(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06F 15/00 (2006.01)
G06F 13/00 (2006.01)

(11) 공개번호 10-2006-0044980
(43) 공개일자 2006년05월16일

(21) 출원번호 10-2005-0026352
(22) 출원일자 2005년03월30일

(30) 우선권주장 10/837,563 2004년04월30일 미국(US)

(71) 출원인 마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이

(72) 발명자 말킨, 마이클 티.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
벤카테산, 라마라스남
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

(74) 대리인 주성민
백만기
이중희

심사청구 : 없음

(54) 랜덤화된 신호 변환 및 적용을 제공하는 방법

요약

랜덤화된 신호 변환 및/또는 그 적용을 제공하기 위한 기술들이 개시된다. 보다 상세하게, 랜덤하게 선택된 기저 함수들을 신호에 적용함으로써 신호(예를 들어, 오디오 신호, 이미지 또는 비디오 신호)가 변환된다. 랜덤화된 신호 변환의 적용은 압축, 노이즈 감소, 해싱, 식별, 인증 및 데이터 내장(예를 들어, 워터마킹)을 포함하지만, 이들로 제한되지는 않는다.

대표도

도 1

색인어

변환, 랜드레트 변환, 압축, 해싱, 랜덤화, 노이즈 감소

명세서

도면의 간단한 설명

도 1은 예시적인 랜드레트 변환(randlet transform)(RT) 시스템.

도 2는 예시적인 RT 방법.

도 3은 RT 기저 함수를 생성하기 위한 예시적인 방법.

도 4는 RT 기저 함수 라이브러리를 생성하기 위한 예시적인 방법.

도 5는 RT 변환을 적용하기 위한 예시적인 방법.

도 6은 RT 기반 압축을 위한 예시적인 방법.

도 7은 RT 기반 노이즈 감소를 위한 예시적인 방법.

도 8은 RT 기반 해싱을 위한 예시적인 함수.

도 9는 RT 기반 워터마킹을 위한 예시적인 방법.

도 10은 RT를 사용하여 변환된 신호의 재구성을 위한 예시적인 방법.

도 11은 본 발명에서 설명된 기술을 구현하기 위해 사용될 수 있는 일반적인 컴퓨터 환경(1100).

<도면의 주요부분에 대한 부호의 설명>

100: 랜드레트 변환 시스템

102: 랜드레트 변환(RT)

104: 입력

106: 기저 함수

108: 의사랜덤 발생기

110: 비밀 키

112: 적용

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 일반적으로 신호 변환에 관한 것으로, 보다 상세하게는, 랜덤화된 신호 변환 및/또는 그 적용에 관한 것이다.

발명이 이루고자 하는 기술적 과제

디지털 통신이 점점 일반화됨에 따라, 변환된 디지털 데이터의 보안 및/또는 인증의 필요성이 점점 더 중요해지고 있다. 디지털 데이터를 전하는 디지털 신호는 종종(항상은 아니지만) 전달되기에 앞서 특정한 포맷으로 변환된다(예를 들어 변환에 의해). 예를 들면, 디지털 데이터를 포함하는 파일은 인터넷을 거쳐 전송하기에 앞서 압축될 수 있다.

더욱 강력한 컴퓨터, 높은 속도의 인터넷 연결 및 우수한 압축 기술이 대부분의 사용자들에게 이용가능하기 때문에, 디지털 미디어 컨텐츠에 대한 요구는 여느 때보다 더 크다. 수백만 개의 좋아하는 음악 및 비디오에 언제든지 즉각적으로 액세스할 수 있으므로, 소비자들은 디지털 배포가 자신들에게 제공하는 편리성에 성원을 보내고 있다. 그들은 음악을 자신의 하드 드라이브나 개인용 컴퓨터 하드 드라이브에 임의의 텔레비전 방송만큼이나 유동적으로 다운로드하거나 스트리밍할 수 있다는 것을 즐긴다.

그러나, 디지털 컨텐츠에 대한 수요가 증가하는 한편, 그 무단 사용에 대한 잠재성 또한 증가한다. 적절한 보안 배포 시스템이 없으면, 디지털 미디어 파일들은 쉽게 복사되거나 혹은 컨텐츠 소유자의 허가없이 더 작은 파일들로 압축될 수 있다. 그리고, 이러한 파일들은 인터넷을 통해 전송되어 다른 사람들이 자유롭게 사용하거나 배포할 수 있게 된다. 이것은 수천 개의 미디어 회사, 레코드 레이블, 영화 제작사 및 레코딩 아티스트들이 가진 저작권을 침해하는 것이다. 그러한 무단 사용은 또한 이러한 엔터티들의 귀중한 수익을 빼앗는다.

현재의 한가지 접근법은 무단 사용을 제한하기 위하여 디지털 컨텐츠를 암호화하는 것이다. 그러나, 이 접근법은 신호 변환을 이용하는 시스템의 속도를 저하시킬 수 있는 부가적인 오버헤드를 가져온다.

따라서, 성능 저하를 제한하면서 부가적인 보안을 제공하는 신호 변환 솔루션이 요구된다.

발명의 구성 및 작용

랜덤화된 신호 변환 및/또는 그 적용을 제공하기 위한 기술들이 개시된다. 보다 상세하게, 랜덤하게 선택된 기저 함수(basis function)를 신호에 적용함으로써 신호(예를 들어, 오디오 혹은 비디오 신호)가 변환된다. 랜덤화된 신호 변환의 적용은 노이즈 감소(denoising), 해싱, 식별, 인증 및 데이터 내장(예를 들어, 워터마킹)을 포함하지만 그것으로 제한되지 않는다.

상세한 설명은 첨부 도면을 참조하여 기술된다. 도면에서, 참조번호의 제일 앞자리의 숫자는 해당 참조번호가 처음 나타나는 도면을 나타낸다. 상이한 도면에서 동일한 참조번호의 사용은 유사하거나 동일한 항목이라는 것을 나타낸다.

이하에서 일반적으로 신호 변환을 개선하기 위한 기술을 설명한다. 보다 상세하게, 본 발명에서 랜드레트 변환(randlet transform)(RT)으로 일컫는 신호 변환의 한 패밀리는 합리적인 성능을 유지하면서 보안을 제공하기 위하여 신호(예를 들어, 오디오 및/또는 비디오 신호)에 적용된다. 각 패밀리 구성원 변환은 비밀 키(K)에 기반하여 랜덤하게 혹은 의사랜덤하게(pseudorandomly) 선택된 기저 함수들의 집합(여기서는 "랜드레트"로 언급함)을 사용한다. 기술된 다양한 구현에서, RT의 적용은 데이터 내장(예를 들어, 워터마킹), 식별, 인증, 해싱, 노이즈 감소 및/또는 압축을 개선할 수 있다.

랜드레트 변환의 개요

도 1은 예시적인 랜드레트 변환(RT) 시스템(100)을 도시한다. RT 모듈(102)은 오디오 및/또는 비디오 신호와 같은 입력 데이터(104)를 수신한다. 신호는 컴퓨터 판독가능 매체, 컴퓨터 네트워크(예를 들어, 인트라넷, 인터넷, 무선 네트워크 등)에 연결된 소스 등에 의해 제공될 수 있다(도 11의 컴퓨팅 환경을 참조하여 더 논의될 것임).

RT 모듈(102)은 랜덤하게 선택된 기저 함수들의 집합(106)을 사용하여 입력 신호를 변환한다. 랜덤성(randomness)은 의사랜덤 발생기(108)에 의해 발생된 난수(혹은 복수의 난수)에 의해 제공된다. 한 구현에서, 의사랜덤 발생기(108)는 비밀 키(K)(110)에 의해 씨드(seed)된다. 비밀 키(K)는 비트 스트림으로서 제공될 수 있다. 한 실시예에서, 발생기(108)는 암호학적으로 강한 의사랜덤 발생기이다. RT 모듈(102)의 출력(예를 들어, 벡터)이 다수의 적용(112)을 위해 사용될 수 있고, 그것은 예를 들어 도 6 - 도 10을 참조하여 더 논의될 것이다.

도 2는 예시적인 RT 방법(200)을 도시한다. RT 기저 함수들이 생성(202)된 후(도 3과 4를 참조하여 더 논의될 것임), 생성된 다수의 기저 함수들이 도 1을 참조하여 논의된 것처럼 랜덤하게 선택된다(204). 한 구현에서, 비밀 키(K)(예를 들어, 의사랜덤 넘버 발생기에 대한 씨드로서 사용된)는 특정 인스턴스에 대하여 어떤 기저 함수가 선택되어야 하는지를 지정한다. 입력 신호(104)는 그 후 랜덤하게 선택된 기저 함수에 의해 변환된다(206). 한 구현에서, 입력 신호는 예를 들어 도 5를 참조하여 나중에 논의될 것처럼 블럭들로 나누어질 수 있다.

또한, RT는 이산 변환(discrete transform)으로서 적용될 수 있다. 제공된 랜덤성은 RT에게 두 가지 다른 이점을 줄 수 있다. 첫째, 공격자는 변환시 어떤 기저 함수가 사용되는지 알 수 없기 때문에 공격이 상대적으로 훨씬 더 어렵게 되어 보안

목적을 위해 유용하다. 둘째, 상대적으로 큰 집합의 기저 함수들로부터 랜덤하게 기저가 선택되기 때문에, 변환에 대한 최악의 경우의 성능(worst-case performence)이 비교적 낮은 확률로 발생한다. 그러므로, RT에 대한 척도는 최악의 경우의 성능보다는 평균 경우의 성능이다.

RT 기저 생성

기저 함수(여기서는 "랜드레트"로도 언급됨)들은 "마더 랜드레트(mother randlet)"로 불리는 일련의 2차원 함수에 기반을 둔다. 다양한 마더 랜드레트들이 아래 논의된다. 1차원, 2차원 또는 3차원(예를 들어, 각각 오디오 신호, 이미지 및 비디오 신호에 대응함)인 기저 함수들이 이용될 수 있다고 여겨진다.

