(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0087295
(43) 공개일자 2013년08월06일

(51) 국제특허분류(Int. Cl.)
H04N 1/387 (2006.01) *G06T 1/00* (2006.01)
G06T 3/00 (2006.01)
(21) 출원번호 10-2012-0008534
(22) 출원일자 2012년01월27일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
차병호
경기도 수원시 영통구 매탄동 1282번지 주공그린빌아파트 504-1302
허준
서울특별시 강남구 일원본동 한솔아파트 206-103
(뒷면에 계속)
(74) 대리인
리앤목특허법인

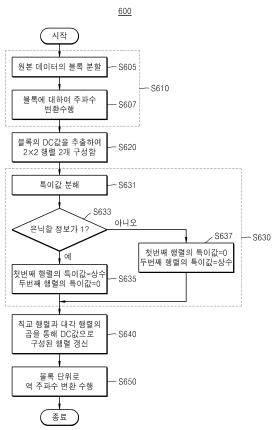
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **주파수 변환과 특이값을 이용하여 데이터에 은닉 정보를 삽입하는 방법 및 장치**

(57) 요 약

데이터에 은닉 정보를 삽입하는 방법에 있어서, 데이터를 소정 크기 단위의 블록으로 분할하고, 블록 단위로 주파수 변환을 수행하는 단계; 블록에서 획득된 적어도 하나 이상의 블록의 DC값들을 이용하여 행렬을 구성하는 단계; 각 행렬에 대하여 특이값 분해를 수행하여 각 행렬의 특이값을 획득하고, 은닉 정보에 따라 각 행렬의 특이값을 조절하는 단계; 조절된 특이값을 반영하여 행렬을 각각 갱신하고, 갱신된 행렬에 따라 각 블록의 DC값을 변경하는 단계; 및 블록 단위로 역 주파수 변환 수행하는 단계를 포함하는 정보 은닉 방법이 개시된다.

대 표 도 - 도6



(72) 발명자

이동훈

서울특별시 광진구 구의2동 28-46 201호

백종현

경기도 성남시 분당구 수내3동 푸른마을쌍용아파트 602-1205

손일권

서울특별시 구로구 신도림동 e편한세상대림4차아파트 1105-2001

특허청구의 범위

청구항 1

데이터에 은닉 정보를 삽입하는 방법에 있어서,

상기 데이터를 소정 크기 단위의 블록으로 분할하고, 상기 블록 단위로 주파수 변환을 수행하는 단계;

상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하는 단계;

상기 각 행렬에 대하여 행렬 분해를 수행하여 대각 행렬을 획득하고, 상기 대각 행렬에 포함된 특이값을 획득하여, 상기 은닉 정보에 따라 상기 특이값을 조절하는 단계;

상기 조절된 특이값을 반영하여 상기 행렬을 각각 갱신하고, 상기 갱신된 행렬에 따라 각 블록의 DC값을 변경하는 단계; 및

상기 블록 단위로 역 주파수 변환을 수행하는 단계를 포함하는 것을 특징으로 하는 정보 은닉 방법.

청구항 2

제1항에 있어서, 상기 주파수 변환은

이산 코사인 변환, 이산 웨이블렛 변환, 하다마드 변환 및 라돈 변환 중 적어도 하나를 포함하는 것을 특징으로 하는 정보 은닉 방법.

청구항 3

제1항에 있어서, 상기 행렬의 특이값을 정하는 단계는

은닉 정보가 1인 경우, 첫번째 행렬의 특이값을 0보다 큰 상수로, 두번째 행렬의 특이값을 0으로 변경하고,

은닉 정보가 0인 경우, 첫번째 행렬의 특이값을 0으로, 두번째 행렬의 특이값을 0보다 큰 상수로 변경하는 단계를 포함하는 것을 특징으로 하는 정보 은닉 방법.

청구항 4

데이터의 은닉 정보를 추출하는 방법에 있어서,

상기 데이터를 소정 크기 단위의 블록으로 분할하고, 상기 블록 단위로 주파수 변환을 수행하는 단계;

상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하는 단계;

상기 각 행렬에 대하여 행렬 분해를 수행하여 대각 행렬을 획득하고, 상기 대각 행렬에 포함된 특이값을 획득하여, 상기 각 행렬의 특이값으로부터 은닉 정보를 추출하는 단계를 포함하는 것을 특징으로 하는 정보 추출 방법.

청구항 5

제4항에 있어서, 상기 주파수 변환은

이산 코사인 변환, 이산 웨이블렛 변환, 하다마드 변환 및 라돈 변환 중 적어도 하나를 포함하는 것을 특징으로 하는 정보 추출 방법.

청구항 6

제4항에 있어서, 상기 은닉 정보를 추출하는 단계는

첫번째 행렬의 특이값이 두번째 행렬의 특이값보다 큰 경우, 은닉 정보를 1로 두고,

그 이외의 경우에는 은닉 정보를 0으로 두는 단계를 포함하는 것을 특징으로 하는 정보 추출 방법.

청구항 7

원본 데이터를 저장하는 저장부; 및

상기 원본 데이터를 소정 크기 단위의 블록으로 분할하고, 상기 블록 단위로 주파수 변환을 수행하여 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하고 상기 각 행렬에 대하여 행렬 분해를 수행하여 대각 행렬을 획득하고, 상기 대각 행렬에 포함된 특이값을 획득하여, 은닉 정보에 따라 상기 특이값을 조절하고, 상기 조절된 특이값을 반영하여 상기 행렬을 각각 갱신하고, 상기 갱신된 행렬에 따라 각 블록의 DC값을 변경하고, 상기 블록 단위로 역 주파수 변환을 수행하는 제어부를 포함하는 것을 특징으로 하는 정보 삽입 장치.

청구항 8

제7항에 있어서, 상기 제어부는

상기 원본 데이터를 소정 크기 단위의 블록으로 분할하는 블록 분할 모듈;

상기 블록 단위로 주파수 변환을 수행하여 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC 값들을 이용하여 행렬을 구성하고 상기 각 행렬에 대하여 행렬 분해를 수행하여 상기 각 행렬의 특이값을 획득하는 특이값 추출 모듈;

상기 은닉 정보에 따라 상기 각 행렬의 특이값을 조절하는 특이값 획득 모듈;

상기 조절된 특이값을 반영하여 상기 행렬을 각각 갱신하고, 상기 갱신된 행렬에 따라 각 블록의 DC값을 변경하여, 상기 블록 단위로 역 이산 코사인 변환을 수행하는 데이터 갱신 모듈을 더 포함하는 것을 특징으로 하는 정보 삽입 장치.

청구항 9

제8항에 있어서, 상기 특이값 결정 모듈은

은닉 정보가 1인 경우, 첫번째 행렬의 특이값을 0보다 큰 임의의 상수로, 두번째 행렬의 특이값을 0으로 변경하고,

은닉 정보가 0인 경우, 첫번째 행렬의 특이값을 0으로, 두번째 행렬의 특이값을 0보다 큰 임의의 상수로 변경하는 것을 특징으로 하는 정보 삽입 장치.

청구항 10

변조된 데이터를 저장하는 저장부; 및

상기 변조된 데이터를 소정 크기 단위의 블록으로 분할하고, 상기 블록 단위로 주파수 변환을 수행하여 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하고, 상기 각 행렬에 대하여 행렬 분해를 수행하여 대각 행렬을 획득하고, 상기 대각 행렬에 포함된 특이값을 획득하고, 상기 각 행렬의 특이값으로부터 은닉 정보를 추출하는 제어부를 포함하는 것을 특징으로 하는 정보 추출 장치.

