(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0135908
(43) 공개일자 2016년11월29일

(51) 국제특허분류(Int. Cl.)
H04N 7/167 (2011.01) *H04N 1/44* (2006.01)
H04N 21/8358 (2011.01) *H04N 5/913* (2006.01)
(52) CPC특허분류
H04N 7/167 (2013.01)
H04N 1/387 (2013.01)
(21) 출원번호 10-2015-0069059
(22) 출원일자 2015년05월18일
심사청구일자 2015년05월18일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김형중
서울특별시 서초구 신반포로 270 117동 2601호 (반포동,반포자이아파트)
(74) 대리인
김등용, 김홍석

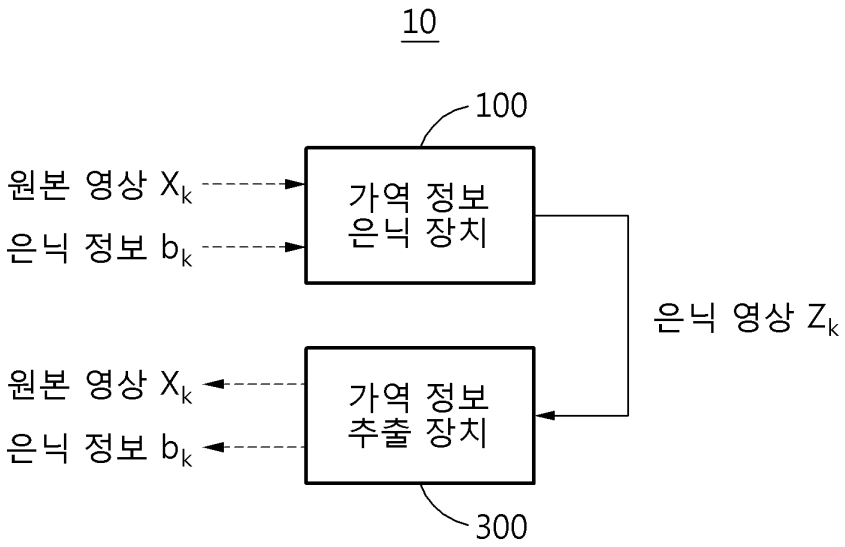
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 **가역 정보 은닉 장치 및 방법과 가역 정보 추출 장치 및 방법**

(57) 요 약

가역 정보 은닉 방법이 개시된다. 상기 가역 정보 은닉 방법은 가역 정보 은닉 장치에서 수행되는 가역 정보 은닉 방법으로서, 소정의 압축 기법을 이용하여 원본 영상 파일을 압축하여 압축 영상 파일을 생성하는 단계, 상기 압축 영상 파일에 포함된 비트 스트림을 미리 정해진 길이를 갖는 분할된 비트 블럭으로 분할하는 단계, 상기 분할된 비트 블럭에 포함된 비트들 중 적어도 일부의 비트의 값을 반전시켜 반전된 비트 블럭을 생성하는 단계, 상기 반전된 비트 블럭의 디코딩 성공 여부를 기초로 상기 분할된 비트 블럭에 은닉 정보를 은닉할지 여부를 결정하는 단계, 및 은닉 여부와 상기 은닉 정보에 따라 상기 분할된 비트 블럭 또는 상기 반전된 비트 블럭을 은닉된 비트 블럭으로 출력하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04N 1/448 (2013.01)
H04N 21/8358 (2013.01)
H04N 5/913 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 10050653
부처명 국가기술표준원
연구관리전문기관 한국산업기술평가관리원
연구사업명 국가표준기술력향상사업
연구과제명 영상 무결성 정보 은닉기술 표준화 연구개발
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2014.10.08 ~ 2016.10.07

명 세 서

청구범위

청구항 1

가역 정보 은닉 장치에서 수행되는 가역 정보 은닉 방법에 있어서,

소정의 압축 기법을 이용하여 원본 영상 파일을 압축하여 압축 영상 파일을 생성하는 단계;

상기 압축 영상 파일에 포함된 비트 스트림을 미리 정해진 길이를 갖는 비트 블럭으로 분할하는 단계;

분할된 비트 블럭에 포함된 비트들 중 적어도 일부의 비트의 값을 반전시켜 반전된 비트 블럭을 생성하는 단계;

상기 반전된 비트 블럭의 디코딩 성공 여부를 기초로 상기 분할된 비트 블럭에 은닉 정보를 은닉할지 여부를 결정하는 단계; 및

은닉 여부와 상기 은닉 정보에 따라 상기 분할된 비트 블럭 또는 상기 반전된 비트 블럭을 은닉된 비트 블럭으로 출력하는 단계를 포함하는,

가역 정보 은닉 방법.

청구항 2

제1항에 있어서,

상기 은닉할지 여부를 결정하는 단계는,

상기 반전된 비트 블럭에 대한 디코딩을 수행하는 단계; 및

상기 반전된 비트 블럭에 대한 디코딩이 성공적으로 수행되지 않은 경우 상기 분할된 비트 블럭에 상기 은닉 정보를 은닉하기로 결정하는 단계를 포함하는,

가역 정보 은닉 방법.

