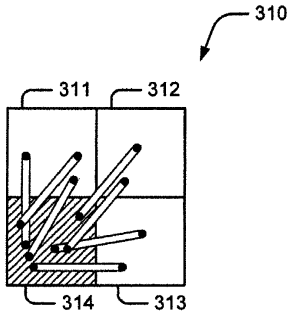
도면2


200
210
230
COA
250
발행자(issuer)
231
데이타
스캔
233
발행자의
개인키
(private-key)
f
m
235
RSA 싸인(sign)
t
237
해쉬(hash)
스캔
100
213
215
텍스트
확인자
(verifier)
251
데이타
f'
스캔
253
발행자의
공개키
(public-key)
259
f=f'
f
m
255
s
RSA 확인
(verify)
스캔
t
257
스캔
해쉬

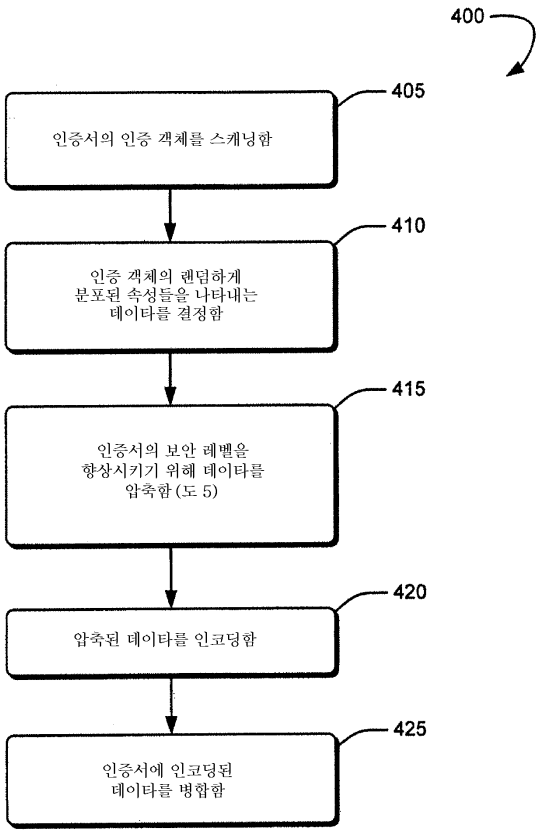
도면3a



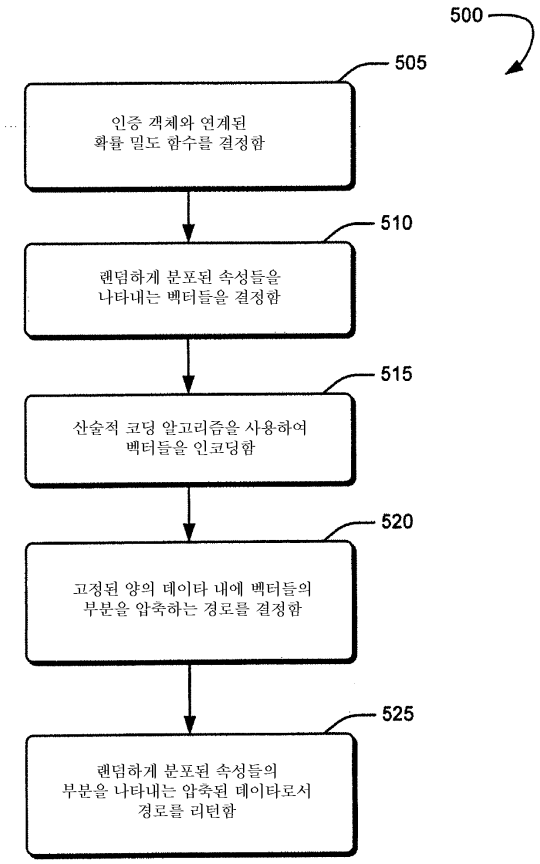
도면3b



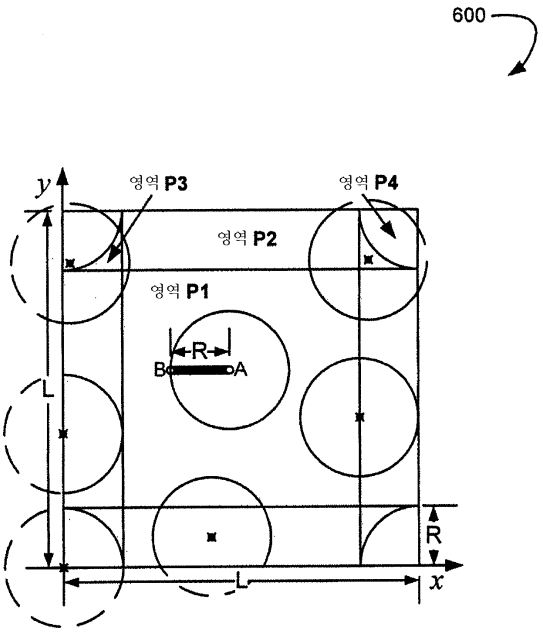