청구항 11

제10항에 있어서, 상기 제어부는

상기 변조된 데이터를 소정 크기 단위의 블록으로 분할하는 블록 분할 모듈;

상기 블록 단위로 주파수 변환을 수행하여 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하고, 상기 각 행렬에 대하여 행렬 분해를 수행하여 상기 각 행렬의 특이값을 획득하는 특이값 추출 모듈; 및

상기 각 행렬의 특이값으로부터 은닉 정보를 추출하는 정보 추출 모듈을 포함하는 것을 특징으로 하는 정보 추출 장치.

청구항 12

제11항에 있어서, 상기 정보 추출 모듈은

첫번째 행렬의 특이값이 두번째 행렬의 특이값보다 큰 경우, 은닉 정보를 1로 두고,

그 이외의 경우에는 은닉 정보를 0으로 두는 것을 특징으로 하는 정보 추출 장치.

명 세 서

기 술 분 야

[0001] 본 발명은 주파수 변환과 특이값을 이용하여 데이터에 은닉 정보를 삽입하는 방법 및 장치에 대한 것이다.

배 경 기 술

[0002] 정보 은닉은 이미지, 음성과 같은 기존의 디지털 데이터에 다른 디지털 데이터를 가시 또는 가청적인 왜곡을 최소화하여 은닉하는 것을 의미한다. 주로 원본 데이터의 배포 과정에서 제작자의 권리를 증명할 수 있는 정보를 삽입함으로써 불법적인 복제나 수정을 막기 위해 이용되고 있다. 그러나 기존의 정보 은닉 기술은 주로 영상 내에 영상을 은닉하는 기술에 중점이 맞추어져 있어서, 은닉 시에 필요로 하는 정보 용량이 크고 은닉 정보의 유동성이 떨어지는 단점이 있다.

[0003] 따라서, 영상 데이터 내에 유동적으로 삽입이 가능한 문자 정보를 은닉할 수 있고, 상대적으로 문자 정보가 영상 정보에 비해 데이터 왜곡에 취약한 점을 극복하기 위하여 특이값 분해(Singular Value Decomposition)를 이용한 정보 은닉 알고리즘을 개발할 필요가 있다.

발명의 내용

[0004] 상기의 문제점을 해결하기 위한 본 발명의 목적은 이미지 또는 영상 데이터를 변조하여 은닉 정보를 삽입하는 방법 및 장치를 제공하는 것이다.

[0005] 상기의 목적을 달성하기 위한 본 발명의 일 실시예가 갖는 하나의 특징은, 데이터에 은닉 정보를 삽입하는 방법에 있어서, 상기 데이터를 소정 크기 단위의 블록으로 분할하고, 상기 블록 단위로 주파수 변환을 수행하는 단계; 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하는 단계; 상기 각 행렬에 대하여 행렬 분해를 수행하여 대각 행렬을 획득하고, 상기 대각 행렬에 포함된 특이값을 획득하여, 상기 은닉 정보에 따라 상기 각 행렬의 특이값을 조절하는 단계; 상기 조절된 특이값을 반영하여 상기 행렬을 각각 갱신하고, 상기 갱신된 행렬에 따라 각 블록의 DC값을 변경하는 단계; 및 상기 블록 단위로 역 주파수 변환을 수행하는 단계를 포함하는 것이다.

[0006] 더하여, 상기 주파수 변환은 이산 코사인 변환, 이산 웨이블렛 변환, 하다마드 변환 및 라돈 변환 중 적어도 하나를 포함하는 것을 특징으로 한다.

[0007] 더하여, 상기 행렬의 특이값을 정하는 단계는 은닉 정보가 1인 경우, 첫번째 행렬의 특이값을 0보다 큰 상수로, 두번째 행렬의 특이값을 0으로 변경하고, 은닉 정보가 0인 경우, 첫번째 행렬의 특이값을 0으로, 두번째 행렬의 특이값을 0보다 큰 상수로 변경하는 단계를 포함하는 것을 특징으로 한다.

[0008] 상기의 목적을 달성하기 위한 본 발명의 일 실시예가 갖는 하나의 특징은, 데이터의 은닉 정보를 추출하는 방법에 있어서, 상기 데이터를 소정 크기 단위의 블록으로 분할하고, 상기 블록 단위로 주파수 변환을 수행하는 단계; 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하는 단계; 상기 각 행렬에 대하여 행렬 분해를 수행하여 대각 행렬을 획득하고, 상기 대각 행렬에 포함된 특이값을 획득하여, 상기 각 행렬의 특이값으로부터 상기 은닉 정보를 추출하는 단계를 포함하는 것이다.

[0009] 더하여, 상기 주파수 변환은 이산 코사인 변환, 이산 웨이블렛 변환, 하다마드 변환 및 라돈 변환 중 적어도 하나를 포함하는 것을 특징으로 한다.

[0010] 더하여, 상기 은닉 정보를 추출하는 단계는 첫번째 행렬의 특이값이 두번째 행렬의 특이값보다 큰 경우, 은닉 정보를 1로 두고, 그 이외의 경우에는 은닉 정보를 0으로 두는 단계를 포함하는 것을 특징으로 한다.

[0011] 상기의 목적을 달성하기 위한 본 발명의 일 실시예가 갖는 하나의 특징은, 원본 데이터를 저장하는 저장부; 및 상기 원본 데이터를 소정 크기 단위의 블록으로 분할하고, 상기 블록 단위로 주파수 변환을 수행하여 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하고, 상기 각 행렬에 대하여 행렬 분해를 수행하여 대각 행렬을 획득하고, 상기 대각 행렬에 포함된 특이값을 획득하여, 상기 은닉 정보에 따라 상기 특이값을 조절하고, 상기 조절된 특이값을 반영하여 상기 행렬을 각각 갱신하고, 상기 갱신된 행렬에 따라 각 블록의 DC값을 변경하고, 상기 블록 단위로 역 주파수 변환을 수행하는 제어부를 포함하는 것을 특징으로 하

는 정보 삽입 장치를 제공하는 것이다.

[0012] 더하여, 상기 제어부는 상기 원본 데이터를 소정 크기 단위의 블록으로 분할하는 블록 분할 모듈; 상기 블록 단위로 주파수 변환을 수행하여 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC 값들을 이용하여 행렬을 구성하고 상기 각 행렬에 대하여 행렬 분해를 수행하여 상기 각 행렬의 특이값을 획득하는 특이값 추출 모듈; 은닉 정보에 따라 상기 각 행렬의 특이값을 조절하는 특이값 획득 모듈; 상기 조절된 특이값을 반영하여 상기 행렬을 각각 갱신하고, 상기 갱신된 행렬에 따라 각 블록의 DC값을 변경하여, 상기 블록 단위로 역 이산 코사인 변환을 수행하는 데이터 갱신 모듈을 더 포함하는 것을 특징으로 한다.

[0013] 더하여, 상기 특이값 결정 모듈은 은닉 정보가 1인 경우, 첫번째 행렬의 특이값을 0보다 큰 임의의 상수로, 두번째 행렬의 특이값을 0으로 변경하고, 은닉 정보가 0인 경우, 첫번째 행렬의 특이값을 0으로, 두번째 행렬의 특이값을 0보다 큰 임의의 상수로 변경하는 것을 특징으로 한다.

[0014] 상기의 목적을 달성하기 위한 본 발명의 일 실시예가 갖는 하나의 특징은, 변조된 데이터를 저장하는 저장부; 및 상기 변조된 데이터를 소정 크기 단위의 블록으로 분할하고, 상기 블록 단위로 주파수 변환을 수행하여 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하고, 상기 각 행렬에 대하여 행렬 분해를 수행하여 상기 각 행렬의 특이값을 획득하고, 상기 각 행렬의 특이값으로부터 은닉 정보를 추출하는 제어부를 포함하는 것을 특징으로 하는 정보 추출 장치를 제공하는 것이다.