도 3은 RT 기저 함수를 생성하기 위한 예시적인 방법(300)을 도시한다. 일반적으로, 랜드레트는 마더 랜드레트를 스케일링(302), 회전(304), 이동(306), 이산화(308) 및 정규화(310)함으로써 생성된다. 단계들(302, 304, 306 및/또는 308 - 310)의 다른 순서들 또한 가능하다. 또한, 회전은 대칭적인 가우시안 분포(Gaussian distribution)와 같은 특정 분포에 대해서는 행해지지 않을 수 있다(즉, 원의 회전은 행해지지 않음).

한 구현에서, 마더 랜드레트 $m(x,y)$가 주어졌을 때 수평이동 a, 수직이동 b, 수평 스케일링 α, 수직 스케일링 β 및 회전 θ를 행한 랜드레트는

$$x[i,j]=\left(\frac{i}{\alpha}\cos\theta-\frac{j}{\beta}\sin\theta\right)-a$$

$$y[i,j]=\left(\frac{i}{\alpha}\sin\theta-\frac{j}{\beta}\cos\theta\right)-b$$

$$r[i,j]=K\bullet m(x[i,j],y[i,j])$$

이다.

따라서, RT의 인스턴스에 사용되는 특정 랜드레트를 선택하기 위하여, 비밀 키(K)가 의사랜덤 넘버 발생기(예를 들어, 도 1의 108)에 씨드를 제공하기 위해 사용된다. 그리고, 랜덤 넘버가 요구될 때마다 이 의사랜덤 넘버 발생기로부터 취해진다.

기저 함수들의 라이브러리

도 4는 RT 기저 함수 라이브러리를 생성하기 위한 예시적인 방법(400)을 도시한다. 일반적으로, 모든 랜드레트들을 독립적이고 랜덤하게 선택함으로써 RT 기저를 정의하는 것이 가능하다. 그러나, 한 구현에서, 랜드레트의 선택을 약간 억제하더라도 동일한 성능이 달성될 수 있으므로, 실용적인 이유로 이것은 불필요하다. 그러므로, 랜드레트의 선택을 제한함으로써 계산 성능이 상당히 개선될 수 있다.

한 구현에서 기저 함수들은, 스케일링과 회전을 각 랜드레트마다 독립적으로 선택하는 대신, 한정된 집합의 스케일링과 회전 동작만을 허용함으로써 제한된다. 각 랜드레트를 다른 모든 랜드레트에 대해 독립적으로 정의하는 대신, 이동되지 않은(non-translated) 랜드레트들의 랜덤 라이브러리가 생성된다. 이러한 랜드레트들은 "스텝마더 랜드레트(step-mother randlet)"로 알려지고, 마더 랜드래트들을 랜덤하게 스케일링하고 회전함으로써(각각 402 및 404) 생성된다. 이러한 모든 스텝마더 랜드레트들의 집합이 "라이브러리"로 언급될 수 있다(406).

각 마더 랜드레트는 양방향으로 랜덤하게 스케일링된다. 스케일링에 대한 분포는 특정 마더 랜드레트와 그 적용 둘 모두에 의존한다. 이에 관한 예는, 이후의 섹션에서 주어진다. 스케일링된 각 마더 랜드레트에 대해, 생성된 회전의 수는 둘레길이(perimeter)에 비례할 수 있다.

스텝마더 랜드레트들이 이동(408), 이산화(410) 및 정규화(412)된다. 스텝마더 랜드레트는, 실수(real number)에 의해 스케일링되고 회전된 마더 랜드레트의 이산화된 버전이기 때문에, 정규화 상수는 랜드레트와 그 랜드레트 자신의 내적을 1과 동일하게 설정함으로써 결정된다. 그러므로,

$$\sum_{i=1}^{T}\sum_{j=1}^{U}(r_k[i,j])^2$$

$$K=\frac{1}{\sqrt{\sum_{i=1}^{T}\sum_{j=1}^{U}(m(x_k[i,j],y_k[i,j]))^2}}$$

이다.

*K*가 *a*와 *β*에 의존한다는 점을 유의해야 한다.

다음 몇 가지 중요한 값들은 RT 기저의 생성을 위한 파라미터들이다.

n : 기저 함수들의 총 수

<*T,U*> : 각각, 변환될 블럭의 폭과 높이

F(·) : 각 랜드레트의 유형을 결정하는 알고리즘

랜드레트들의 완전한 집합이 라이브러리로부터 스텝마더 랜드레트들을 랜덤하게 선택하고 이동(408)함으로써 생성된다. 이것은 n 개의 3-튜플 <*i,a,b*>의 리스트를 생성함으로써 행해지며, 각각의 3-튜플은 변환에 사용될 하나의 랜드레트를 나타낸다. 3-튜플에서, *i*는 라이브러리로의 인덱스이고, 따라서 랜드레트에 대한 스케일링과 회전을 암시적으로 결정한다. *i*는 함수 *F(·)*에 의해 랜덤하게 선택된다. 사용된 정확한 함수 *F*는 적용에 따라 달라진다. *a*와 *b*는 랜드레트의 중심점에 대한 실수화된 수평 및 수직 이동이며, 각각 *[0,T]* 및 *[0,U]*로부터 균일하고 랜덤하게 선택된다. 한 구현에서, 리스트가 생성되고 나면, 그 리스트는 랜드레트의 크기에 따라 소트된다. 예를 들어, 가장 큰 랜드레트들이 제일 처음에, 그리고 가장 작은 랜드레트들이 맨 마지막에 놓이게 된다.

마더 랜드레트

상기 논의된 것처럼, 마더 랜드레트들은 도 4를 참조하여 논의된 바와 같이 다른 모든 랜드레트들이 생성되게 하는 기본 랜드레트들이다. 마더 랜드레트들은 (0,0) 주변을 중심으로 하여 국부화된 효율적인 지원을 갖는 2차원의 실수화된 함수들이다. 일반적으로, 두 가지 형태의 마더 랜드레트들, 즉 저주파 랜드레트와 고주파 랜드레트가 있다. 두 가지 유형 모두 수평 방향으로 가우시안 형상을 갖는다. 수직 방향으로는, 저주파 랜드레트들은 가우시안 형상을 가지는 반면 고주파 랜드레트들은 진동하는 형상을 갖는다. 고주파 랜드레트만이 또한 가우시안 랜드레트로 알려진다. 그것은 이미지 또는 오디오 컨텐츠의 저주파 성분을 찾는 데에 유용하다. 그것은 각 방향이 다른 폭을 가질 수는 있지만, 수평과 수직 방향 모두에서 가우시안 형상을 갖는다.

가우시안 랜드레트(Gaussian Randlet) :

$$m(x,y)=C\bullet e^{\sigma_x x^2+\sigma_y y^2}$$

고주파 랜드레트들은 수평 방향으로는 가우시안 모양을 가지고 수직 방향으로는 다양한 진동하는 모양들을 갖는다. 랜드레트들은 회전될 것이기 때문에, 부드러운 방향(smooth direction)을 가우시안의 방향으로 언급하고, 거친 방향(rough direction)을 진동하는 함수의 방향으로 언급한다. 수직 방향에서의 변동(variation)은 이러한 랜드레트들에게 에지 감지 특성(edge-detection properties)을 부여한다. *θ*도만큼 회전될 때, 그들은 *θ*도에서 에지를 감지하는 경향이 있을 것이다. 다른 형태의 랜드레트들은 다음을 포함한다.

하프 랜드레트(Half Randlet) :

$$m(x,y)=C\bullet ye^{\sigma_x x^2+\sigma_y y^2}$$

멕시칸 해트 랜드레트(Mexican Hat Randlet) :

$$m(x,y) = C \bullet y^2 e^{\sigma_x x^2 + \sigma_y y^2}$$

웨이블릿 랜드레트(Wavelet Randlet) :

$$m(x,y) = C \bullet w(y) e^{\sigma_x x^2}$$

웨이블릿 랜드레트의 $w(y)$ 부분은 1차원 웨이블릿 함수이다. 한 구현에서, 웨이블릿 랜드레트를 스케일링할 때, 고정된 크기의 웨이블릿을 선택하는 대신 웨이블릿 패밀리가 선택될 수 있고, 스케일링하는 대신 웨이블릿 패밀리의 더 길거나 더 짧은 구성원이 선택될 수 있다.

일반적으로, 고주파 랜드레트들은 랜드레트들이 거친 방향에서보다 부드러운 방향에서 더 길도록 스케일링된다. 이것은 에지를 감지하는 랜드레트의 능력을 강화한다.

한 구현에서, 마더 랜드레트들은 가우시안, 하프, 멕시칸 해트 및/또는 웨이블릿 랜드레트들의 조합에 의해 얻어질 수 있다.

RT 변환

도 5는 RT 변환을 적용하는 예시적인 방법(500)을 도시한다. 각 랜드레트를 차례로 신호에 투영(projecting)함으로써 변환이 행해진다(502). 랜드레트들은 의사랜덤하게 선택될 수 있다(예를 들어, 도 1-2를 참조하여 논의된 것처럼). 각 투영이 행해진 후, 신호로부터 감산된다(504). 감산 후 신호에 남아있는 것이 "나머지(residue)"라고 불린다. RT 변환 방법(500)은 각 선택된 랜드레트를 이전 랜드레트의 나머지에 투영함으로써 계속된다(506). 이러한 방식으로, 변환이 본래의 신호로 수렴되고, 계수의 제곱이 지수적으로 감소하는 경향이 있다.

랜드레트 k와 랜드레트 $k-1$의 나머지의 내적을 구함으로써, 각 랜드레트에 대한 변환 계수 k가 계산된다(508). 만약 랜드레트 k가 r_k로 표시되고, 랜드레트 m의 나머지가 R_m으로, 그리고 계수 n이 c_n으로 표시된다면,

$$c_k = \sum_{i=1}^{T} \sum_{j=1}^{U} R_{k-1}[i,j] \bullet r_k[i,j]$$

이다.

각 계수가 생성되면 그것은 양자화되며(510), 양자화된 값이 변환에서의 계수로서 저장된다(512). 한 구현에 따라, 이 양자화된 값은 신호로부터도 감산된다(504). 한 구현에서, 랜드레트의 유형과 스케일링의 레벨 수에 기초하여 균일한 양자화기가 사용된다. 예를 들어, 랜덤 넘버에 기초하여 계수를 반올림(rounding)하기 위하여 랜덤화된 반올림 또한 사용될 수 있다. 랜덤화된 반올림의 영향은 알고리즘의 반복적인 수렴에 의해 수용될 수 있다.