청구항 3

제1항에 있어서,

상기 은닉할지 여부를 결정하는 단계는,

상기 반전된 비트 블럭에 대한 디코딩을 수행하는 단계;

상기 반전된 비트 블럭에 대한 디코딩이 성공적으로 수행된 경우, 디코딩의 결과로부터 추출되는 픽셀값들이 미리 정해진 범위를 초과하는지 여부를 결정하는 단계; 및

상기 미리 정해진 범위를 초과하는 픽셀값이 적어도 하나 존재하는 경우 상기 분할된 비트 블럭에 상기 은닉 정보를 은닉하기로 결정하는 단계를 포함하는,

가역 정보 은닉 방법.

청구항 4

소정의 압축 기법을 이용하여 원본 영상 파일을 압축하여 압축 영상 파일을 생성하는 영상 압축부;

상기 압축 영상 파일에 포함된 비트 스트림을 미리 정해진 길이를 갖는 비트 블럭으로 분할하는 비트 블럭 분할부;

분할된 비트 블럭에 포함된 비트들 중 적어도 일부의 비트의 값을 반전시켜 반전된 비트 블럭을 생성하는 비트 블럭 반전부;

상기 반전된 비트 블럭의 디코딩 성공 여부를 기초로 상기 분할된 비트 블럭에 은닉 정보를 은닉할지 여부를 결정하는 은닉 여부 결정부; 및

은닉 여부와 상기 은닉 정보에 따라 상기 분할된 비트 블럭 또는 상기 반전된 비트 블럭을 은닉된 비트 블럭으로 출력하는 정보 은닉부를 포함하는,

가역 정보 은닉 장치.

청구항 5

가역 정보 추출 장치에서 수행되는 가역 정보 추출 방법에 있어서,

은닉된 비트 블럭에 포함된 비트들 중 적어도 일부의 비트의 값을 반전시켜 반전된 비트 블럭을 생성하는 단계;

상기 은닉된 비트 블럭과 상기 반전된 비트 블럭을 디코딩하는 단계;

디코딩 결과를 기초로 상기 은닉된 비트 블럭에 은닉 정보가 은닉되어 있는지 여부를 결정하는 단계; 및

상기 은닉 정보를 상기 은닉된 비트 블럭으로부터 추출하는 단계를 포함하는,

가역 정보 추출 방법.

청구항 6

제5항에 있어서,

상기 은닉 정보가 은닉되어 있는지 여부를 결정하는 단계는,

상기 은닉된 비트 블럭에 대한 디코딩 또는 상기 반전된 비트 블럭에 대한 디코딩 실패한 경우에 상기 은닉 정보가 은닉되어 있는 것으로 결정하는,

가역 정보 추출 방법.

청구항 7

제5항에 있어서,

상기 은닉 정보가 은닉되어 있는지 여부를 결정하는 단계는,

상기 은닉된 비트 블럭에 대한 디코딩이 실패한 경우, 상기 은닉된 비트 블럭에 대한 디코딩이 성공하였으나 상기 은닉된 비트 블럭에 대한 디코딩의 결과로부터 추출된 픽셀값들 중 미리 정해진 범위를 벗어나는 픽셀값이 존재하는 경우, 상기 반전된 비트 블럭에 대한 디코딩이 실패한 경우, 및 상기 반전된 비트 블럭에 대한 디코딩이 성공하였으나 상기 반전된 비트 블럭에 대한 디코딩의 결과로부터 추출된 픽셀값들 중 상기 미리 정해진 범위를 벗어나는 픽셀값이 존재하는 경우에, 상기 은닉 정보가 은닉되어 있는 것으로 결정하는,

가역 정보 추출 방법.

청구항 8

수신된 은닉 영상 파일에 포함된 비트 스트림을 미리 정해진 길이를 갖는 비트 블럭으로 분할하는 은닉 영상 입력부;

상기 비트 블럭에 포함된 비트들 중 적어도 일부의 비트의 값을 반전시켜 반전 비트 블럭을 생성하는 비트 블럭 반전부;

상기 비트 블럭과 상기 반전 비트 블럭에 대한 디코딩을 수행하는 디코딩부; 및

디코딩 결과에 기초하여 상기 비트 블럭으로부터 은닉 정보를 추출하는 은닉 정보 추출부를 포함하는,

가역 정보 추출 장치.