[0015] 더하여, 상기 제어부는 상기 변조된 데이터를 소정 크기 단위의 블록으로 분할하는 블록 분할 모듈; 상기 블록 단위로 주파수 변환을 수행하여 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하고, 상기 각 행렬에 대하여 행렬 분해를 수행하여 상기 각 행렬의 특이값을 획득하는 특이값 추출 모듈; 및 상기 각 행렬의 특이값으로부터 은닉 정보를 추출하는 정보 추출 모듈을 포함하는 것을 특징으로 한다.

[0016] 더하여, 상기 정보 추출 모듈은 첫번째 행렬의 특이값이 두번째 행렬의 특이값보다 큰 경우, 은닉 정보를 1로 두고, 그 이외의 경우에는 은닉 정보를 0으로 두는 것을 특징으로 한다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 일 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 은닉 정보를 삽입하고 삽입된 은닉 정보를 데이터로부터 추출하는 시스템을 나타낸 블록도이다.

도 2는 본 발명의 제1 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 은닉 정보를 삽입하기 위한 정보 삽입 장치의 구조를 나타낸 블록도이다.

도 3은 본 발명의 제2 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 은닉 정보를 삽입하기 위한 정보 삽입 장치의 구조를 나타낸 블록도이다.

도 4는 본 발명의 제3 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 삽입된 은닉 정보를 추출하기 위한 정보 추출 장치의 구조를 나타낸 블록도이다.

도 5는 본 발명의 제4 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 삽입된 은닉 정보를 추출하기 위한 정보 추출 장치의 구조를 나타낸 블록도이다.

도 6은 본 발명의 제1 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 은닉 정보를 삽입하는 방법을 나타낸 순서도이다.

도 7은 본 발명의 제3 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 삽입된 은닉 정보를 추출하는 방법을 나타낸 순서도이다.

도 8은 본 발명의 일 실시 예에 의한 데이터에 은닉 정보를 삽입하는 방법을 나타낸 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하 본 발명의 바람직한 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 또한, 도면 전체에 걸쳐 동일한 구성 요소들은 가능한 한 동일한 도면 부호로 나타내고 있음에 유의하여야 한다.

[0019] 이하에서 설명되는 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이거나 사전적인 의미로 한정해서 해석되어서는 아니 되며, 발명자는 그 자신의 발명을 가장 최선의 방법으로 설명하기 위한 용어로 적절하게 정의

할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야만 한다. 따라서 본 명세서에 기재된 실시 예와 도면에 도시된 구성은 본 발명의 가장 바람직한 일 실시 예에 불과할 뿐이고, 본 발명의 기술적 사상을 모두 대변하는 것은 아니므로, 본 출원시점에 있어서 이들을 대체할 수 있는 다양한 균등물과 변형 예들이 있을 수 있음을 이해하여야 한다.

[0020] 도 1은 본 발명의 일 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 은닉 정보를 삽입하고 삽입된 은닉 정보를 데이터로부터 추출하는 시스템을 나타낸 블록도이다.

[0021] 본 발명의 일 실시 예에 있어서, 데이터는 이미지뿐만 아니라 영상 데이터도 적용될 수 있으며 가시적으로 출력될 수 있는 것이면 변조되는 데이터 종류에 대한 제한은 없다.

[0022] 도 1을 참조하면, 본 발명의 일 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 은닉 정보를 삽입하고 삽입된 은닉 정보를 데이터로부터 추출하는 시스템은 정보 삽입 장치(200) 및 정보 추출 장치(400)를 포함할 수 있다.

[0023] 정보 삽입 장치(200)는 주파수 변환과 특이값 분해를 이용하여 데이터에 은닉 정보를 삽입하는 장치이다. 더 구체적으로, 원본 데이터를 소정 크기 단위의 블록으로 분할하고, 상기 블록 단위로 주파수 변환을 수행하여 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하고, 상기 각 행렬에 대하여 행렬 분해를 수행하여 상기 각 행렬의 특이값(singular value)을 획득하고, 은닉 정보에 따라 상기 각 행렬의 특이값을 조절하고, 상기 조절된 특이값을 반영하여 상기 행렬을 각각 갱신하고, 상기 갱신된 행렬에 따라 각 블록의 DC값을 변경하고, 상기 블록 단위로 역 주파수 변환을 수행한다.

[0024] 더하여 본 발명의 일 실시 예에 있어서, 데이터에 삽입되는 은닉 정보는 문자, 숫자 등의 텍스트 정보, 비디오 및 오디오 정보를 포함하는 미디어 정보 등을 포함할 수 있으며 은닉 정보의 종류에 대한 제한은 없다. 단 은닉 정보는 이진 정보로 변환할 수 있으며 삽입되는 정보는 0 또는 1인 것으로 정하였다. 즉, 데이터에 삽입되는 정보는 이진 정보일 수 있다. 또한, 은닉 정보는 이진 정보로 변환될 수 있는 모든 정보가 될 수 있다.

[0025] 더하여 본 발명의 일 실시 예에 있어서, 행렬 분해는 특이값 분해가 포함될 수 있다. 특이값 분해(Singular Value Decomposition, SVD)는 행렬을 특정한 구조로 분해하는 방식으로, 직교 정사각행렬을 고유값을 기저로 하여 대각행렬로 분해할 수 있다. 즉, 행렬 M에 대하여 직교 행렬, 대각 행렬 및 유니터리 행렬 등 세 행렬의 곱으로 나타내는 것을 M의 특이값 분해라고 하며, 이때 대각 행렬의 대각선 성분들은 M의 특이값이 된다. 이하 본 발명의 일 실시 예에 있어서 행렬 분해는 특이값 분해를 수행하는 것을 기준으로 설명하기로 한다.

[0026] 정보 추출 장치(400)는 정보 삽입 장치(200)에 의해 정보가 삽입된 데이터로부터 삽입된 정보를 추출한다. 더 구체적으로, 원본 데이터를 소정 크기 단위의 블록으로 분할하고, 블록 단위로 주파수 변환을 수행하여 블록에서 획득된 적어도 하나 이상의 블록의 DC값들을 이용하여 행렬을 구성하고, 상기 각 행렬에 대하여 특이값 분해를 수행하여 상기 각 행렬의 특이값을 획득하고, 은닉 정보에 따라 상기 각 행렬의 특이값을 조절하고, 상기 조절된 특이값을 반영하여 상기 행렬을 각각 갱신하고, 상기 갱신된 행렬에 따라 각 블록의 DC값을 변경하고, 상기 블록 단위로 역 주파수 변환을 수행한다.

[0027] 정보 삽입 장치(200) 및 정보 추출 장치(400)는 사용자가 이용하는 다양한 형태의 장치로서, 예를 들면, PC(Personal Computer), 노트북 컴퓨터, 휴대폰(mobile phone), 태블릿 PC, 내비게이션(navigation) 단말기, 스마트폰(smart phone), PDA(Personal Digital Assistants), 스마트 TV(Smart TV), PMP(Portable Multimedia Player) 및 디지털방송 수신기를 포함할 수 있다. 물론 이는 예시에 불과할 뿐이며, 상술한 예 이외에도 현재 개발되어 상용화되었거나 향후 개발될 모든 통신이 가능한 장치를 포함하는 개념으로 해석되어야 한다. 더하여, 정보 삽입 장치(200)와 정보 추출 장치(400)는 이외에도 데이터에 정보를 삽입하는 서버 장치일 수 있다.

[0028] 더하여, 본 발명의 일 실시 예에서 정보 삽입과 정보 추출은 각각 분리되어 각각 다른 장치에서 수행될 수 있도록 표현되어 있으나, 정보 삽입과 정보 추출이 하나의 장치에서 이루어 질 수 있도록 구성될 수 있다.