양자화가 완료되면, 다음 나머지가 계산된다(514). 만약 $Q(\cdot)$가 양자화기라면,

$$R_k[i,j] = R_{k-1}[i,j] - Q(c_k) \bullet r_k[i,j]$$

이다.

한 구현에서, 랜드레트들이 전체 신호 블럭에 대해 투영되지는 않는다. 랜드레트들이 무시할 수 없는 값들을 가지는 영역만을 고려하여, 전처리 단계(도시되지 않음)에서 랜드레트의 유효 밑넓이(effective footprint)가 계산된다. 그 후 랜드레트들은 그 영역에서만 투영된다.

대안적인 구현에서, 기저 함수들이 표준(normal)으로서 위치되고, 그 후 그들의 위치는 최대 제곱의 근처 장소로 섭동(perturbation)된다. 이것은 변환이 더 적은 계수들을 가지고 수렴하도록 하지만, 추가 정보가 수평 및 수직 섭동(perturbation)을 주는 각 계수와 함께 저장되어야 할 것이다.

각 랜드레트의 중심이 전체 신호 블럭을 가로질러 균일하게 분포하기 때문에, 랜드레트들의 끝이 블럭의 외부에 도달할 수 있다. 이것은 블럭 경계에서 에지 효과(edge effect)를 초래한다. 이러한 에지 효과들은 각 에지에서 각 블럭을 자신의 거울 신호(mirror signal)로 패딩함으로써 제거될 수 있다. 일반적으로, 매우 큰 이미지에 대해서도 5 내지 10픽셀(예를 들어, 이미지에 대하여)의 패딩이면 충분하다.

RT 변환 확장

일반적으로, RT의 특정 인스턴스가 특정 크기의 신호 블럭(예를 들어, 이미지)에서 동작하기 위하여 생성된다. 이렇게 하기 위한 세 가지 방식이 있다. 첫째, 랜드레트들이 [0,1]의 범위에서 중심을 갖도록 선택될 수 있고, 선택된 신호 블럭의 실제 크기로 변환이 확장될 수 있다. 이 방법의 한가지 장점은 변환의 많은 계수들이 스케일링 불변이 될 것이라는 점이다. 그러나, 이러한 변환이 큰 데이터 블럭에 대해 잘 스케일링될 것이라는 것을 보장하기 위하여, 엄청난 수의 랜드레트들이 선택될 필요가 있을 수 있다. 이러한 랜드레트들은 작은 신호들에 대해서는 중복되지만, 변환이 큰 스케일로 행해지는 것을 가능하게 하기 위해서는 필수적일 것이다.

또다른 방법은 변환을 최대 신호 블럭 크기에 대하여 정의하는 것이다. 이 방법은 최대 블럭 크기가 알려지기 때문에 기저 함수들의 수가 제한될 수 있다는 점만 제외하면 이전 방법과 유사하다. 그러나 작은 블럭에 대한 중복되는 기저 함수들의 문제가 여전히 존재한다.

세 번째 방법은 비교적 작은 블럭 - 예를 들어, 50 * 50 혹은 100 * 100의 이미지 - 에 대하여 변환을 생성하는 것이다. 이 크기보다 더 큰 어떠한 블럭도 이 크기의 블럭들로 분해되고, 변환이 모든 블럭들에 대해 개별적으로 수행된다. 이 방법은 이전 두 방법들의 과다한 기저 함수들을 방지할 수 있기 때문에 변환에 대하여 이점이 있을 수 있다. 그러나, 첫 번째 방법은 적은 개수의 기저 함수들이 사용될 수 있는 해싱과 워터마킹 같은 RT의 적용에 대해 유용하다. 이들은, 아래의 해싱 및 워터마킹 섹션에서 더 논의된다.

또한, 대부분의 신호 블럭들이 블럭 크기의 정수 배로 오지 않을 것이므로 블럭들은 블럭 크기의 배수인 크기를 이루기 위하여 제로 값으로 패딩될 수 있다. 이러한 패딩은 아래 논의된 역변환이나 재구성의 일부로서 제거될 수 있다.

한 구현에서, 기저 함수들은 완전하고 독립적으로 랜덤일 필요는 없다. 예를 들어, 첫 번째 기저 함수는 완전하게 랜덤하게 선택될 수 있다. 각 후속하는 기저 함수에 대하여 일련의 선형 제약이 생성될 수 있고, 그것은 이전에 선택된 모든 기저 함수들로의 직교성 및/또는 정규화를 보장하는 제약을 포함한다. 그러한 제약들은 또한 기저 함수의 형상이 랜드레트임을 보장할 수 있다. 그 후 다음 기저 함수가 제약들을 충족시키는 함수들로부터 랜덤하게 선택될 수 있다. 그러나 추가의 기저 함수들이 선택됨에 따라, 함수들이 모든 제약들을 충족시키기는 더 힘들어질 수 있다. 이러한 상황에서, 다음 기저 함수는 바람직한 기저 함수의 크기와 함께 변할 수 있는 어떠한 임계값에 의해 정의되는 것과 같이, 제약들을 대략적으로 충족시키는(예를 들어, 거의 직교하는) 함수들 사이에서 랜덤하게 선택될 수 있다. 한 구현에서, 이러한 프로세스는 최적화 알고리즘에 의해 구현될 수 있다.

압축

도 6은 RT 기반 압축에 대한 예시적인 방법(600)을 도시한다. 양자화 후[예를 들어, 도 5의 단계(510)] 많은 변환 계수들이 제로일 수 있다. 계수들의 이러한 분포는 이러한 계수들이 제거(602)될 수 있기 때문에 압축에 매우 적합하다.

게다가, 가장 작은 랜드레트에 대응하는 계수들을 버림으로써, 손실 압축(lossy compression)이 임의의 레벨로 수행될 수 있다(602). 도 4를 참조하여 논의된 랜드레트들의 소트된 리스트에 대해서, 리스트의 끝 부분에 있는 랜드레트들은 무시하고 리스트의 시작부 가까이에 있는 랜드레트들만을 사용하여 손실 압축이 달성될 수 있다. 기타 손실 압축 기술들은 다음과 같이 이용될 수 있다. (1) 계수들이 더 거칠게 압축될 수 있고/거나 (2) 예를 들어, 크기(예를 들어, 절대값)가 특정 임계값보다 낮은 계수들을 버리는 것과 같이, 임계값들이 계수들의 값에 적용될 수 있다.

게다가, 손실 압축의 비율이 또한 동적으로 변화될 수 있고, 따라서 신호 블럭에 소모되는 대역폭의 양은 이용가능한 대역폭에 따르게 된다. 또한, 기본적인 표현이 먼저 나타나고 상세 사항이 나중에 채워지도록 이미지가 반복적으로 전송될 수 있다. 더욱이, 기저 함수들의 리스트가 크기에 의해 소트되면(도 4를 참조하여 논의된 것처럼) 이것은 자동으로 발생한다.

노이즈 감소(denoising)

도 7은 RT 기반 노이즈 감소에 대한 예시적인 방법(700)을 도시한다. 먼저, 작은 기저 함수들이 덜 강조된다(de-emphasized)(702). 그러면, 남아있는 기저 함수들의 중첩(super-position)은 많은 노이즈를 상쇄한다(704).

해싱

RT는 이미지 해싱과 같은 멀티미디어 신호 해싱에 대해 이상적인 툴이다. 이 섹션은 부분적으로 특정하게 이미지 해싱을 논의하지만 RT 기반 해싱은 일반적으로 도 8을 참조하여 논의될 것처럼 신호들에 적용될 수 있다고 여겨진다.

이미지 해싱에 대하여, 생성된 해시 값은 이미지에서의 섭동들에 강하다고 여겨지며, 기저 함수들의 랜덤화된 본질은 해시가 예측하기 어렵다는 것을 확실히 한다. 완전한 변환보다 해싱을 위한 요구사항이 더 적기 때문에, 도 5의 RT의 변경된 버전이 해싱을 위해 사용될 수 있다. 특히, 해시 값을 생성하기 위해 변환을 사용할 때 본래의 신호를 생성하기 위하여 해시 값을 역변환할 수 있어야 하는 것이 필수적인 것은 아니다. 그러므로 완전한 이미지 변환을 수행할 때보다 해싱할 때 훨씬 더 적은 계수들이 사용된다.

부가적으로, 해싱할 때, 예를 들어 모든 이미지에 대해 행해질 때, 각 계수가 다른 계수들 모두와 동일한 분포로부터 취해지도록 하는 것이 유용할 수 있다. 그러므로 RT가 해싱을 위해 사용될 때, 나머지는 사용되지 않는다. 이것은 해싱 알고리즘을 단순화하고 해시 계수들의 제곱이 이전 랜드레트들에 의해 감소되지 않는다는 것을 보장한다. 또한, 나머지들이 취해질 때, 나중의 계수들은 이전의 계수들에 의존하고, 따라서 신호에서의 작은 섭동이 나중의 계수들에서 큰 변화를 초래할 수 있다. 이것은 근사적인 해시에 대해 바람직하지 않은 성질이다.

한 구현에서, 해시된 벡터가 적합한 격자(lattice)를 사용하여 양자화될 수 있다. 예를 들어, 그에 대한 개인 키가 쉽게 양자화를 허용하는 공개 키 격자를 가질 수 있으나, 공개 키로부터의 양자화는 더 많은 에러를 도입한다. 따라서, 공개 키 기저는 적합한 단일모듈의 행렬 변환 하의 격자에 대한 개인 키 기저의 이미지일 것이다. 게다가, 양자화는 또한 작은 변화를 무시할 수 있게 한다.

또한, 해시를 위한 변환을 선택할 때 랜드레트들은 크기에 의해 소트될 필요가 없다(도 4를 참조하여 논의된 것과 같이). 도 8에 도시된 것처럼, RT 기반 해싱은 먼저 신호를 설정된 크기 - 예를 들어 256 * 256 - 로 스케일링(802)하고, 그 후 선택된 랜드레트들 각각을 나머지를 사용하지 않고서 신호에 직접 투영함(804)으로써 행해진다. 변환 계수들이 계산된다(806)(도 5를 참조하여 논의된 바와 같이). 생성된 계수들이 그 후 (엄격하게) 양자화된다(808).