청구항 9

가역 정보 은닉 장치에서 수행되는 가역 정보 은닉 방법에 있어서,

소정의 압축 기법을 이용하여 원본 영상 파일을 압축하여 압축 영상 파일을 생성하는 단계;

소정의 암호화 기법을 이용하여 상기 압축 영상 파일을 암호화하여 암호화 파일을 생성하는 단계;

상기 암호화 파일에 포함된 비트 스트림을 미리 정해진 길이를 갖는 비트 블럭으로 분할하는 단계;

분할된 비트 블럭에 포함된 비트들 중 적어도 일부의 비트의 값을 반전시켜 반전된 비트 블럭을 생성하는 단계;

상기 반전된 비트 블럭의 복호화 성공 여부를 기초로 상기 분할된 비트 블럭에 은닉 정보를 은닉할지 여부를 결정하는 단계; 및

은닉 여부와 상기 은닉 정보에 따라 상기 분할된 비트 블럭 또는 상기 반전된 비트 블럭을 은닉된 비트 블럭으로 출력하는 단계를 포함하는,

가역 정보 은닉 방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 가역 정보 은닉 장치 및 방법과 가역 정보 추출 장치 및 방법에 관한 것으로, 특히 비트 블럭에 대한 디코딩 성공 여부에 따라 은닉 정보를 은닉하고 추출할 수 있는 가역 정보 은닉 장치 및 방법과 가역 정보 추출 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 많은 정보들이 디지털 형태로 저장됨에 따라, 쉽게 복사되거나 변경될 수 있는 디지털 매체를 보호하기 위하여 여러 가지 정보 보호 기법들이 개발되고 있다.

[0003] 그 중 정보 은닉(information hiding) 기법은 암호화와 함께 기밀성을 보장하기 위해 널리 사용되고 있다. 이러한, 정보 은닉 기법은 디지털 매체를 변경함으로써 디지털 매체에 데이터를 삽일할 수 있다.

[0004] 이와 관련하여, 대한민국공개특허 제10-2007-0076130호(발명의 명칭 : 영상 인증을 위한 정보 삽입 및 추출 방법)는 정보의 삽입 및 추출 과정에서 원정보(original data)의 손실이 발생하지 않는 무손실 정보 은닉(losseless data embedding) 방법에 관한 것으로, 이미지를 다수 개의 블록으로 분할하고, 분할된 각 블록을 서브블록으로 분할하고, 분할된 각 서브블록 중 하나의 픽실에 인증 정보를 삽입하되, 서브블록 중 최소 픽셀값을 갖는 픽셀에 인증 정보(이진 정보)를 삽입하는 기술이 개시하고 있다.

[0005] 그러나, 영상을 압축할 경우, 난수 수준의 출력이 생성됨에 따라, 원본 영상이 아닌 압축된 영상에 가역적으로 정보를 은닉하는 것은 용이하지 않다는 한계가 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명이 이루고자 하는 기술적인 과제는 비트 블럭에 대한 디코딩 성공 여부에 따라 은닉 정보를 은닉하고 추출할 수 있는 가역 정보 은닉 장치 및 방법과 가역 정보 추출 장치 및 방법을 제공하는 것이다.

과제의 해결 수단

[0007] 본 발명의 실시 예에 따른 가역 정보 은닉 방법은 가역 정보 은닉 장치에서 수행되는 가역 정보 은닉 방법으로서, 소정의 압축 기법을 이용하여 원본 영상 파일을 압축하여 압축 영상 파일을 생성하는 단계, 상기 압축 영상 파일에 포함된 비트 스트림을 미리 정해진 길이를 갖는 비트 블럭으로 분할하는 단계, 분할된 비트 블럭에 포함된 비트들 중 적어도 일부의 비트의 값을 반전시켜 반전된 비트 블럭을 생성하는 단계, 상기 반전된 비트 블럭의 디코딩 성공 여부를 기초로 상기 분할된 비트 블럭에 은닉 정보를 은닉할지 여부를 결정하는 단계, 및 은닉 여부와 상기 은닉 정보에 따라 상기 분할된 비트 블럭 또는 상기 반전된 비트 블럭을 은닉된 비트 블럭으로 출력하는 단계를 포함한다.

[0008] 또한, 본 발명의 실시 예에 따른 가역 정보 은닉 장치는 소정의 압축 기법을 이용하여 원본 영상 파일을 압축하여 압축 영상 파일을 생성하는 영상 압축부, 상기 압축 영상 파일에 포함된 비트 스트림을 미리 정해진 길이를 갖는 비트 블럭으로 분할하는 비트 블럭 분할부, 상기 분할된 비트 블럭에 포함된 비트들 중 적어도 일부의 비

트의 값을 반전시켜 반전된 비트 블럭을 생성하는 비트 블럭 반전부, 상기 반전된 비트 블럭의 디코딩 성공 여부를 기초로 상기 분할된 비트 블럭에 은닉 정보를 은닉할지 여부를 결정하는 은닉 여부 결정부, 및 은닉 여부와 상기 은닉 정보에 따라 상기 분할된 비트 블럭 또는 상기 반전된 비트 블럭을 은닉된 비트 블럭으로 출력하는 정보 은닉부를 포함한다.

[0009] 또한, 본 발명의 실시 예에 따른 가역 정보 추출 방법은, 가역 정보 추출 장치에서 수행되는 가역 정보 추출 방법으로서, 은닉된 비트 블럭에 포함된 비트들 중 적어도 일부의 비트의 값을 반전시켜 반전된 비트 블럭을 생성하는 단계, 상기 은닉된 비트 블럭과 상기 반전된 비트 블럭을 디코딩하는 단계, 디코딩 결과를 기초로 상기 은닉된 비트 블럭에 은닉 정보가 은닉되어 있는지 여부를 결정하는 단계, 및 상기 은닉 정보를 상기 은닉된 비트 블럭으로부터 추출하는 단계를 포함한다.