도면4


400
405
인증서의 인증 객체를 스캐닝함
410
인증 객체의 랜덤하게
분포된 속성들을 나타내는
데이타를 결정함
415
인증서의 보안 레벨을
향상시키기 위해 데이타를
압축함(도 5)
420
압축된 데이타를 인코딩함
425
인증서에 인코딩된
데이타를 병합함

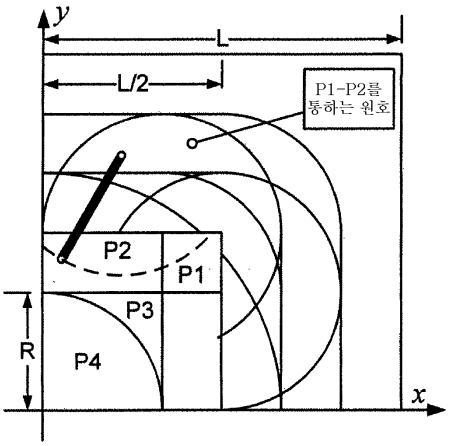
도면5


500
505
인증 객체와 연계된
확률 밀도 함수를 결정함
510
랜덤하게 분포된 속성들을
나타내는 벡터들을 결정함
515
산술적 코딩 알고리즘을 사용하여
벡터들을 인코딩함
520
고정된 양의 데이타 내에 벡터들의
부분을 압축하는 경로를 결정함
525
랜덤하게 분포된 속성들의
부분을 나타내는 압축된 데이타로서
경로를 리턴함