마지막으로, 양자화된 변환 계수들에 에러 정정이 적용되고(810), 계수들이 저장된다(812). 한 구현에서, 해시 값을 축소하고 섭동에 훨씬 더 저항력 있게 하기 위하여, 에러 정정 코드의 디코더가 사용된다.

식별/인증을 위한 해싱

이미지들(및 일반적으로 신호들)은, RT 기반 해싱을 수행(도 8을 참조하여 논의된 바와 같이)하고 다양한 해시 값들을 비교함으로써 비교될 수 있다. 그러나, 이미지 식별이나 인증에 대해 에러 정정 디코딩이 필수적인 것은 아니다(810). 결과적으로, 각 신호 혹은 이미지는 양자화된 변환 계수들의 벡터와 결합된다. 디스턴스 메트릭(distance metric)에 기반하여 계수들의 벡터를 비교함으로써, 신호들은 신속하게 비교될 수 있다.

한 구현에서, 놈(norm) L_2가 이용된다. n이 큰 경우, 놈 L_n은 더 나은 결과를 낳을 수 있다(계수들 사이의 작은 차이는 경시하는 반면, 계수들 사이의 큰 차이점은 확대하기 때문임).

계수들이 직접적으로 또는 비율로서 비교될 수 있다. 예를 들어, 하나의 이미지에서 통계의 비율을 다른 이미지에서 동일한 통계의 비율과 비교하는 것은, 동일화 공격(equalization attack)을 물리치는 데에 도움을 줄 수 있다. 이것은 변환 계수들을 정규화하는 것과 유사하다. 대안적으로, 통계는 계수들의 부분집합의 함수로 형성될 수 있다. 마찬가지로, 이들은 직접적으로, 또는 비율로서 비교될 수 있다.

RT 워터마킹

도 9는 RT 기반 워터마킹을 위한 예시적인 방법(900)을 도시한다. 방법(900)은 데이터 내장을 위해 더 일반적으로 이용될 수 있다고 여겨진다. 워터마킹(더 일반적으로는 데이터 내장)에 있어서는, RT 기반 해싱(도 8의 논의 참조)에서와 동일하게, RT는 비교적 적은 수의 소트되지 않은 랜드레트에 대해 정의되고, 나머지들은 취해지지 않는다. 먼저, 신호 크기가 스케일링된다(902). 이미지 신호에 대하여, 변환은 표준 크기(canonical size) *[0,1]* * *[0,1]* 의 이미지에 대해 정의되고, 주어진 이미지의 크기로 스케일링된다. 변환은 랜드레트들을 직접 신호로 투영(904)하고 도 5 및 도 8을 참조하여 논의된 것처럼 변환 계수들을 계산함(906)에 의해 수행된다.

그 후 워터마크가 변환 계수들에 적용되고(908), 그것은 예를 들어 변환을 역변환하기 위한 최소-놈 행렬 솔루션을 통해 다시 신호로 삽입된다(910). 행렬이 올바르게 작용할 것을 보장하기 위하여 랜드레트들이 실질적으로 오버랩되지 않도록 선택될 수 있다. 그러나, 이것은 워터마크를 식별하여 무효화하는것을 더 쉽게 할 수 있다.

역변환 혹은 재구성

도 10은 RT를 사용하여 변환된 신호의 재구성을 위한 예시적인 방법(1000)을 도시한다. 변환을 행할 때 나머지들이 사용되기 때문에(도 5를 참조하여 논의된 것처럼) 각 랜드레트의 투영은 이전 랜드레트들에 직교한다. 이것은 단순히 각 랜드레트의 투영을 합함으로써 본래의 이미지가 재구성될 수 있다는 것을 의미한다. 즉, 각 랜드레트를 대응하는 변환 계수와 곱하고(1002) 그것들을 합산하여(1004), 입력 신호를 제공한다(1006).

예를 들어, 만약 *I[i,j]*가 이미지라면,

$$I[i,j] = \sum_{k=1}^{n} c_k \cdot r_k[i,j]$$

이다.

한 구현에서, 재구성 방법(1000)은 거의 직교하는(almost-orthogonal) 기저 함수들에 적용될 수 있다. 따라서, 재구성 방법(1000)은 나머지들이 사용될 때, 기저 함수들이 직교할 때, 또는 기저 함수들이 거의 직교할 때 적용될 수 있다.

하드웨어 구현

도 11은 본 발명에서 설명된 기술을 구현하기 위해 사용될 수 있는 일반적인 컴퓨터 환경(1100)을 도시한다. 예를 들어, 컴퓨터 환경(1100)은 이전 도면들을 참조하여 논의된 태스크를 수행하는 것과 관련된 명령들을 실행하기 위하여 이용될 수 있다. 컴퓨터 환경(1100)은 컴퓨터 환경의 단지 하나의 예일 뿐이며 컴퓨터와 네트워크 아키텍처의 사용 혹은 기능성의 범위에 어떠한 제한을 가하고자 하는 것은 아니다. 컴퓨터 환경(1100)이 예시적인 컴퓨터 환경(1100)에 도시된 컴포넌트들 중 어느 하나 혹은 조합에 관계되어 어떠한 의존성이나 요구사항을 가지는 것으로 해석되어서는 안 된다.

컴퓨터 환경(1100)은 컴퓨터(1102)의 형태로 범용 컴퓨팅 장치를 포함한다. 컴퓨터(1102)의 컴포넌트들은 하나 이상의 프로세서나 프로세싱 유닛(1104)(선택적으로 암호화 프로세서나 보조 프로세서를 포함함), 시스템 메모리(1106) 및 프로세서(1104)를 포함한 다양한 시스템 컴포넌트들을 시스템 메모리(1106)로 연결하는 시스템 버스(1108)를 포함하지만 이들로 제한되지 않는다.

시스템 버스(1108)는 메모리 버스나 메모리 컨트롤러, 주변 버스(peripheral bus), 가속 그래픽 포트(accelerated graphics port), 다양한 버스 구조를 사용하는 프로세서 또는 로컬 버스를 포함하여, 하나 이상의 다양한 형태의 버스 구조를 나타낸다. 예를 들어, 그러한 구조들은 산업 표준 구조(Industry Standard Architecture: ISA) 버스, 마이크로 채널 구

조(Micro Channel Architecture:MCA) 버스, 강화된 ISA(Enhanced ISA:EISA) 버스, 비디오 전자 표준 협회(Video Electronics Standards Association:VESA) 로컬 버스, Mezzanine 버스로 잘 알려진 주변 컴포넌트 인터커넥트(Peripheral Component Interconnects:PCI) 버스를 포함할 수 있다.

컴퓨터(1102)는 다양한 컴퓨터 판독가능 매체를 포함할 수 있다. 그러한 매체는 컴퓨터(1102)에 의해 액세스 가능한 임의의 가용 매체일 수 있으며, 휘발성과 비휘발성, 분리가능과 분리불가능 매체 모두를 포함한다.

시스템 메모리(1106)는 랜덤 액세스 메모리(RAM)(1110)와 같은 휘발성 메모리의 형태 및/또는 판독전용 메모리(ROM)(1112)와 같은 비휘발성 메모리의 형태의 컴퓨터 판독가능 매체를 포함한다. 컴퓨터를 시작할 때 등에서, 컴퓨터(1102) 내의 구성요소들 간의 정보의 전달을 돕는 기본 루틴을 포함하는 기본 입력/출력 시스템(BIOS)(1114)은 ROM(1112)에 저장된다. RAM(1110)은 전형적으로 즉시 액세스 가능하고/가능하거나 현재 프로세싱 유닛(1104)에 의해 실행중인 데이터 및/또는 프로그램 모듈을 포함한다.

컴퓨터(1102)는 또한 기타 분리가능/분리불가능, 휘발성/비휘발성 컴퓨터 저장 매체를 포함할 수 있다. 예를 들어, 도 11은 분리 불가능한 비휘발성 자기 매체(도시되지 않음)에 대한 판독 및 기입을 위한 하드 디스크 드라이브(1116), 분리 가능한 비휘발성 자기 디스크(1120)(예를 들면, "플로피 디스크")에 대한 판독 및 기입을 위한 자기 디스크 드라이브(1118) 및 CD-ROM, DVD-ROM 또는 기타 광학 매체와 같은 분리가능한 비휘발성 광학 디스크(1124)에 대한 판독 및 기입을 위한 광학 디스크 드라이브(1122)를 도시한다. 하드 디스크 드라이브(1116), 자기 디스크 드라이브(1118) 및 광학 디스크 드라이브(1122)는 하나 이상의 데이터 매체 인터페이스(1126)에 의해 각각 시스템 버스(1108)로 연결된다. 대안으로, 하드 디스크 드라이브(1116), 자기 디스크 드라이브(1118) 및 광학 디스크 드라이브(1122)는 하나 이상의 인터페이스(도시되지 않음)에 의해 시스템 버스(1108)로 연결될 수 있다.

디스크 드라이브와 그 관련 컴퓨터 판독가능 매체는 컴퓨터(1102)에게 컴퓨터 판독가능 명령, 데이터 구조, 프로그램 모듈 및 기타 데이터의 비휘발성 저장소를 제공한다. 본 예는 하드 디스크(1116), 분리가능 자기 디스크(1120) 및 분리가능 광학 디스크(1124)를 도시하고 있지만, 컴퓨터에 의해 액세스 가능한 데이터를 저장할 수 있는 여러 형태의 컴퓨터 판독가능 매체들 또한 예시된 컴퓨팅 시스템과 환경을 구현하기 위해 사용될 수 있으며, 그러한 매체로는 자기 카세트 또는 다른 자기 저장 장치, 플래시 메모리 카드, CD-ROM, DVD(digital versatile disk) 또는 기타 광학 저장소, RAM, ROM, EEPROM 등이 있다.

예를 들어, 운영 시스템(1126), 하나 이상의 어플리케이션 프로그램(1128), 기타 프로그램 모듈(1130) 및 프로그램 데이터(1132)를 포함하는 임의의 개수의 프로그램 모듈들이, 하드 디스크(1116), 자기 디스크(1120), 광학 디스크(1124), ROM(1112) 및/또는 RAM(1110)에 저장될 수 있다. 그러한 운영 시스템(1126), 하나 이상의 어플리케이션 프로그램(1128), 기타 프로그램 모듈(1130) 및 프로그램 데이터(1132)(또는 이들의 임의의 조합) 각각은 분산 파일 시스템을 지원하는 상주 컴포넌트의 전부 또는 일부를 구현할 수 있다.