[0010] 또한, 본 발명의 실시 예에 따른 가역 정보 추출 장치는 수신된 은닉 영상 파일에 포함된 비트 스트림을 미리 정해진 길이를 갖는 비트 블럭으로 분할하는 은닉 영상 입력부, 상기 비트 블럭에 포함된 비트들 중 적어도 일부의 비트의 값을 반전시켜 반전 비트 블럭을 생성하는 비트 블럭 반전부, 상기 비트 블럭과 상기 반전 비트 블럭에 대한 디코딩을 수행하는 디코딩부, 및 디코딩 결과에 기초하여 상기 비트 블럭으로부터 은닉 정보를 추출하는 은닉 정보 추출부를 포함한다.

[0011] 또한, 본 발명의 다른 실시 예에 따른 가역 정보 은닉 방법은, 가역 정보 은닉 장치에서 수행되는 가역 정보 은닉 방법으로서, 소정의 압축 기법을 이용하여 원본 영상 파일을 압축하여 압축 영상 파일을 생성하는 단계, 소정의 암호화 기법을 이용하여 상기 압축 영상 파일을 암호화하여 암호화 파일을 생성하는 단계, 상기 암호화 파일에 포함된 비트 스트림을 미리 정해진 길이를 갖는 비트 블럭으로 분할하는 단계, 분할된 비트 블럭에 포함된 비트들 중 적어도 일부의 비트의 값을 반전시켜 반전된 비트 블럭을 생성하는 단계, 상기 반전된 비트 블럭의 복호화 성공 여부를 기초로 상기 분할된 비트 블럭에 은닉 정보를 은닉할지 여부를 결정하는 단계, 및 은닉 여부와 상기 은닉 정보에 따라 상기 분할된 비트 블럭 또는 상기 반전된 비트 블럭을 은닉된 비트 블럭으로 출력하는 단계를 포함한다.

발명의 효과

[0012] 본 발명의 실시 예에 따른 가역 정보 은닉 장치 및 방법과 가역 정보 추출 장치 및 방법에 의할 경우, 영상 파일에 추가적인 은닉 정보를 가역적으로 은닉하거나 수신된 영상 파일에 은닉된 은닉 정보를 추출할 수 있다.

도면의 간단한 설명

[0013] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 따른 가역 정보 은닉 시스템을 도시한다.

도 2는 도 1에 도시된 가역 정보 은닉 장치의 기능 블럭도이다.

도 3은 본 발명의 일 실시 예에 따른 압축 영상 파일의 비트스트림 구조를 설명하기 위한 도면이다.

도 4는 도 1에 도시된 가역 정보 추출 장치의 기능 블럭도이다.

도 5는 도 4에 도시된 은닉 정보 추출부에 의한 은닉 정보 추출 과정을 설명하기 위한 흐름도이다.

도 6은 도 4에 도시된 은닉 정보 추출부에 의한 은닉 정보 추출 과정의 다른 실시 예를 설명하기 위한 흐름도이다.

도 7은 도 1에 도시된 가역 정보 은닉 장치의 다른 실시 예를 도시한다.

도 8은 도 1에 도시된 가역 정보 추출 장치의 다른 실시 예를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0014] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0015] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시

예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0016] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0017] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0018] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0019] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0020] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0021] 도 1은 본 발명의 일 실시 예에 따른 가역 정보 은닉 시스템을 도시한다.

[0022] 도 1을 참조하면, 가역 정보 은닉 시스템(10)은 가역 정보 은닉 장치(100)와 가역 정보 추출 장치(300)를 포함한다.

[0023] 가역 정보 은닉 장치(100)는 원본 영상 파일의 비트 스트림(X_k)을 기설정된 압축 포맷으로 상기 원본 영상을 압축하여 압축 영상 파일을 생성한다. 또한, 가역 정보 은닉 장치(100)는 생성된 압축 영상 파일의 비트 스트림에 은닉 정보(b_k)를 은닉시킨 후 정보 은닉 영상 파일을 생성한다. 생성된 은닉 영상 파일의 비트 스트림(Z_k)은 가역 정보 은닉 장치(100)에 의해 출력될 수 있다.

[0024] 가역 정보 추출 장치(300)는 가역 정보 은닉 장치(100)로부터 제공된 은닉 영상 파일의 비트 스트림(Z_k)을 입력받아, 비트 스트림(Z_k)으로부터 은닉 정보(b_k)를 추출하고 원본 영상 파일을 획득한다.