[0029] 정보 삽입 장치(200)와 정보 추출 장치(400)는 유선 또는 무선으로 데이터의 송수신이 가능하며, 예를 들면 근거리 무선통신(블루투스(Bluetooth), Zigbee, RFID(Radio Frequency Identification), 적외선 통신(IrDA, infrared Data Association), UWB(Ultra Wideband) 등) 또는 근거리 유선통신(USB 등) 중에서 하나 이상의 방식으로 통신을 수행할 수 있다.

[0030] 또한 정보 삽입 장치(200)와 정보 추출 장치(400)는 네트워크를 통해 데이터를 송수신할 수 있다. 이러한 네트워크는 인터넷 프로토콜(IP)을 통하여 대용량 데이터의 송수신 서비스 및 끊기는 현상이 없는 데이터 서비스를

제공하는 아이피망으로, 아이피를 기반으로 서로 다른 망을 통합한 아이피망 구조인 올 아이피(All IP)망 일 수 있다. 또한, 네트워크는 유선네트워크, Wibro(Wireless Broadband)망, WCDMA를 포함하는 3 세대 이동네트워크, HSDPA(High Speed Downlink Packet Access)망 및 LTE망을 포함하는 3.5세대 이동네트워크, LTE advanced를 포함하는 4세대 이동네트워크, 위성네트워크 및 와이파이(Wi-Fi)망을 포함하는 무선랜 중 하나 이상을 포함하여 이루어질 수 있다.

[0031] 도 2는 본 발명의 제1 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 은닉 정보를 삽입하기 위한 정보 삽입 장치(200)의 구조를 나타낸 블록도이다. 도 2의 정보 삽입 장치(200)는 도 3의 정보 삽입 장치(300)와 대응될 수 있다.

[0032] 도 2를 참조하면, 본 발명의 제1 실시 예에 의한 정보 삽입 장치(200)는 저장부(210) 및 제어부(220)를 포함할 수 있다.

[0033] 본 발명의 제1 실시 예에 있어서, 저장부(210)는 정보 삽입 장치(200)의 동작에 필요한 데이터 혹은 프로그램을 저장한다. 기본적으로 정보 삽입 장치(200)의 운용 프로그램(OS) 및 하나 이상의 응용 프로그램을 저장할 수 있다. 구체적으로, 저장부(210)는 은닉 정보를 삽입할 원본 데이터를 저장할 수 있다. 저장부(210)는 램(RAM, Read Access Memory), 롬(ROM, Read Only Memory), 하드디스크(HDD, Hard Disk Drive), 플래시 메모리, CD-ROM, DVD와 같은 모든 종류의 저장 매체를 포함할 수 있다.

[0034] 제어부(220)는 정보 삽입 장치(200)의 동작 전반을 제어하는 것으로서, 기본적으로 저장부(210)에 저장한 운영 프로그램을 기반으로 동작하여 정보 삽입 장치(200)의 기본적인 플랫폼 환경을 구축하고, 사용자의 선택에 따라서 응용 프로그램을 실행하여 임의 기능을 제공한다.

[0035] 구체적으로, 제어부(220)는 원본 데이터를 소정 크기 단위의 블록으로 분할하고, 상기 블록 단위로 주파수 변환을 수행하여 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하고, 상기 각 행렬에 대하여 특이값 분해를 수행하여 상기 각 행렬의 특이값을 획득하고, 은닉 정보에 따라 상기 각 행렬의 특이값을 조절하고, 상기 조절된 특이값을 반영하여 상기 행렬을 각각 갱신하고, 상기 갱신된 행렬에 따라 각 블록의 DC값을 변경하고, 상기 블록 단위로 역 주파수 변환을 수행한다.

[0036] 이때 주파수 변환은 이산 코사인 변환(DCT; Discrete Cosine Transform), 이산 웨이블렛 변환(DWT; Discrete Wavelet Transform), 하다마드(Hadamard) 변환 및 라돈(Radon) 변환 중 적어도 하나를 포함할 수 있다.

[0037] 도 3은 본 발명의 제2 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 은닉 정보를 삽입하기 위한 정보 삽입 장치(300)의 구조를 나타낸 블록도이다. 도 2의 정보 삽입 장치(200)는 도 3의 정보 삽입 장치(300)와 대응될 수 있다.

[0038] 도 3을 참조하면, 본 발명의 제2 실시 예에 의한 정보 삽입 장치(300)는 저장부(310), 제어부(320), 입력부(330), 출력부(340) 및 통신부(350)를 포함할 수 있다. 상기 저장부(310)와 제어부(320)는 도 2의 저장부(210) 및 제어부(220)와 대응되는 것으로서 중복되는 내용은 생략하기로 한다.

[0039] 본 발명의 제2 실시 예에 있어서, 제어부(320)는 블록 분할 모듈(321), 특이값 추출 모듈(322), 특이값 획득 모듈(323) 및 데이터 갱신 모듈(324)을 포함할 수 있다.

[0040] 블록 분할 모듈(321)은 원본 데이터(311)를 소정 크기 단위의 블록으로 분할한다. 하나의 블록에는 적어도 하나 이상의 픽셀(원본 데이터(311)가 이미지 또는 영상 데이터인 경우) 또는 픽셀과 대응되는 단위 요소를 가지고 각 단위 요소 또는 픽셀은 고유한 값을 가진다. 본 발명에서는 설명의 편의를 위해 픽셀을 기준으로 설명하기로 한다. 본 발명의 일 실시 예에 있어서, 블록을 기준으로 주파수를 변환하여 적어도 하나 이상의 블록의 DC값을 추출하고 DC값을 이용하여 행렬을 구성하고 행렬의 특이값을 바꾸어 원본 데이터(112)를 변조할 수 있다.

[0041] 본 발명의 일 실시 예에서, 데이터의 블록을 분할하기 전에 원본 데이터에서 특정 채널의 데이터를 분리하여 은닉 정보를 삽입할 수 있다. 예를 들면, 이미지 데이터가 RGB 채널을 가지는 경우, B 채널을 분리하여 본 발명에 따라 은닉 정보를 삽입할 수 있다. YUV, HSV 채널을 가지는 경우에도 마찬가지로 특정 채널을 분리하여 은닉 정보를 삽입할 수 있다.

[0042] 특이값 추출 모듈(322)은 블록 분할 모듈(321)에 의해 분할된 블록에서 은닉 정보를 삽입하고자 하는 적어도 하나 이상의 블록에 대하여 블록 단위로 주파수 변환을 수행하여 각 블록에서 획득된 DC 값들을 이용하여 행렬을 구성하고 구성된 행렬에 대하여 특이값 분해를 수행하여 행렬의 특이값을 추출할 수 있다. 이하 도 8을 참조하

여 특이값 추출 방법에 대해 자세히 설명하기로 한다.

[0043] 도 8은 본 발명의 일 실시 예에 의한 데이터에 은닉 정보를 삽입하는 방법을 나타낸 예시도이다.

[0044] 도 8(a)를 참조하면, 원본 데이터를 소정 크기 단위의 블록으로 분할하여 은닉 정보를 삽입할 블록을 선택한다. 특정 채널에 대하여 은닉 정보를 삽입하고자 하는 경우에는 원본 데이터에서 특정 채널을 분리하여 블록을 분할할 수 있다. 이때 행렬 크기에 따라 선택할 블록의 개수가 달라지며, 2 by 2 행렬을 이용하는 경우에는 8개의 블록을 중복 없이 선택한다. 또한, 3 by 3 행렬을 이용하는 경우, 18개의 블록의 블록을 중복 없이 선택한다.