사용자는 키보드(1134)와 포인팅 장치(1136)(예를 들어, "마우스")와 같은 입력 장치를 통해 명령어와 정보를 컴퓨터(1102)로 입력할 수 있다. 기타 입력 장치(1138)(상세하게 도시되지 않음)들은 마이크, 조이스틱, 게임패드, 위성 디쉬, 직렬 포트, 스캐너 등을 포함할 수 있다. 이러한 기타 입력 장치들은 시스템 버스(1108)로 연결된 입력/출력 인터페이스(1140)를 통해 프로세싱 유닛(1104)으로 연결되지만, 병렬 포트, 게임 포트 또는 USB와 같은 기타 인터페이스 및 버스 구조에 의해 연결될 수도 있다.

모니터(1142) 또는 다른 형태의 디스플레이 장치 또한 비디오 어댑터(1144)와 같은 인터페이스를 통해 시스템 버스(1108)로 연결될 수 있다. 모니터(1142) 외에, 다른 출력 주변 장치들은 입력/출력 인터페이스(1140)를 통해 컴퓨터(1102)로 연결될 수 있는 스피커(도시되지 않음) 및 프린터(1146)와 같은 컴포넌트를 포함할 수 있다.

컴퓨터(1102)는 원격 컴퓨팅 장치(1148)와 같은 하나 이상의 원격 컴퓨터로의 논리적 연결을 사용하여 네트워크 환경에서 동작할 수 있다. 예를 들어, 원격 컴퓨팅 장치(1148)는 PC, 휴대용 컴퓨터, 서버, 라우터, 네트워크 컴퓨터, 피어 디바이스 또는 다른 공통 네트워크 노드, 게임 컨솔 등이 될 수 있다. 원격 컴퓨팅 장치(1148)는 컴퓨터(1102)와 관련되어 여기에 기술된 많은 또는 모든 요소들과 특징들을 포함할 수 있는 휴대용 컴퓨터로서 도시된다.

컴퓨터(1102)와 원격 컴퓨터(1148) 사이의 논리적 연결은 근거리 통신망(LAN)(1150)과 일반적인 광역 통신망(WAN)(1152)으로서 기술된다. 그러한 네트워킹 환경은 사무실, 기업규모 컴퓨터 네트워크, 인트라넷 및 인터넷에서 일반적인 것이다.

LAN 네트워킹 환경에서 구현될 때, 컴퓨터(1102)는 네트워크 인터페이스 또는 어댑터(1154)를 통해 근거리 통신망(1150)에 연결된다. 광역 통신망(WAN) 네트워킹 환경에서 구현될 때, 컴퓨터(1102)는 광역 통신망(1152)을 통한 통신을 설정하기 위하여 전형적으로 모뎀(1156)이나 다른 수단을 포함한다. 컴퓨터(1102)로 내장되거나 외장일 수 있는 모뎀(1156)은 입력/출력 인터페이스(1140)나 다른 적절한 메커니즘을 통해 시스템 버스(1108)로 연결될 수 있다. 도시된 네트워크 연결들은 예이며, 컴퓨터들(1102, 1148) 사이에 통신 링크(들)를 설정하는 다른 수단이 사용될 수 있다는 것을 알아야 한다.

컴퓨팅 환경(1100)과 함께 도시된 것과 같은 네트워크 환경에서, 컴퓨터(1102)와 관련되어 기술된 프로그램 모듈 또는 그 일부는 원격 메모리 저장 장치에 저장될 수 있다. 예를 들어, 원격 어플리케이션 프로그램(1158)은 원격 컴퓨터(1148)의 메모리 장치에 상주한다. 예시의 목적으로, 어플리케이션 프로그램 및 운영 시스템과 같은 기타 실행가능한 프로그램 컴포넌트들이 개별적인 블럭으로 도시되어 있지만, 그러한 프로그램 및 컴포넌트들은 컴퓨팅 장치(1102)의 상이한 저장 컴포넌트들에 여러 시기에 상주하며 컴퓨터의 데이터 프로세서(들)에 의해 실행된다는 점을 알아야 한다.

다양한 모듈과 기술들이 하나 이상의 컴퓨터나 다른 장치들에 의해 실행되는, 프로그램 모듈과 같은 컴퓨터 실행 가능한 명령어의 일반적인 문맥으로 여기에 기술될 수 있다. 일반적으로, 프로그램 모듈들은 특정 태스크를 수행하거나 특정 추상 데이터 타입을 구현하는 루틴, 프로그램, 객체, 컴포넌트, 데이터 구조 등을 포함한다. 전형적으로, 프로그램 모듈의 기능은 다양한 실시예에서 바라는 대로 결합되거나 분산될 수 있다.

이러한 모듈과 기술의 구현은 소정 형태의 컴퓨터 판독가능 매체에 저장되거나 그러한 매체들을 거쳐 전송될 수 있다. 컴퓨터 판독가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있다. 제한적이지 않은 예로서, 컴퓨터 판독가능 매체는 "컴퓨터 저장 매체"와 "통신 매체"를 포함할 수 있다.

"컴퓨터 저장 매체"는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 다른 데이터와 같은 정보의 저장을 위한 방법이나 기술로 구현되는 휘발성 및 비휘발성, 분리가능 및 분리불가능 매체를 포함한다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD 또는 기타 광학 저장소, 자기 카세트, 자기 테이프, 자기 디스크 저장소 또는 기타 자기 저장 장치, 또는 원하는 정보를 저장하기 위해 사용될 수 있고, 컴퓨터에 의해 액세스될 수 있는 기타 매체를 포함하지만, 이들로 제한되는 것은 아니다.

"통신 매체"는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호나 기타 전송 메커니즘 내의 다른 데이터를 포함한다. 통신 매체는 또한 정보 전달 매체를 포함한다. "변조된 데이터 신호"라는 용어는 신호 내에서 정보를 암호화하기 위한 방식으로 하나 이상의 특성이 설정 또는 변화된 신호를 의미한다. 제한하지 않는 예로서, 통신 매체는 유선 네트워크나 직접 유선연결된 연결과 같은 유선 매체 및 음향, RF, 적외선, 무선 피델러티(예를 들어, IEEE 802.11b 무선 네트워킹)(Wi-Fi), 셀룰러, 블루투스 가동형 등의 무선 매체 및 기타 무선 매체를 포함한다. 상술한 것들의 임의의 조합 또한 컴퓨터 판독가능 매체의 범위에 포함된다.

결론

본 발명이 구조적인 특성 및/또는 방법론적인 행위에 특유한 언어로 기술되고 있지만, 첨부된 특허청구범위에 정의된 발명이 기술된 특유의 특성이나 행위로 필수적으로 제한되는 것은 아니라는 것이 이해되어야 한다. 예를 들어, 본 발명에서 논의된 기술이 오디오 신호, 이미지 및/또는 비디오 신호(즉, 각각 1, 2, 또는 3 차원 신호)에 적용될 수 있다. 그러므로, 특정한 특성 및 행위들은 청구하고자 하는 본 발명을 구현하는 예시적인 형태로서 기술된다.

발명의 효과

본 발명에 따르면, 성능 저하를 제한하면서도 부가적인 보안을 제공할 수 있는 랜덤화된 신호 변환 및/또는 그 적용이 제공된다.

(57) 청구의 범위

청구항 1.

생성된 복수의 기저 함수(basis function)를 랜덤하게 선택하는 단계, 및

상기 랜덤하게 선택된 기저 함수들을 신호에 적용하는 단계

를 포함하는 방법.

청구항 2.

제1항에 있어서,

상기 기저 함수들은 1차원, 2차원 및 3차원 함수들을 포함하는 그룹의 하나 이상의 항목으로부터 선택되는 함수들의 집합으로부터 생성되는 방법.

청구항 3.

제1항에 있어서,

상기 기저 함수들 각각은 마더 랜드레트(mother randlet)를 스케일링, 회전, 이동, 이산화 및 정규화하는 것을 포함하는 그룹으로부터 선택된 동작에 의해 생성되는 방법.

청구항 4.

제3항에 있어서,

상기 기저 함수들은 스케일링과 회전 연산의 한정된 집합만을 허용함으로써 제한되는 방법.

청구항 5.

제3항에 있어서,

각 기저 함수를 다른 모든 기저 함수에 독립적으로 정의하는 대신에, 상기 마더 랜드레트들을 랜덤하게 스케일링하고 회전함으로써, 이동되지 않은 기저 함수들의 라이브러리(library of non-translated basis functions)가 생성되는 방법.

청구항 6.

제3항에 있어서,

스케일링 시, 웨이블릿 패밀리가 선택되는 방법.

청구항 7.

제3항에 있어서,

상기 마더 랜드레트는 가우시안, 하프(half), 멕시칸 해트(Mexican Hat), 웨이블릿(wavelet) 랜드레트 및 그들의 조합들을 포함하는 그룹으로부터 선택되는 방법.

청구항 8.

제1항에 있어서, 상기 적용하는 단계는

선택된 각 기저 함수를 상기 신호 상에 투영(projection)하는 단계,

상기 신호로부터 각 투영을 감산하는 단계,

선택된 각 기저 함수를 이전 기저 함수의 나머지(residue) 상에 투영하는 단계,

각 기저 함수에 대한 변환 계수를 계산하는 단계,

상기 변환 계수들을 양자화하는 단계,

상기 양자화된 변환 계수들을 저장하는 단계, 및

다음 나머지를 계산하는 단계

를 포함하는 방법.

청구항 9.

제1항에 있어서,

상기 방법은 상기 신호를 압축하기 위하여 사용되며, 상기 적용하는 단계는

선택된 각 기저 함수를 상기 신호 상에 투영하는 단계,

상기 신호로부터 각 투영을 감산하는 단계,

각 기저 함수에 대한 변환 계수를 계산하는 단계,

상기 변환 계수들을 양자화하는 단계,

선택한 양자화된 변환 계수들을 제거하는 단계, 및

상기 양자화된 변환 계수들을 저장하는 단계

를 포함하는 방법.

청구항 10.