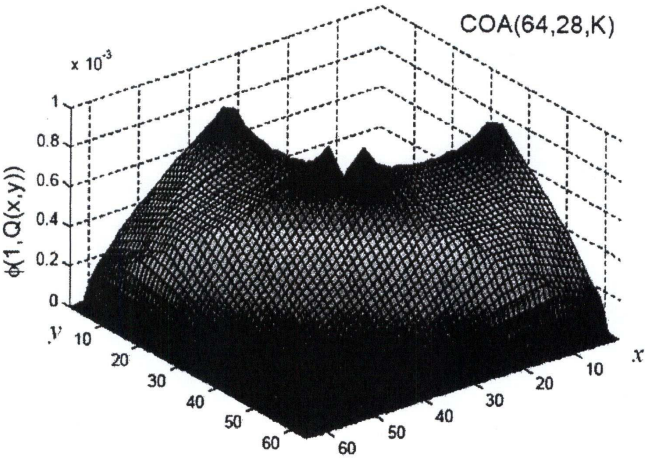
도면6


600
y
영역 P3
영역 P4
영역 P2
영역 P1
R
B
A
L
R
L
x

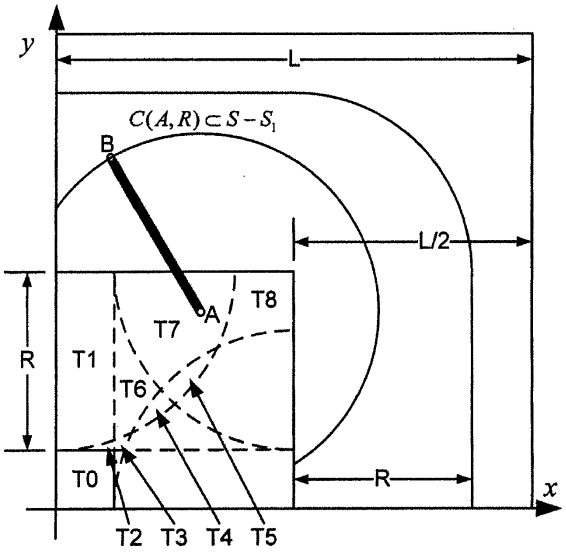
도면7


y
L
L/2
P1-P2를
통하는 원호
P2
P1
P3
P4
R
x

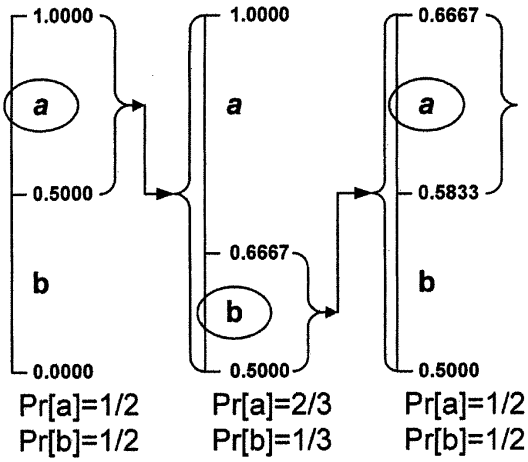
도면8


COA(64,28,K)
x 10^-3
1
0.8
0.6
0.4
0.2
0
ϕ(1,Q(x,y))
y
10
20
30
40
50
60
x
10
20
30
40
50
60