[0025] 가역 정보 은닉 시스템(10)을 구성하는 가역 정보 은닉 장치(100)와 가역 정보 추출 장치(300)는 물리적으로 하나의 장치로 구현될 수 있으며, 실시 예에 따라서는 별도의 물리적인 장치를 의미할 수 있다. 또한, 은닉 영상 파일은 유·무선 통신망을 통하여 가역 정보 은닉 장치(100)로부터 가역 정보 추출 장치(300)로 송신될 수 있으며, 실시 예에 따라서는 휴대용 저장 장치 등을 통하여 가역 정보 은닉 장치(100)로부터 가역 정보 추출 장치(300)로 전달될 수 있다.

[0026] 또한, 가역 정보 은닉 장치(100) 및/또는 가역 정보 추출 장치(300)는 PC(personal computer), 태블릿 PC, 노트북(notebook), 넷-북(net-book), e-리더(e-reader), PDA(personal digital assistant), PMP(portable multimedia player), MP3 플레이어, 또는 MP4 플레이어와 같은 데이터 처리 장치나 모바일폰(mobile phone), 스마트폰(smart phone)과 같은 핸드헬드 장치(handheld device)로 구현될 수 있다.

[0027] 도 2는 도 1에 도시된 가역 정보 은닉 장치의 기능 블럭도이다.

[0028] 도 1과 도 2를 참조하면, 가역 정보 은닉 장치(100)는 영상 압축부(110), 비트 블럭 분할부(130), 비트 블럭 반전부(150), 은닉 여부 결정부(170), 및 정보 은닉부(190)를 포함한다.

[0029] 영상 압축부(110)는 알려져 있는 임의의 영상 압축 기법, 예컨대 MPEG, JPEG, AVI, H.263, H.264 등 다양한 압축 포맷의 압축 기법(인코딩 기법) 또는 앞으로 예상되는 임의의 영상 압축 기법을 이용하여 원본 영상을 압축하여 압축 영상 파일을 생성할 수 있다.

[0030] 비트 블럭 분할부(130)는 영상 압축부(110)에 의해 압축된 압축 영상 파일의 비트 스트림을 미리 정해진 길이(L 비트, L은 2 이상의 자연수)를 갖는 복수의 비트 블럭들로 분할한다. 비트 블럭 분할부(130)의 구체적인 동작은 도 3을 통하여 설명하기로 한다.

[0031] 비트 블럭 반전부(150)는 비트 블럭 분할부(130)로부터 출력된 비트 블럭(Y_k)에 포함된 비트들 중 적어도 일부의 비트의 값을 반전시킬 수 있다. 즉, 비트 블럭 반전부(150)는 비트 블럭(Y_k)에 포함된 비트들 전부의 값을 반전시키거나 일부의 비트의 값을 반전시킬 수 있다. 비트의 값을 반전시킨다는 것은 반전시킬 대상 비트의 값이 "1"인 경우 "0"으로 변환시키고, 반전시킬 대상 비트의 값이 "0"인 경우 "1"로 변환시킴을 의미할 수 있다. 비트 블럭 반전부(150)는 반전된 비트 블럭($\overline{Y_k}$)을 출력할 수 있다.

[0032] 은닉 여부 결정부(170)는 비트 블럭 반전부(150)로부터 반전된 비트 블럭($\overline{Y_k}$)을 수신하고, 비트 블럭(Y_k)에 은닉 정보(b_k)를 은닉할지 여부를 결정하고, 은닉 여부에 대한 정보를 출력한다.

[0033] 즉, 은닉 여부 결정부(170)는 반전된 비트 블럭($\overline{Y_k}$)을 대상으로 미리 디코딩 동작을 수행하고, 디코딩 성공 여부에 따라 비트 블럭(Y_k)에 은닉 정보(b_k)를 은닉할지 여부를 결정한다. 구체적으로 은닉 여부 결정부(170)는 반전된 비트 블럭($\overline{Y_k}$)이 성공적으로 디코딩된 경우 비트 블럭(Y_k)에 은닉 정보(b_k)를 은닉하지 않기로 결정한다. 또한, 은닉 여부 결정부(170)는 반전된 비트 블럭($\overline{Y_k}$)이 성공적으로 디코딩되지 못한 경우 비트 블럭(Y_k)에 은닉 정보(b_k)를 은닉하기로 결정한다.

[0034] 다른 실시 예로, 은닉 여부 결정부(170)는 반전된 비트 블럭($\overline{Y_k}$)을 대상으로 미리 디코딩 동작을 수행하고, 디코딩 성공 여부와 디코딩의 결과로 추출되는 픽셀값들의 범위에 기초하여 비트 블럭(Y_k)에 은닉 정보(b_k)를 은닉할지 여부를 결정할 수 있다. 구체적으로 은닉 여부 결정부(170)는 반전된 비트 블럭($\overline{Y_k}$)이 성공적으로 디코딩되지 못한 경우 비트 블럭(Y_k)에 은닉 정보(b_k)를 은닉하기로 결정한다. 또한, 은닉 여부 결정부(170)는 반전된 비트 블럭($\overline{Y_k}$)이 성공적으로 디코딩된 경우에는 추가적으로 디코딩 결과로 추출된 픽셀값들의 범위를 고려하여 은닉 여부를 결정한다. 즉, 디코딩 결과로 추출된 픽셀값들 중 미리 정해진 범위를 벗어나는 픽셀값이 존재하는 경우 은닉 여부 결정부(170)는 은닉 정보(b_k)를 은닉하기로 결정하고, 미리 정해진 범위를 벗어나는 픽셀값이 존재하지 않는 경우 은닉 여부 결정부(170)는 은닉 정보(b_k)를 은닉하지 않기로 결정한다.