제1항에 있어서,

상기 방법은 비교적 작은 기저 함수들을 덜 강조하고(de-emphasize), 남아있는 기저 함수들을 중첩(superposition)함으로써 상기 신호의 노이즈를 감소시키기 위하여 사용되는 방법.

청구항 11.

제1항에 있어서,

상기 방법은 상기 신호를 해싱하기 위하여 사용되며, 상기 적용하는 단계는

상기 신호를 스케일링하는 단계,

선택된 각 기저 함수를 상기 스케일링된 신호 상에 투영하는 단계,

각 기저 함수에 대한 변환 계수를 계산하는 단계,

상기 변환 계수들을 양자화하는 단계,

상기 양자화된 변환 계수들에 에러 정정을 적용하는 단계, 및

상기 양자화된 변환 계수들을 저장하는 단계

를 포함하는 방법.

청구항 12.

제11항에 있어서,

상기 해시된 신호의 값은 식별 또는 인증을 위하여 이용되는 방법.

청구항 13.

제1항에 있어서,

상기 방법은 상기 신호를 워터마킹하기 위하여 사용되며, 상기 적용하는 단계는

상기 신호를 스케일링하는 단계,

선택된 각 기저 함수를 상기 스케일링된 신호 상에 투영하는 단계,

각 기저 함수에 대한 변환 계수를 계산하는 단계,

상기 변환 계수들에 워터마크를 적용하는 단계, 및

상기 워터마크를 상기 신호에 삽입하는 단계

를 포함하는 방법.

청구항 14.

제1항에 있어서, 상기 적용하는 단계는 변환된 신호를 제공하며, 상기 변환된 신호는

각 기저 함수를 대응하는 변환 계수와 승산하는 단계, 및

상기 승산의 결과들을 합산하는 단계

를 포함하는 동작들에 의해 재구성되는 방법.

청구항 15.

신호를 수신하고, 랜덤하게 선택된 복수의 기저 함수를 상기 신호에 적용하기 위한 랜드레트 변환(RT) 모듈, 및

상기 랜덤하게 선택된 기저 함수들을 선택하기 위하여 상기 RT 모듈에 의해 이용되는 랜덤 넘버를 발생하기 위해 상기 RT 모듈에 연결된 의사랜덤 발생기

를 포함하는 시스템.

청구항 16.

제15항에 있어서, 상기 의사랜덤 발생기는 상기 랜덤 넘버를 발생하기 위한 씨드(seed)로서 비밀 키를 이용하는 시스템.

청구항 17.

제16항에 있어서, 상기 씨드는 비트 스트림인 시스템.

청구항 18.

제15항에 있어서, 상기 기저 함수들 각각은 마더 랜드레트를 스케일링, 회전, 이동, 이산화 및 정규화함으로써 생성되는 시스템.

청구항 19.

명령어들이 저장되어 있는 하나 이상의 컴퓨터 판독가능 매체로서, 상기 명령어들은 실행 시에 기계에게

생성된 복수의 기저 함수를 랜덤하게 선택하는 단계, 및

상기 랜덤하게 선택된 기저 함수들을 신호에 적용하는 단계

를 포함하는 동작들을 수행하도록 지시하는 하나 이상의 컴퓨터 판독가능 매체.

청구항 20.

제19항에 있어서,

상기 기저 함수들은 1차원, 2차원 및 3차원 함수들을 포함하는 그룹의 하나 이상의 항목으로부터 선택된 함수들의 집합으로부터 생성되는 하나 이상의 컴퓨터 판독가능 매체.

청구항 21.

제19항에 있어서,

상기 기저 함수들 각각은 마더 랜드레트를 스케일링, 회전, 이동, 이산화 및 정규화함으로써 생성되는 하나 이상의 컴퓨터 판독가능 매체.

청구항 22.

제21항에 있어서,

상기 기저 함수들은 스케일링과 회전 연산의 한정된 집합만을 허용함으로써 제한되는 하나 이상의 컴퓨터 판독가능 매체.

청구항 23.

제21항에 있어서,

각 기저 함수를 다른 모든 기저함수에 독립적으로 정의하는 대신, 상기 마더 랜드레트들을 랜덤하게 스케일링하고 회전함으로써, 이동되지 않은 기저 함수들의 라이브러리가 생성되는 하나 이상의 컴퓨터 판독가능 매체.

청구항 24.

제21항에 있어서,

스케일링 시, 웨이블릿 패밀리가 선택되는 하나 이상의 컴퓨터 판독가능 매체.

청구항 25.

제21항에 있어서,

상기 마더 랜드레트는 가우시안, 하프, 멕시칸 해트, 웨이블릿 랜드레트 및 그들의 조합들을 포함하는 그룹으로부터 선택되는 하나 이상의 컴퓨터 판독가능 매체.

청구항 26.

제19항에 있어서, 상기 적용하는 단계는

선택된 각 기저 함수를 상기 신호 상에 투영하는 단계,

상기 신호로부터 각 투영을 감산하는 단계,

선택된 각 기저 함수를 이전 기저 함수의 나머지 상에 투영하는 단계,

각 기저 함수에 대한 변환 계수를 계산하는 단계,

상기 변환 계수들을 양자화하는 단계,

상기 양자화된 변환 계수들을 저장하는 단계, 및

다음 나머지를 계산하는 단계

를 포함하는 하나 이상의 컴퓨터 판독가능 매체.

청구항 27.

제19항에 있어서,

상기 동작들은 상기 신호를 압축하기 위해 사용되며, 상기 적용하는 단계는

선택된 각 기저 함수를 상기 신호 상에 투영하는 단계,

상기 신호로부터 각 투영을 감산하는 단계,

각 기저 함수에 대한 변환 계수를 계산하는 단계,

상기 변환 계수들을 양자화하는 단계,

선택한 양자화된 변환 계수들을 제거하는 단계, 및

상기 양자화된 변환 계수들을 저장하는 단계

를 포함하는 하나 이상의 컴퓨터 판독가능 매체.

청구항 28.

제19항에 있어서,

상기 동작들은 비교적 작은 기저 함수들을 덜 강조하고, 남아있는 기저 함수들을 중첩함으로써 상기 신호의 노이즈를 감소시키기 위하여 사용되는 하나 이상의 컴퓨터 판독가능 매체.

청구항 29.

제19항에 있어서,

상기 동작들은 상기 신호를 해싱하기 위해 사용되며, 상기 적용하는 단계는

상기 신호를 스케일링하는 단계,

선택된 각 기저 함수를 상기 스케일링된 신호 상에 투영하는 단계,

각 기저 함수에 대한 변환 계수를 계산하는 단계,

상기 변환 계수들을 양자화하는 단계,

상기 양자화된 변환 계수들에 에러 정정을 적용하는 단계, 및

상기 양자화된 변환 계수들을 저장하는 단계

를 포함하는 하나 이상의 컴퓨터 판독가능 매체.

청구항 30.

제29항에 있어서,

상기 해시된 신호의 값은 식별 또는 인증을 위해 이용되는 하나 이상의 컴퓨터 판독가능 매체.

청구항 31.

제19항에 있어서, 상기 행위들은 상기 신호를 워터마킹하기 위해 사용되며, 상기 적용하는 단계는

상기 신호를 스케일링하는 단계,

선택된 각 기저 함수를 상기 스케일링된 신호 상에 투영하는 단계,

각 기저 함수에 대한 변환 계수를 계산하는 단계,

상기 변환 계수들에 워터마크를 적용하는 단계, 및

상기 워터마크를 상기 신호에 삽입하는 단계

를 포함하는 하나 이상의 컴퓨터 판독가능 매체.

청구항 32.

제19항에 있어서,

상기 적용하는 단계는 변환된 신호를 제공하며, 상기 변환된 신호는

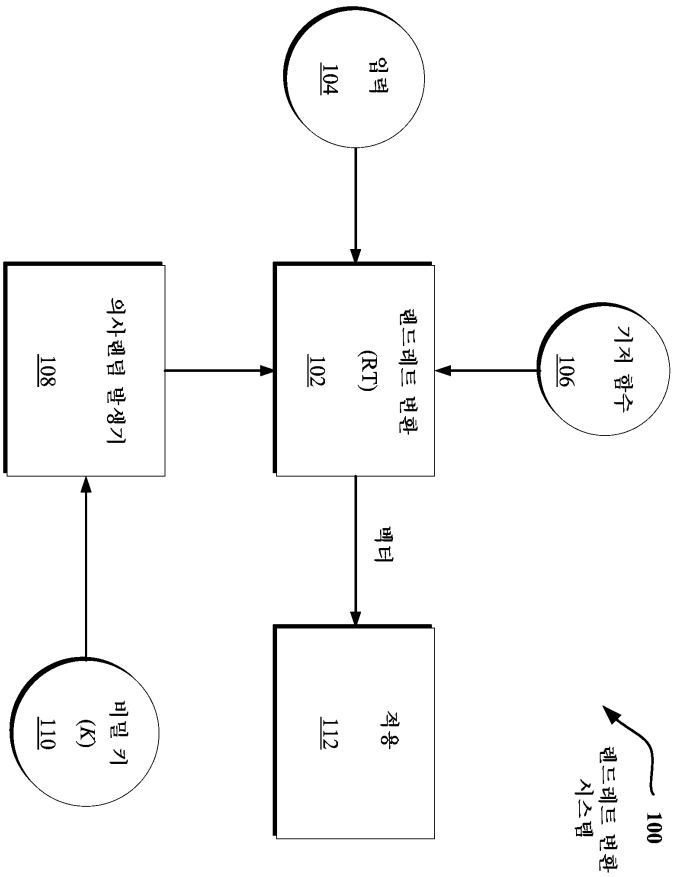
각 기저 함수를 대응하는 변환 계수와 승산하는 단계, 및

상기 승산의 결과들을 합산하는 단계

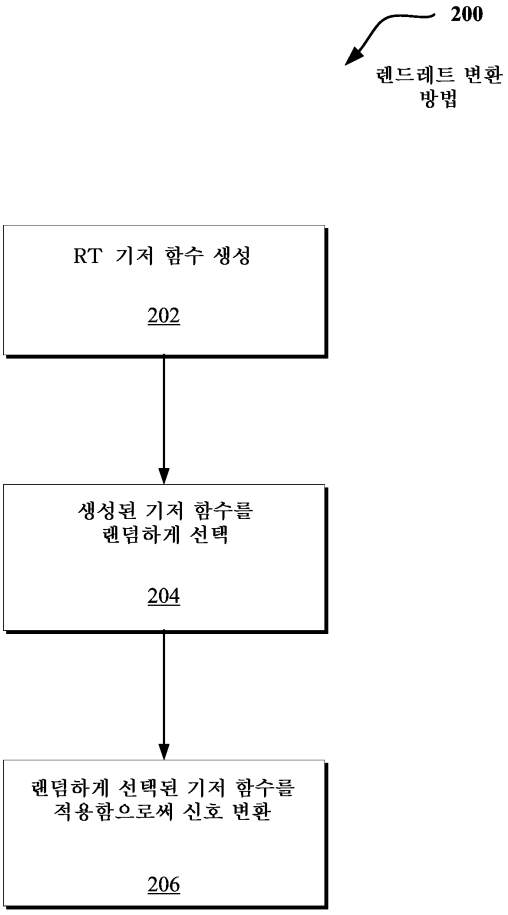
를 포함하는 동작들에 의해 재구성되는 하나 이상의 컴퓨터 판독가능 매체.