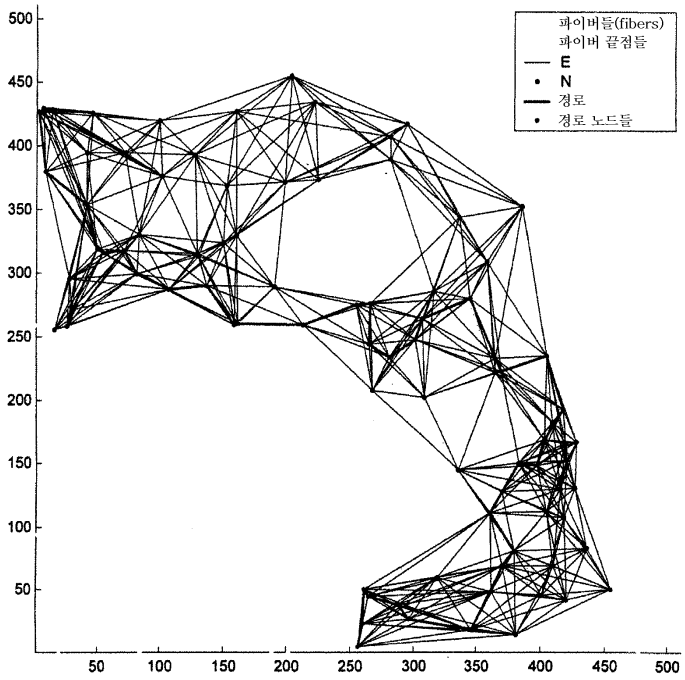
도면9


y
L
C(A,R)⊂S−S1
B
A
L/2
R
T1
T2
T3
T4
T5
T6
T7
T8
T0
R
x

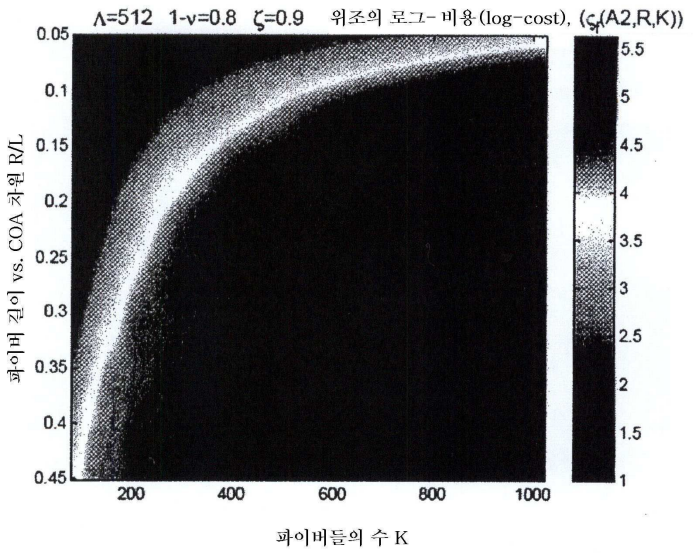
도면10


1.0000
a
0.5000
b
0.0000
Pr[a]=1/2
Pr[b]=1/2
1.0000
a
0.6667
b
0.5000
Pr[a]=2/3
Pr[b]=1/3
0.6667
a
0.5833
b
0.5000
Pr[a]=1/2
Pr[b]=1/2

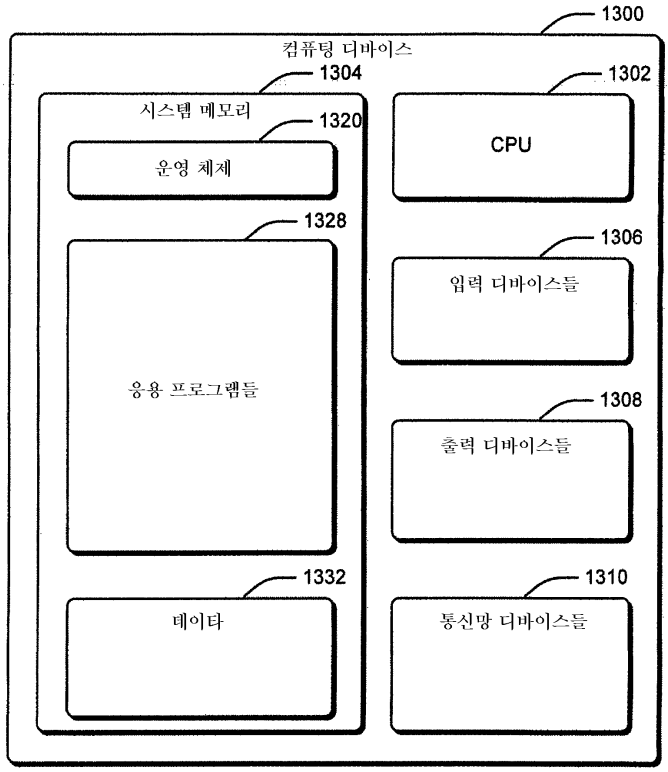
도면11


파이버들(fibers)
파이버 끝점들
E
N
경로
경로 노드들
500
450
400
350
300
250
200
150
100
50
50
100
150
200
250
300
350
400
450
500

도면12


Λ=512 1-ν=0.8 ζ=0.9 위조의 로그-비용(log-cost), (ζ(A2,R,K))
파이버 길이 vs. COA 차원 R/L
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
0.45
200
400
600
800
1000
파이버들의 수 K
5.5
5
4.5
4
3.5
3
2.5
2
1.5
1

도면13


1300
컴퓨팅 디바이스
1304
시스템 메모리
1320
운영 체제
1328
응용 프로그램들
1332
데이타
1302
CPU
1306
입력 디바이스들
1308
출력 디바이스들
1310
통신망 디바이스들