[0035] 은닉 여부 결정부(170)가 추가적으로 픽셀값을 고려하여 은닉 여부를 결정하는 이유는 다음과 같다. 영상이 8비트로 양자화되었다고 가정할 경우, 영상의 픽셀값들은 0과 255 사이의 값([0,255])을 가지게 된다. 따라서, 은닉 여부 결정부(170)에 의해 추출된 픽셀 값들이 미리 정해진 범위(예컨대, [0,255])를 벗어난 경우에는 디코딩이 실패한 경우와 마찬가지로 은닉 정보(b_k)를 은닉하기로 결정한다.

[0036] 정보 은닉부(190)은 은닉 여부 결정부(170)으로부터 출력된 은닉 여부에 관한 정보에 기초하여 비트 블럭(Y_k)에 은닉 정보(b_k)를 은닉하고, 은닉된 비트 블럭(Z_k)을 출력할 수 있다.

[0037] 구체적으로, 은닉 여부 결정부(170)가 은닉 정보를 은닉하지 않기로 결정한 경우, 정보 은닉부(190)는 비트 블

력 분할부(130)로부터 수신된 비트 블럭(Y_k)을 출력한다(즉, $Z_k=Y_k$).

[0038] 은닉 여부 결정부(170)가 은닉 정보를 은닉하기로 결정한 경우, 정보 은닉부(190)는 비트 블럭(Y_k)과 반전된 비트 블럭($\overline{Y_k}$) 중 어느 하나를 은닉된 비트 블럭(Z_k)으로 출력한다(즉, $Z_k = Y_k$ 또는 $Z = \overline{Y_k}$). 구체적으로, 은닉 정보(b_k)가 "0"과 "1" 중 어느 하나(예컨대, "0")인 경우 정보 은닉부(190)는 비트 블럭(Y_k)을 은닉된 비트 블럭(Z_k)으로 출력한다(즉, $Z_k = Y_k$). 은닉 정보(b_k)가 "0"과 "1" 중 다른 하나(예컨대, "1")인 경우 정보 은닉부(190)는 반전된 비트 블럭($\overline{Y_k}$)을 은닉된 비트 블럭(Z_k)으로 출력한다(즉, $Z = \overline{Y_k}$).

[0039] 상기에서는 은닉 정보(b_k)가 하나의 비트로 표현되는 정보인 경우를 예로 설명하였으나, 은닉 정보(b_k)는 2 이상의 비트로 표현되는 정보일 수도 있다.

[0040] 도 3은 본 발명의 일 실시 예에 따른 압축 영상 파일의 비트스트림 구조를 설명하기 위한 도면이다.

[0041] 도 3을 참조하면, 압축 영상 파일의 비트 스트림은 헤더 및 페이로드로 구성되며, 비트 블럭 분할부(130)는 압축 영상 파일의 비트 스트림 중 헤더를 제외한 페이로드의 비트 스트림을 기설정된 길이(L비트) 단위로 분할하여 n(n은 1 이상의 자연수) 개의 비트 블럭들(Y_k, k는 1보다 크거나 같고 n보다 작거나 같은 자연수)로 분할할 수 있다. 이때, 마지막 비트 블럭(Y_n)의 길이는 M비트(M은 1보다 크거나 같고 n보다 작거나 같은 자연수)로, M의 값이 n보다 작은 경우 비트 블럭(Y_n)은 은닉 대상 비트 블럭에서 제외될 수 있다.

[0042] 도 4는 도 1에 도시된 가역 정보 추출 장치의 기능 블럭도이다.

[0043] 도 4를 참조하면, 가역 정보 추출 장치(300)는 은닉 영상 입력부(310), 비트 블럭 반전부(330), 디코딩부(350), 및 은닉 정보 추출부(370)를 포함한다.

[0044] 은닉 영상 입력부(310)는 가역 정보 은닉 장치(100)로부터 또는 소정의 입력 장치로부터 은닉 영상 파일 또는 은닉 영상 파일의 비트 스트림(Z_k)을 수신할 수 있다. 실시 예에 따라, 은닉 영상 입력부(310)는 가역 정보 은닉 장치(100)로부터 은닉 영상 파일을 수신하고, 수신된 은닉 영상 파일의 비트 스트림을 미리 결정된 길이(예컨대, L비트)를 갖는 복수의 비트 블럭들로 분할 한 후 상기 복수의 비트 블럭들 각각을 출력할 수 있다.