도면

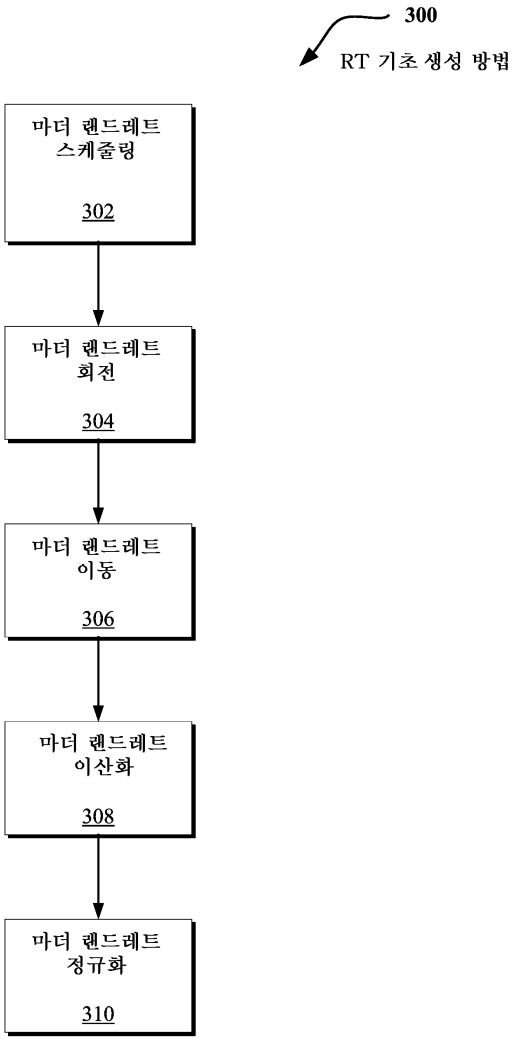
도면1


입력
104
렌드레트 변환
(RT)
102
기저 함수
106
의사랜덤 발생기
108
비밀 키
(K)
110
펑터
적용
112
100
렌드레트 변환
시스템

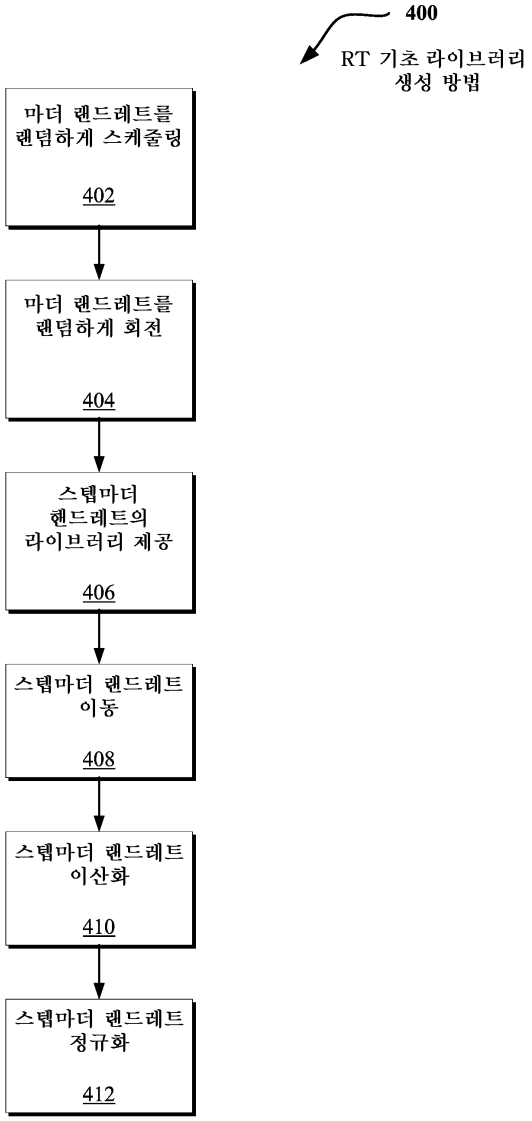
도면2


200
랜드레트 변환 방법
RT 기저 함수 생성
202
생성된 기저 함수를 랜덤하게 선택
204
랜덤하게 선택된 기저 함수를 적용함으로써 신호 변환
206

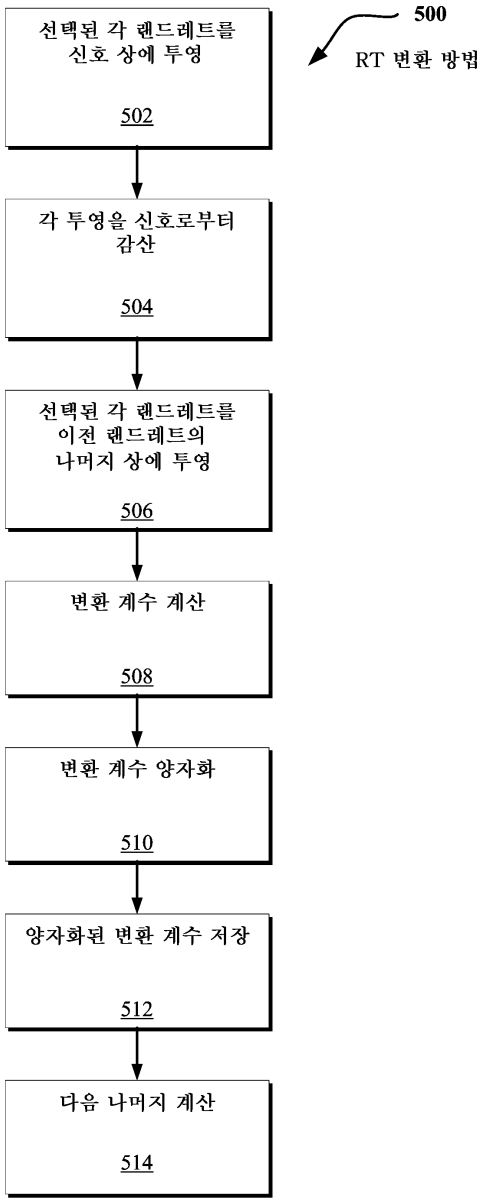
도면3


300
RT 기초 생성 방법
마더 랜드레트 스케줄링
302
마더 랜드레트 회전
304
마더 랜드레트 이동
306
마더 랜드레트 이산화
308
마더 랜드레트 정규화
310

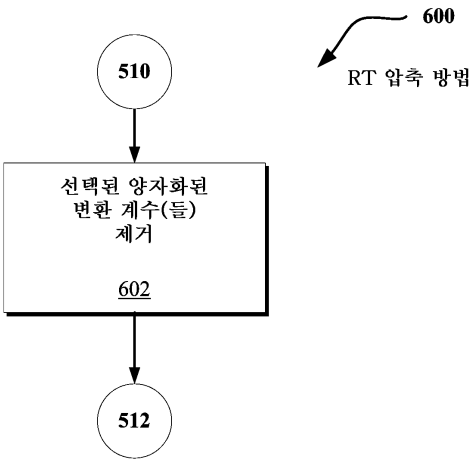
도면4


400
RT 기초 라이브러리 생성 방법
마더 랜드레트를 랜덤하게 스케줄링
402
마더 랜드레트를 랜덤하게 회전
404
스텝마더 핸드레트의 라이브러리 제공
406
스텝마더 랜드레트 이동
408
스텝마더 랜드레트 이산화
410
스텝마더 랜드레트 정규화
412

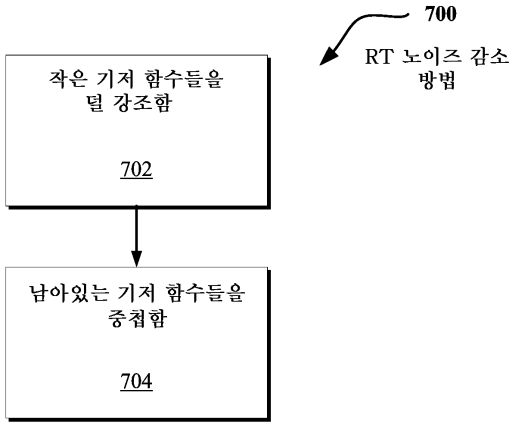
도면5


500
RT 변환 방법
선택된 각 랜드레트를 신호 상에 투영
502
각 투영을 신호로부터 감산
504
선택된 각 랜드레트를 이전 랜드레트의 나머지 상에 투영
506
변환 계수 계산
508
변환 계수 양자화
510
양자화된 변환 계수 저장
512
다음 나머지 계산
514