[0045] 선택한 블록에 대하여 각각 블록 단위로 주파수 변환을 수행하고, 각 블록의 DC 값을 추출하여 행렬을 구성하고 각 행렬에 대하여 특이값 분해를 수행하면, 두 개의 직교 행렬과 한 개의 대각행렬로 분해된다. 이 중 특이값은 대각행렬의 대각 원소로 나타나고, 이 원소들은 내림차순으로 정렬되어 있다. 특이값은 원본 이미지의 명도 및 채도의 강도를 나타내므로, 이의 변경을 통한 정보 은닉 시에 이미지를 열화를 줄이기 위해 이미지의 기여도가 적은, 낮은 차수의 특이값을 선택할 수 있다. 따라서 본 발명의 일 실시 예에서 특이값은 대각 행렬의 (2, 2)에 위치한 값이 사용될 수 있다. 다른 행렬에 대하여도 특이값 분해를 적용하여 같은 위치의 특이값을 선택하며, 각 행렬에서 선택된 특이값이 정보 은닉에 이용될 수 있다. 행렬의 개수에 따라 정보 은닉에 이용되는 특이값의 개수가 달라질 수 있으며, 이하 설명의 편의를 위해 2개의 행렬을 구성하고 2개의 특이값을 정보 은닉에 이용하는 것을 기준으로 설명하기로 한다.

[0046] 다시 도 3으로 돌아가서 계속 설명하면, 특이값 획득 모듈(323)은 은닉 정보에 따라 상기 각 행렬의 특이값을 조절한다.

[0047] 자세히 설명하면, 은닉 정보에 따라 선택된 2개의 특이값의 대소 관계를 임의로 조정함으로써 정보를 은닉할 수 있다. 예를 들면, 은닉 정보가 1일 경우에는 2개의 특이값 중 먼저 선택된 네 개의 블록에서 얻어진 특이값을 0보다 큰 상수로 변경하고, 나머지 네 개의 블록에서 얻어진 특이값을 0으로 바꾼다. 은닉 정보가 0일 경우에는 1의 경우와 반대로 먼저 선택된 행렬의 특이값을 0으로, 다른 행렬의 특이값을 0보다 큰 상수로 바꾼다.

[0048] 데이터 갱신 모듈(324)은 은닉 정보에 따라 바뀐 특이값을 반영하여 상기 행렬을 각각 갱신하고, 상기 갱신된 행렬에 따라 각 블록의 DC값을 변경하여, 상기 블록 단위로 역 주파수 변환을 수행한다.

[0049] 자세히 설명하면, 각각의 대각 행렬의 (2,2) 위치의 원소를 바꾼 특이값으로 교체한 후, 특이값 분해 시에 얻어졌던 기존의 두 개의 직교 행렬과의 곱을 통해 정보가 은닉된 두 개의 행렬을 얻을 수 있다. 정보 은닉을 위해 선택되었던 DC 값들을 구해진 행렬 내의 원소들로 대체하면 1비트의 정보 은닉이 완료되며 처음에 수행했던 블록 단위 주파수 변환과 같은 크기의 블록 단위로 역 주파수 변환을 수행하게 되면 알고리즘의 수행이 완료된다. 대체될 DC 값의 위치는 은닉 정보를 삽입하기 전의 행렬 구성 시에 선택된 블록의 위치와 동일할 수 있다. 원본 데이터 내에서 선택되는 블록이 겹치지 않게 블록을 이동하며 은닉할 정보에 따라 정보 삽입 과정을 반복할 수 있다.

[0050] 입력부(330)는 사용자의 조작에 따라서 정보 삽입 장치(300)을 제어하거나 동작하기 위한 사용자 입력 신호를 발생하는 수단으로서, 다양한 방식의 입력 수단으로 구현될 수 있다. 예를 들어, 입력부(330)는 키 입력 수단, 터치 입력 수단, 제스처 입력 수단, 음성 입력 수단 중에서 하나 이상을 포함할 수 있다. 키 입력 수단은, 키 조작에 따라서 해당 키에 대응하는 신호를 발생시키는 것으로서, 키패드, 키보드가 해당된다. 터치 입력 수단은, 사용자가 특정 부분을 터치하는 동작을 감지하여 입력 동작을 인식하는 것으로서, 터치 패드, 터치 스크린, 터치 센서를 들 수 있다. 제스처 입력 수단은, 사용자의 동작, 예를 들어, 단말을 흔들거나 움직이는 동작, 단말에 접근하는 동작, 눈을 깜빡이는 동작 등 지정된 특정 동작을 특정 입력 신호로 인식하는 것으로서, 지자기 센서, 가속도 센서, 카메라, 고도계, 자이로 센서, 근접 센서 중에서 하나 이상을 포함하여 이루어질 수 있다.

[0051] 본 발명의 제2 실시 예에 있어서, 입력부(330)는 사용자의 조작에 따라서 은닉 정보와 은닉 정보를 삽입할 원본 데이터(311)를 선택하여 은닉 정보를 삽입할 수 있다.

[0052] 출력부(340)는 본 발명의 제2 실시 예에 있어서 데이터에 정보를 삽입하기 위한 사용자 인터페이스를 화면에 출력한다. 예를 들면, LCD((Liquid Crystal Display), TFT-LCD(Thin Film Transistor-Liquid Crystal Display), LED(Light Emitting Diodes), OLED(Organic Light Emitting Diodes), AMOLED(Active Matrix Organic Light Emitting Diodes), 플렉시블 디스플레이(flexible display), 3차원 디스플레이 중에서 어느 하나가 될 수 있다.

[0053] 본 발명의 제2 실시 예에 있어서, 통신부(350)는 정보 추출 장치(400, 500)와 유무선 통신 또는 적외선 통신, 네트워크 등을 통해 데이터를 송수신할 수 있다.

[0054] 도 4는 본 발명의 제3 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 삽입된 은닉 정보를 추출하기 위한 정보 추출 장치(400)의 구조를 나타낸 블록도이다. 도 4를 참조하면, 본 발명의 제3 실시 예에 의한 정보 추출 장치(400)는 저장부(410) 및 제어부(420)를 포함할 수 있고, 도 4의 정보 추출 장치(400)는 도 5의 정보 추출 장치(500)와 대응될 수 있다.

[0055] 본 발명의 제3 실시 예에 있어서, 저장부(410)는 정보 추출 장치(400)의 동작에 필요한 데이터 혹은 프로그램을 저장한다. 기본적으로 정보 추출 장치(400)의 운용 프로그램(OS) 및 하나 이상의 응용 프로그램을 저장한다. 자세히 설명하면, 은닉 정보를 추출할 변조된 데이터를 저장할 수 있다. 저장부(410)는 램(RAM, Read Access Memory), 롬(ROM, Read Only Memory), 하드디스크(HDD, Hard Disk Drive), 플래시 메모리, CD-ROM, DVD와 같은 모든 종류의 저장 매체를 포함할 수 있다.

[0056] 제어부(420)는 정보 추출 장치(400)의 동작 전반을 제어하는 것으로서, 기본적으로 저장부(410)에 저장한 운영 프로그램을 기반으로 동작하여 정보 추출 장치(400)의 기본적인 플랫폼 환경을 구축하고, 사용자의 선택에 따라서 응용 프로그램을 실행하여 임의 기능을 제공한다.

[0057] 구체적으로, 제어부(420)는 은닉 정보가 삽입되어 데이터가 변조된 데이터를 소정 크기 단위의 블록으로 분할하고, 상기 블록 단위로 주파수 변환을 수행하여 상기 블록에서 획득된 적어도 하나 이상의 상기 블록의 DC값들을 이용하여 행렬을 구성하고, 상기 각 행렬에 대하여 특이값 분해를 수행하여 상기 각 행렬의 특이값을 획득하고, 상기 각 행렬의 특이값으로부터 은닉 정보를 추출한다.