[0045] 비트 블럭 반전부(330)는 은닉 영상 입력부(310)로부터 비트 스트림(Z_k)을 수신하고, 비트 스트림(Z_k)에 포함된 비트들 중 적어도 일부의 값을 반전시킨 후 반전된 비트 블럭($\overline{Z}_k$)을 출력할 수 있다. 이때, 상기 적어도 일부는 가역 정보 은닉 장치(100)의 비트 블럭 반전부(150)에 의해 값이 반전된 비트들을 의미할 수 있다.

[0046] 디코딩부(350)는 은닉 영상 입력부(310)로부터 출력된 비트 스트림(Z_k) 및/또는 비트 블럭 반전부(330)로부터 출력된 반전된 비트 스트림($\overline{Z}_k$)을 디코딩할 수 있다. 디코딩 동작의 성공 여부와 디코딩 결과는 디코딩부(350)에 의해 은닉 정보 추출부(370)로 출력될 수 있다.

[0047] 은닉 정보 추출부(370)는 비트 스트림(Z_k)에 은닉 정보(b_k)가 은닉되었는지 여부, 즉 은닉 여부를 결정하고, 은닉된 은닉 정보(b_k)를 비트 스트림(Z_k)으로부터 추출할 수 있다.

[0048] 구체적으로, 은닉 정보 추출부(370)는 다음과 같이 3가지 경우에 따라 은닉 여부를 결정하고 은닉 정보(b_k)를 추출할 수 있다.

[0049] 첫째, 비트 스트림(Z_k)에 대한 디코딩이 실패한 경우, 은닉 정보 추출부(370)는 "0"과 "1" 중 어느 하나(예컨대, "1")을 은닉 정보(b_k)로 추출할 수 있다. 이 경우 반전된 비트 스트림($\overline{Z}_k$)을 디코딩함으로써 원

본 영상을 획득할 수 있다.

[0050] 둘째, 비트 스트림(Z_k)에 대한 디코딩은 성공하였으나 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩이 실패한 경우, 은닉 정보 추출부(370)는 "0"과 "1" 중 다른 하나(예컨대, "0")을 은닉 정보(b_k)로 추출할 수 있다. 이 경우 비트 스트림(Z_k)을 디코딩함으로써 원본 영상을 획득할 수 있다.

[0051] 셋째, 비트 스트림(Z_k)에 대한 디코딩과 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩이 모두 성공한 경우, 은닉 정보 추출부(370)는 비트 스트림(Z_k)에 은닉 정보(b_k)가 은닉되어 있지 않은 것으로 결정할 수 있다. 이 경우 비트 스트림(Z_k)을 디코딩함으로써 원본 영상을 획득할 수 있다.

[0052] 다른 실시 예로, 은닉 정보 추출부(370)은 다음과 같이 5 가지의 경우에 따라 은닉 여부를 결정하고 은닉 정보(b_k)를 추출할 수 있다.

[0053] 첫째, 비트 스트림(Z_k)에 대한 디코딩이 실패한 경우, 은닉 정보 추출부(370)는 "1"을 은닉 정보(b_k)로 추출할 수 있다. 이 경우 반전된 비트 스트림($\bar{Z}_k$)을 디코딩함으로써 원본 영상을 획득할 수 있다.

[0054] 둘째, 비트 스트림(Z_k)에 대한 디코딩이 성공하였으나 디코딩 결과로부터 추출된 픽셀값들 중 미리 정해진 범위를 벗어나는 픽셀값이 존재하는 경우, 은닉 정보 추출부(370)는 "1"을 은닉 정보(b_k)로 추출할 수 있다. 이 경우 반전된 비트 스트림($\bar{Z}_k$)을 디코딩함으로써 원본 영상을 획득할 수 있다.

[0055] 셋째, 비트 스트림(Z_k)에 대한 디코딩이 성공되었고 디코딩 결과로부터 추출된 픽셀값들이 모두 미리 정해진 범위 내이며 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩이 실패한 경우, 은닉 정보 추출부(370)는 "0"을 은닉 정보(b_k)로 추출할 수 있다. 이 경우 비트 스트림(Z_k)을 디코딩함으로써 원본 영상을 획득할 수 있다.

[0056] 넷째, 비트 스트림(Z_k)에 대한 디코딩이 성공되었고 비트 스트림(Z_k)에 대한 디코딩 결과로부터 추출된 픽셀값들이 모두 미리 정해진 범위 내이며 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩이 성공되었고, 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩 결과로부터 추출된 픽셀값들 중 미리 정해진 범위를 벗어나는 픽셀값이 존재하는 경우, 은닉 정보 추출부(370)는 "0"을 은닉 정보(b_k)로 추출할 수 있다. 이 경우 비트 스트림(Z_k)을 디코딩함으로써 원본 영상을 획득할 수 있다.

[0057] 다섯째, 비트 스트림(Z_k)에 대한 디코딩과 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩이 모두 성공하였고, 비트 스트림(Z_k)에 대한 디코딩 결과로부터 추출된 픽셀값들과 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩 결과로부터 추출된 픽셀값들이 모두 미리 정해진 범위 내인 경우, 은닉 정보 추출부(370)는 비트 스트림(Z_k)에 은닉 정보(b_k)가 은닉되어 있지 않은 것으로 결정한다. 이 경우 비트 스트림(Z_k)을 디코딩함으로써 원본 영상을 획득할 수 있다.