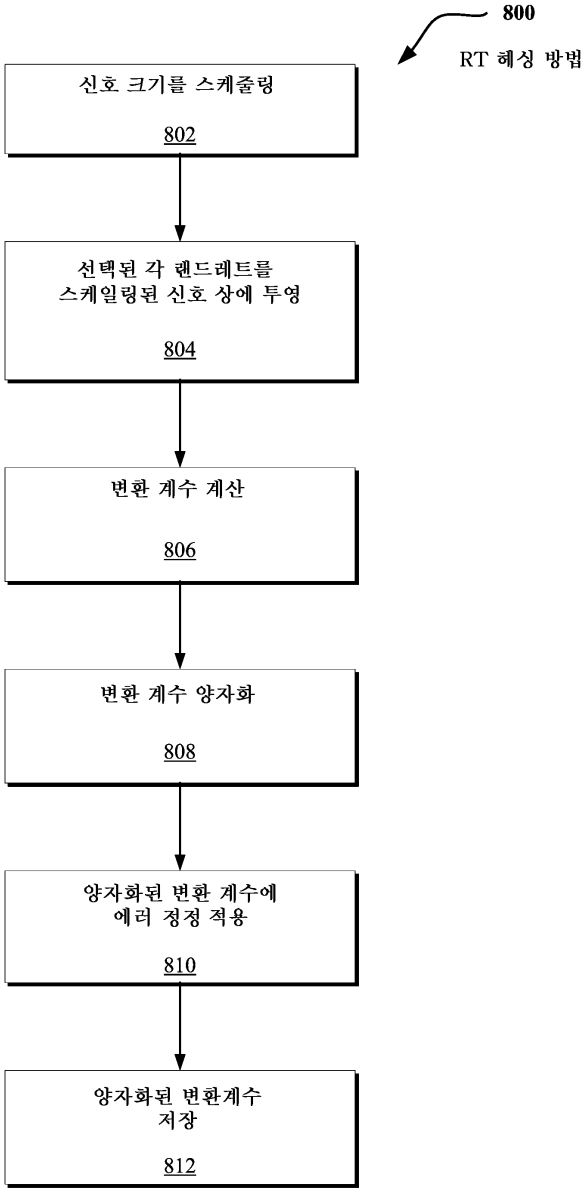
도면6


600
RT 압축 방법
510
선택된 양자화된 변환 계수(들) 제거
602
512

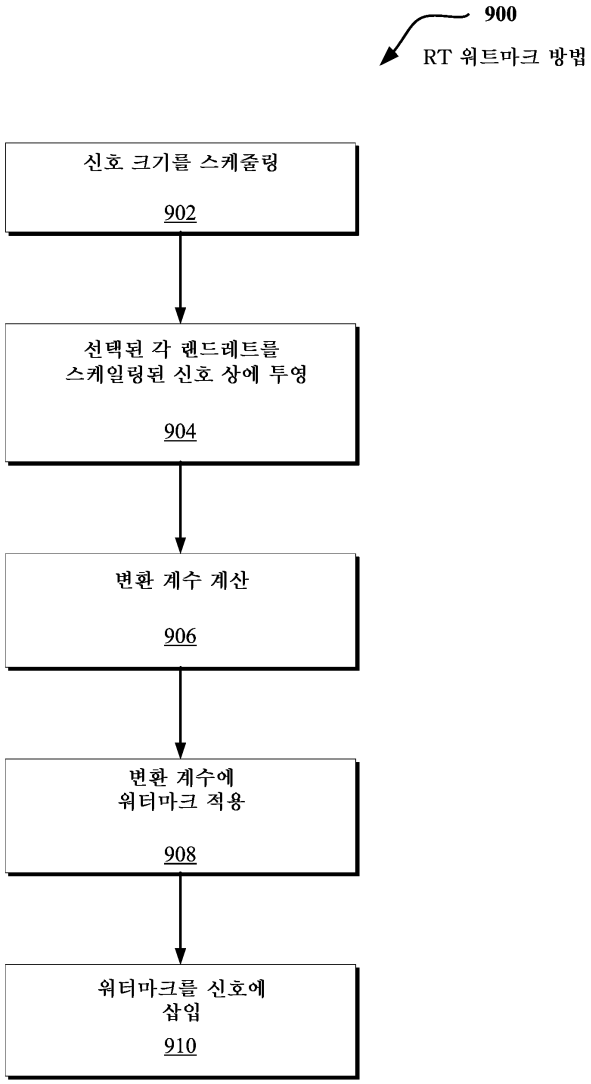
도면7


700
RT 노이즈 감소 방법
작은 기저 함수들을 덜 강조함
702
남아있는 기저 함수들을 중첩함
704

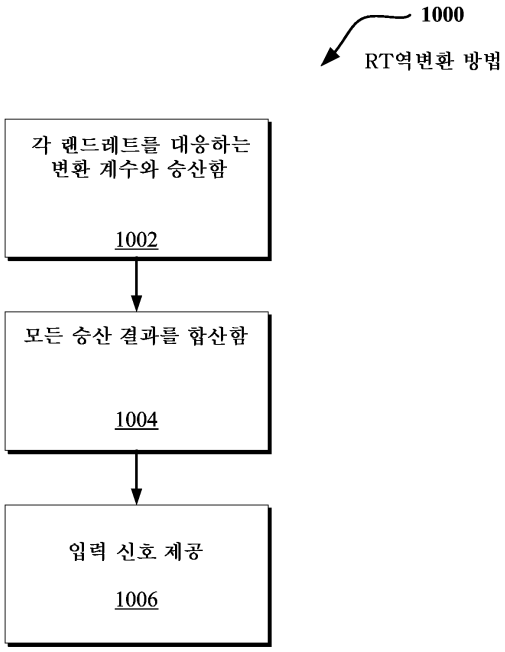
도면8


800
RT 헤싱 방법
신호 크기를 스케줄링
802
선택된 각 랜드레트를 스케일링된 신호 상에 투영
804
변환 계수 계산
806
변환 계수 양자화
808
양자화된 변환 계수에 에러 정정 적용
810
양자화된 변환계수 저장
812

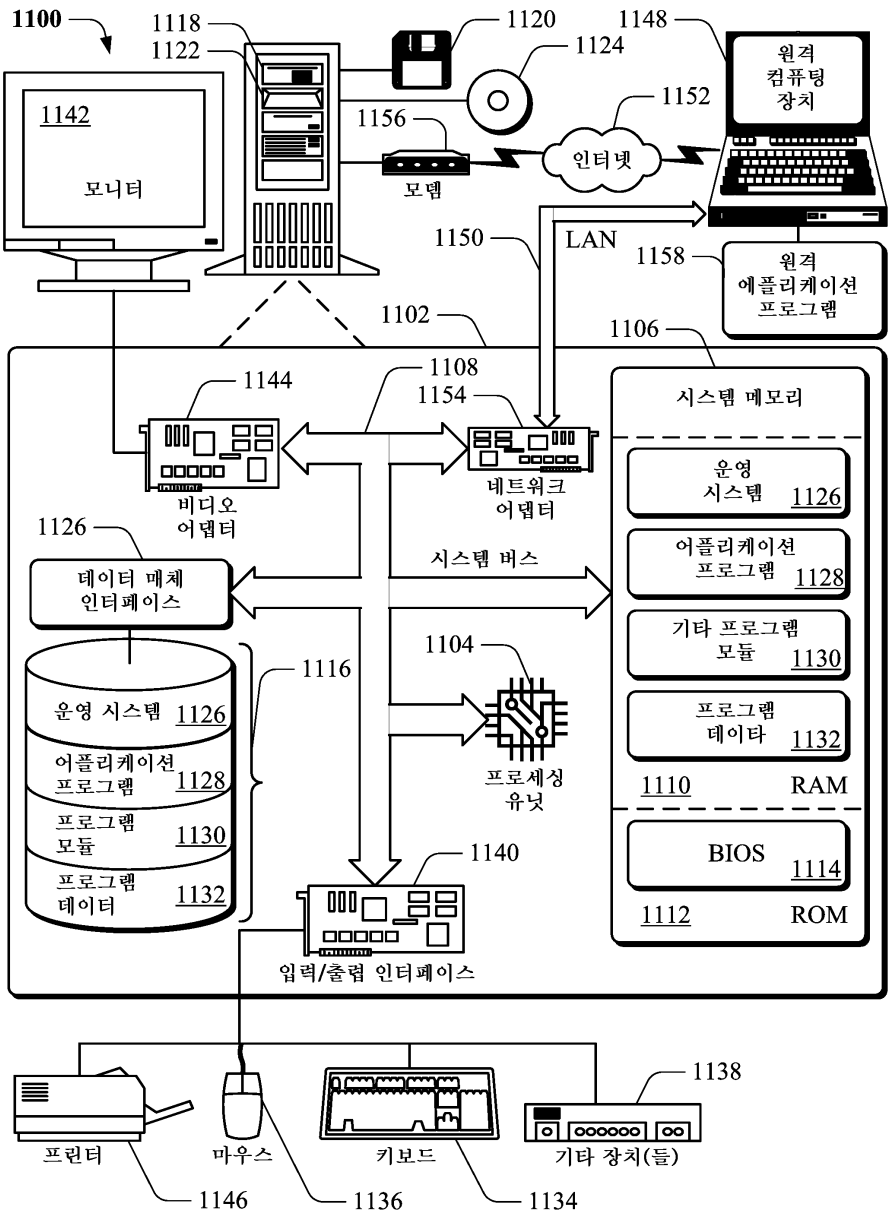
도면9


900
RT 워트마크 방법
신호 크기를 스케줄링
902
선택된 각 랜드레트를
스케일링된 신호 상에 투영
904
변환 계수 계산
906
변환 계수에
워터마크 적용
908
워터마크를 신호에
삽입
910

도면10


1000
RT역변환 방법
각 랜드레트를 대응하는 변환 계수와 승산함
1002
모든 승산 결과를 합산함
1004
입력 신호 제공
1006

도면11


1100
1118
1122
1120
1124
1148
원격
컴퓨팅
장치
1142
모니터
1156
모뎀
인터넷
1152
1150
LAN
1158
원격
에플리케이션
프로그램
1102
1106
1144
1108
1154
시스템 메모리
비디오
어댑터
네트워크
어댑터
운영
시스템
1126
1126
데이터 매체
인터페이스
시스템 버스
어플리케이션
프로그램
1128
기타 프로그램
모듈
1130
1104
1116
운영 시스템 1126
어플리케이션
프로그램 1128
프로그램
모듈 1130
프로그램
데이터 1132
프로세싱
유닛
프로그램
데이터
1132
1110
RAM
BIOS
1114
1140
1112
ROM
입력/출력 인터페이스
1138
프린터
마우스
키보드
기타 장치(들)
1146
1136
1134