[0058] 도 5는 본 발명의 제4 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 삽입된 은닉 정보를 추출하기 위한 정보 추출 장치(500)의 구조를 나타낸 블록도이다.

[0059] 도 5를 참조하면, 본 발명의 제4 실시 예에 의한 정보 추출 장치(400)는 저장부(410), 제어부(420), 입력부(530), 출력부(540) 및 통신부(550)를 포함할 수 있고, 도 4의 정보 추출 장치(400)는 도 5의 정보 추출 장치(500)와 대응될 수 있다. 상기 저장부(410)와 제어부(420)는 도 4의 저장부(310) 및 제어부(320)와 대응되는 것으로서 중복되는 내용은 생략하기로 한다.

[0060] 본 발명의 제4 실시 예에 있어서, 제어부(520)는 블록 분할 모듈(521), 특이값 추출 모듈(522) 및 정보 추출 모듈(523)을 포함할 수 있다.

[0061] 블록 분할 모듈(521)은 변조된 데이터(511)를 소정 크기 단위의 블록으로 분할한다. 본 발명의 일 실시 예에 있어서, 블록 단위로 주파수 변환을 수행하여 DC 값을 추출하고 각 블록의 DC 값을 이용하여 행렬을 구성하여 특이값을 추출하고, 각 행렬의 특이값을 비교함으로써 은닉 정보를 추출할 수 있다.

[0062] 특이값 추출 모듈(522)은 블록 단위로 주파수 변환을 수행하여 각 블록에서 획득된 DC값들을 이용하여 행렬을 구성하고, 상기 각 행렬에 대하여 특이값 분해를 수행하여 상기 각 행렬의 특이값을 획득할 수 있다.

[0063] 정보 추출 모듈(523)은 상기 각 행렬의 특이값으로부터 은닉 정보를 추출할 수 있다. 자세히 설명하면, 각 행렬의 특이값의 대소 여부를 판단함으로써 숨겨진 정보를 추출할 수 있다. 은닉 정보가 문자 정보인 경우에는, 추출된 이진 정보를 7비트씩 분할하여 최상위 비트 0을 추가한 후 아스키 코드(ASCII code)에 따라 복호하면 은닉된 문자 정보를 복원해 낼 수 있다. 은닉된 정보의 종류는 이진 정보로 변환될 수 있는 것이면 제한되지 않는다.

[0064] 입력부(530)는 사용자의 조작에 따라서 정보 추출 장치(500)을 제어하거나 동작하기 위한 사용자 입력 신호를 발생하는 수단으로서, 다양한 방식의 입력 수단으로 구현될 수 있다. 예를 들어, 입력부(530)는 키 입력 수단, 터치 입력 수단, 제스처 입력 수단, 음성 입력 수단 중에서 하나 이상을 포함할 수 있다. 키 입력 수단은, 키 조작에 따라서 해당 키에 대응하는 신호를 발생시키는 것으로서, 키패드, 키보드가 해당된다. 터치 입력 수단은, 사용자가 특정 부분을 터치하는 동작을 감지하여 입력 동작을 인식하는 것으로서, 터치 패드, 터치 스크린, 터치 센서를 들 수 있다. 제스처 입력 수단은, 사용자의 동작, 예를 들어, 단말을 흔들거나 움직이는 동작, 단말에 접근하는 동작, 눈을 깜빡이는 동작 등 지정된 특정 동작을 특정 입력 신호로 인식하는 것으로서, 지자기 센서, 가속도 센서, 카메라, 고도계, 자이로 센서, 근접 센서 중에서 하나 이상을 포함하여 이루어질 수 있다.

[0065] 본 발명의 제4 실시 예에 있어서, 입력부(530)는 사용자의 조작에 따라서 은닉 정보를 추출할 변조된 데이터

(511)를 선택하여 은닉 정보를 추출할 수 있다.

[0066] 출력부(540)는 본 발명의 제4 실시 예에 있어서 데이터에 삽입된 은닉 정보를 추출하기 위한 사용자 인터페이스를 화면에 출력한다. 예를 들면, LCD((Liquid Crystal Display), TFT-LCD(Thin Film Transistor-Liquid Crystal Display), LED(Light Emitting Diodes), OLED(Organic Light Emitting Diodes), AMOLED(Active Matrix Organic Light Emitting Diodes), 플렉시블 디스플레이(flexible display), 3차원 디스플레이 중에서 어느 하나가 될 수 있다.

[0067] 본 발명의 제4 실시 예에 있어서, 통신부(550)는 정보 삽입 장치(200,300)와 유무선 통신 또는 적외선 통신, 네트워크 등을 통해 데이터를 송수신할 수 있다. 따라서, 정보 추출 장치(500)는 정보가 삽입된 변조된 데이터(511)를 정보 삽입 장치(200,300)로부터 수신할 수 있다.

[0068] 도 6은 본 발명의 제1 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 은닉 정보를 삽입하는 방법을 나타낸 순서도(600)이다.

[0069] 도 6을 참조하면, 데이터를 소정 크기 단위의 블록으로 분할하고(S605) 분할된 블록 단위로 주파수 변환을 수행한다(S607).

[0070] 그리고 각 블록의 DC 값을 추출하여 행렬을 구성한다(S620). 본 발명의 일 실시 예에 따르면, 8개의 블록을 선택하고 선택한 블록의 DC 값을 추출하여 2 by 2 행렬을 2개 구성할 수 있다.

[0071] 상기 각 행렬에 대하여 특이값 분해를 수행하여 상기 각 행렬의 특이값을 획득하고, 은닉 정보에 따라 상기 각 행렬의 특이값을 조절할 수 있다(S630). 구체적으로, 각 행렬에 대하여 특이값 분해를 수행하고(S631), 은닉 정보가 1인 경우 첫번째 행렬의 특이값을 0보다 큰 상수로 두고 두번째 행렬의 특이값을 0으로 둘 수 있다(S635). 은닉 정보가 1이 아닌 경우, 즉 0인 경우, 첫번째 행렬의 특이값을 0으로 두고 두번째 행렬의 특이값을 0보다 큰 상수로 둘 수 있다(S637).

[0072] 특이값 분해 시 계산되었던 직교 행렬과 S630 단계에서 조절된 특이값이 반영된 대각 행렬의 곱을 통해 DC 값으로 구성된 행렬을 갱신하고, 상기 갱신된 행렬에 따라 각 블록의 DC 값을 변경할 수 있다(S640). 변경된 각 블록의 DC 값에 따라 블록 단위로 역 주파수 변환을 수행하여(S650) 은닉 정보가 삽입된 데이터를 생성할 수 있다.

[0073] 도 7은 본 발명의 제3 실시 예에 의한 주파수 변환과 특이값 분해를 이용하여 데이터에 삽입된 은닉 정보를 추출하는 방법을 나타낸 순서도(700)이다.

[0074] 도 7을 참조하면, 데이터를 소정 크기 단위의 블록으로 분할하고(S711) 분할된 블록 단위로 주파수 변환을 수행한다(S713).

[0075] 그리고 각 블록의 DC 값을 추출하여 행렬을 구성한다(S720). 본 발명의 일 실시 예에 따르면, 8개의 블록을 선택하고 선택한 블록의 DC 값을 추출하여 2 by 2 행렬을 2개 구성할 수 있다.

[0076] 각 행렬의 특이값을 비교하여(S730), S730 단계의 판단 결과에 따라, 데이터에 삽입된 은닉 정보를 추출할 수 있다. 구체적으로, 각 행렬의 특이값을 분해하여 특이값을 추출하고(S730), 첫번째 행렬의 특이값이 두번째 행렬의 특이값보다 큰 경우 은닉 정보는 1로 두고(S735), 그 이외의 경우에는 은닉 정보를 0으로 둘 수 있다(S737). 은닉 정보의 값이나 각 행렬의 특이값을 비교하는 방법은 경우에 따라 다르게 설정할 수 있으며, 두 개의 행렬의 특이값을 비교하여 은닉 정보를 추출할 수 있는 것이면 제한되지 않는다. 이때 첫번째 행렬과 두번째 행렬은 정해진 규칙에 따라 설정될 수 있는 것으로, 블록 순서대로 정해지지 않을 수 있다.

[0077] 다른 블록에 대하여도 특이값을 추출하여 은닉 정보를 추출할 수 있고(S740) 추출된 은닉 정보를 이용하여 문자 정보 또는 영상 정보를 얻을 수 있다(S750).

[0078] QIM(Quantized Index Modulation) 및 기존의 특이값 분해를 이용한 알고리즘은 값 자체에 기반한 정보 은닉 기술이므로, 스테고 이미지(Stego image), 즉 은닉 정보가 삽입된 데이터에 왜곡이 가해질 경우 원본 데이터가 숨겨진 비트에 해당하지 않는 구간 또는 값으로 변경 되어 정보 추출 시에 오류가 발생할 수 있고, 추가적으로 특이값 분해를 이용하는 경우, 은닉된 정보를 추출하기 위해서는 반드시 원본 데이터의 대각 행렬, 은닉된 정보의 유니터리 행렬 및 스케일링 상수가 필요하다.

[0079] 또한 정보가 은닉된 스테고 이미지의 크기가 변경될 경우 은닉 시에 얻어진 행렬과 차원이 맞지 않아 올바른 정보를 추출해 내기가 어렵다. 이미지가 모바일 환경이나 웹 환경을 통해 주로 공유되고 배포된다는 점을 가정하

였을 때, 공유 과정에서 겪게 되는 크기 변화, 필터링, 압축은 이미지 데이터를 변경시킨다.

[0080] 이와 같이 데이터가 변경될 경우 기존의 방식들은 정보의 완벽한 복원을 보장할 수 없다. 또한 특정 집단이 아닌 불특정 다수의 개인이 모바일 서비스를 이용하기 때문에 스테고 이미지만으로 은닉된 정보의 복원이 가능한 알고리즘이 아니라면 실효성을 갖기 힘들다.

[0081] 본 발명의 일 실시 예에 따르면, 특이값 분해를 이용하여 QIM(Quantized Index Modulation)이 적용된 기술 또는 특이값에 대해 가법적인(additive) 과정을 통해 정보를 은닉한 다른 기술과 성능을 비교했을 때 더 높은 신뢰도의 정보 추출율을 보장할 수 있다. 이는 특이값이 왜곡에 대해 안정적인 특성을 갖고 있고, 본 발명의 알고리즘은 특정한 값이나 구간을 이용한 알고리즘이 아니라 특이값의 대소 관계를 이용한 상대적인 정보 은닉 기술이기 때문에 기존의 기술보다 더 높은 오차 허용 범위를 가질 수 있다.

[0082] 또한 본 발명은 기존의 워터마킹과 달리 이미지가 아닌 문자 정보를 은닉할 수 있다는 점에서 은닉할 수 있는 정보의 내용과 그 분량이 유동적으로 조절이 가능하고 하나의 데이터에 다른 정보를 삽입함으로써 서로 다른 이종신호의 동시 전송이 가능하다.

[0083] 본 발명은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터(정보 처리 기능을 갖는 장치를 모두 포함한다)가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광데이터 저장 장치 등이 있다.

[0084] 비록 상기 설명이 다양한 실시예들에 적용되는 본 발명의 신규한 특징들에 초점을 맞추어 설명되었지만, 본 기술 분야에 숙달된 기술을 가진 사람은 본 발명의 범위를 벗어나지 않으면서도 상기 설명된 장치 및 방법의 형태 및 세부 사항에서 다양한 삭제, 대체, 및 변경이 가능함을 이해할 것이다. 따라서, 본 발명의 범위는 상기 설명에서보다는 첨부된 특허청구범위에 의해 정의된다. 특허청구범위의 균등 범위 안의 모든 변형은 본 발명의 범위에 포섭된다.

부호의 설명

[0085] 200, 300: 정보 삽입 장치 210, 310: 저장부

311: 원본 데이터 220, 320: 제어부

321: 블록 분할 모듈 322: 특이값 추출 모듈

323: 특이값 획득 모듈 324: 데이터 갱신 모듈

330: 입력부 340: 출력부

350: 통신부 400, 500: 정보 추출 장치

410, 510: 저장부 511: 변조된 데이터

420, 520: 제어부 521: 블록 분할 모듈

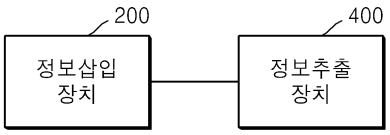
522: 특이값 추출 모듈 523: 정보 추출 모듈

530: 입력부 540: 출력부

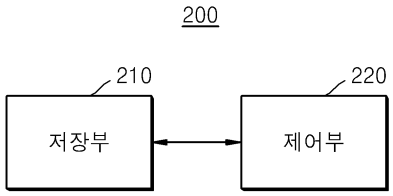
550: 통신부

도면

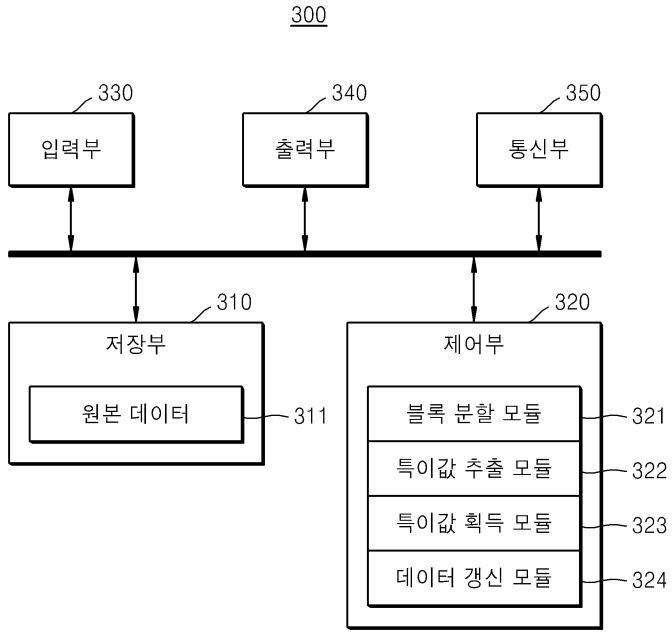
도면1



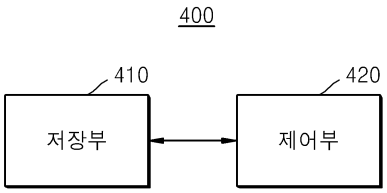
도면2


200
210
저장부
220
제어부

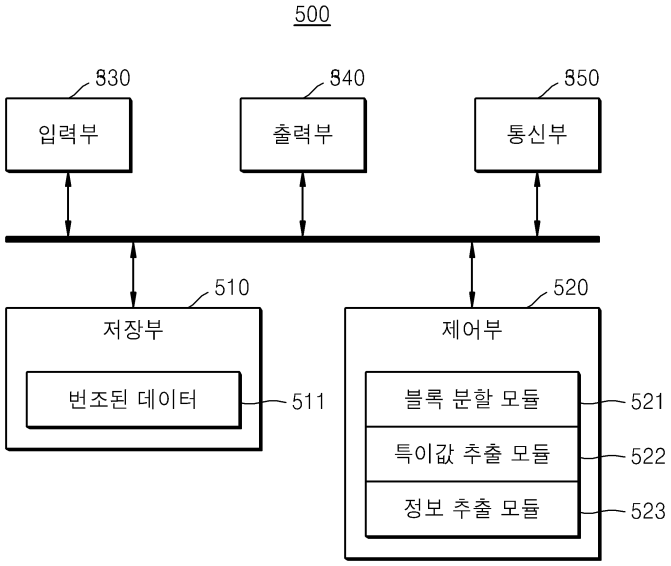
도면3


300
330
입력부
340
출력부
350
통신부
310
저장부
원본 데이터
311
320
제어부
블록 분할 모듈
321
특이값 추출 모듈
322
특이값 획득 모듈
323
데이터 갱신 모듈
324

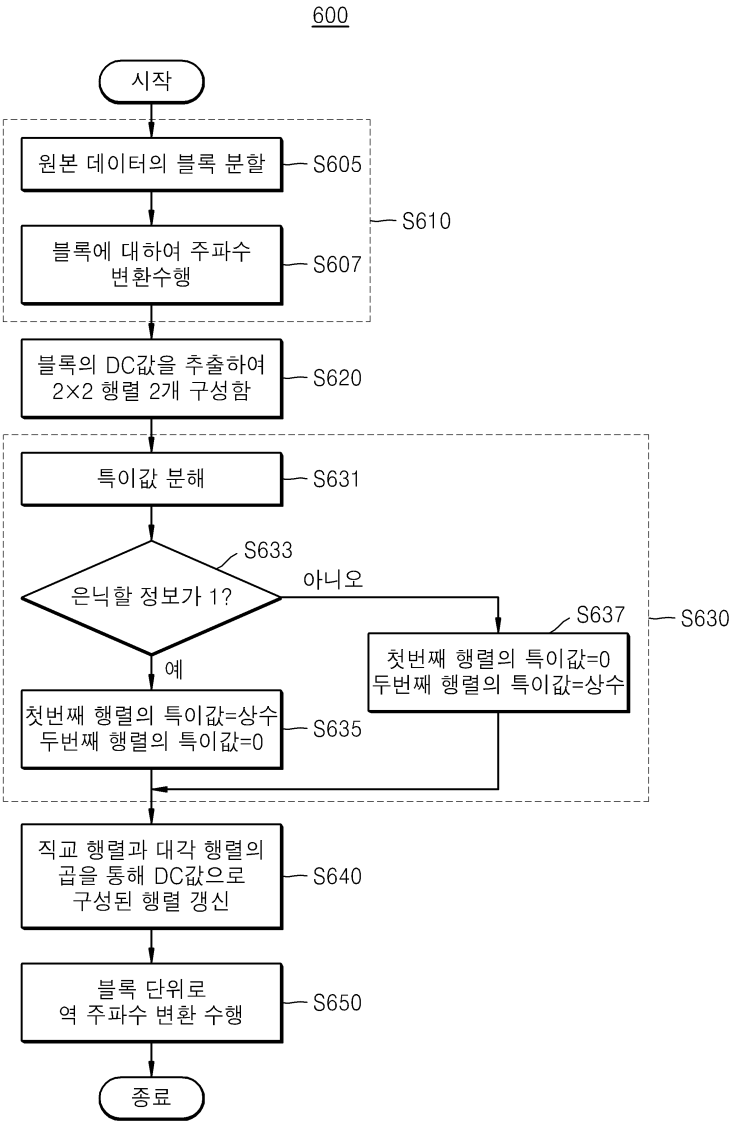
도면4


400
410
저장부
420
제어부

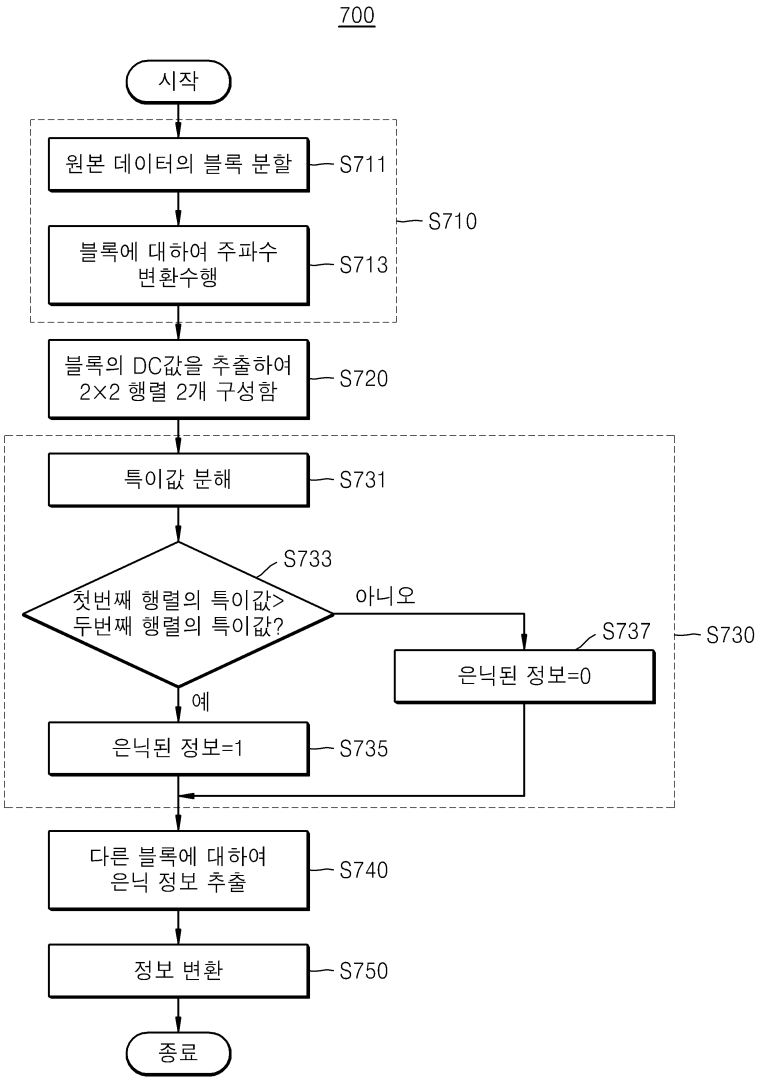
도면5


500
530
입력부
540
출력부
550
통신부
510
저장부
번조된 데이터
511
520
제어부
블록 분할 모듈
521
특이값 추출 모듈
522
정보 추출 모듈
523

도면6

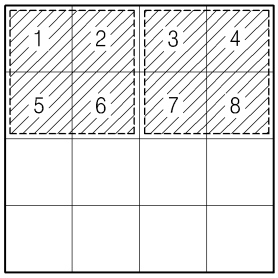

600
시작
원본 데이터의 블록 분할
S605
블록에 대하여 주파수 변환수행
S607
S610
블록의 DC값을 추출하여 2×2 행렬 2개 구성함
S620
특이값 분해
S631
S633
은닉할 정보가 1?
아니오
예
S637
첫번째 행렬의 특이값=0 두번째 행렬의 특이값=상수
첫번째 행렬의 특이값=상수 두번째 행렬의 특이값=0
S635
S630
직교 행렬과 대각 행렬의 곱을 통해 DC값으로 구성된 행렬 갱신
S640
블록 단위로 역 주파수 변환 수행
S650
종료

도면7


700
시작
원본 데이터의 블록 분할
S711
블록에 대하여 주파수 변환수행
S713
S710
블록의 DC값을 추출하여 2×2 행렬 2개 구성함
S720
특이값 분해
S731
S733
첫번째 행렬의 특이값> 두번째 행렬의 특이값?
아니오
S737
은닉된 정보=0
S730
예
은닉된 정보=1
S735
다른 블록에 대하여 은닉 정보 추출
S740
정보 변환
S750
종료

도면8

(a)



(b)