[0058] 도 5는 도 4에 도시된 은닉 정보 추출부에 의한 은닉 정보 추출 과정을 설명하기 위한 흐름도이다.

[0059] 도 5를 참조하면, 은닉 정보 추출부(370)는 비트 스트림(Z_k)의 디코딩 성공(또는 실패) 여부를 판단한다(S100). 디코딩 성공 여부는 디코딩부(350)로부터 출력되는 디코딩 성공 여부에 대한 정보를 이용하여 판단될 수 있다.

[0060] 비트 스트림(Z_k)에 대한 디코딩이 실패한 경우, 은닉 정보 추출부(370)는 "1"을 은닉 정보(b_k)로 추출하고, 원본 영상을 획득하기 위한 디코딩 대상(Y_k)을 반전된 비트 스트림($\bar{Z}_k$)으로 결정할 수 있다(S200).

[0061] 비트 스트림(Z_k)에 대한 디코딩이 성공한 경우, 은닉 정보 추출부(370)는 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩 성공(또는 실패) 여부를 판단한다(S300).

[0062] 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩이 실패한 경우, 은닉 정보 추출부(370)는 "0"을 은닉 정보(b_k)로 추출하고, 원본 영상을 획득하기 위한 디코딩 대상(Y_k)을 비트 스트림(Z_k)으로 결정할 수 있다(S400).

[0063] 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩이 성공한 경우, 은닉 정보 추출부(370)는 은닉 정보(b_k)가 은닉되어 있지 않은 것으로 결정하고, 원본 영상을 획득하기 위한 디코딩 대상(Y_k)을 비트 스트림(Z_k)으로 결정할 수 있다(S500).

[0064] 도 6은 도 4에 도시된 은닉 정보 추출부에 의한 은닉 정보 추출 과정의 다른 실시 예를 설명하기 위한 흐름도이다.

[0065] 도 6을 참조하면, 은닉 정보 추출부(370)는 비트 스트림(Z_k)의 디코딩 성공 여부를 판단한다(S100).

[0066] 비트 스트림(Z_k)에 대한 디코딩이 실패한 경우, 은닉 정보 추출부(370)는 "1"을 은닉 정보(b_k)로 추출하고, 원본 영상을 획득하기 위한 디코딩 대상(Y_k)을 반전된 비트 스트림($\bar{Z}_k$)으로 결정할 수 있다(S200).

[0067] 비트 스트림(Z_k)에 대한 디코딩이 성공한 경우, 은닉 정보 추출부(370)는 비트 스트림(Z_k)에 대한 디코딩 결과로부터 추출된 픽셀값들 중 미리 정해진 범위를 벗어나는 픽셀이 존재하는지 여부를 결정한다(S210).

[0068] 미리 정해진 범위를 벗어나는 픽셀이 존재하는 경우, 은닉 정보 추출부(370)는 "1"을 은닉 정보(b_k)로 추출하고, 원본 영상을 획득하기 위한 디코딩 대상(Y_k)을 반전된 비트 스트림($\bar{Z}_k$)으로 결정할 수 있다(S230).

[0069] 미리 정해진 범위를 벗어나는 픽셀이 존재하지 않는 경우, 은닉 정보 추출부(370)는 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩 성공 여부를 판단한다(S300).

[0070] 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩이 실패한 경우, 은닉 정보 추출부(370)는 "0"을 은닉 정보(b_k)로 추출하고, 원본 영상을 획득하기 위한 디코딩 대상(Y_k)을 비트 스트림(Z_k)으로 결정할 수 있다(S400).

[0071] 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩이 성공한 경우, 은닉 정보 추출부(370)는 반전된 비트 스트림($\bar{Z}_k$)에 대한 디코딩 결과로부터 추출된 픽셀값들 중 미리 정해진 범위를 벗어나는 픽셀이 존재하는지 여부를 결정한다(S410).

[0072] 미리 정해진 범위를 벗어나는 픽셀이 존재하는 경우, 은닉 정보 추출부(370)는 "0"을 은닉 정보(b_k)로 추출하고, 원본 영상을 획득하기 위한 디코딩 대상(Y_k)을 비트 스트림(Z_k)으로 결정할 수 있다(S430).

[0073] 미리 정해진 범위를 벗어나는 픽셀이 존재하지 않는 경우, 은닉 정보 추출부(370)는 은닉 정보(b_k)가 은닉되어 있지 않은 것으로 결정하고, 원본 영상을 획득하기 위한 디코딩 대상(Y_k)을 비트 스트림(Z_k)으로 결정할 수 있다(S500).

[0074] 도 7은 도 1에 도시된 가역 정보 은닉 장치의 다른 실시 예를 도시한다.

[0075] 도 7을 참조하면, 가역 정보 은닉 장치(101)는 영상 압축부(110), 암호화부(120), 비트 블럭 분할부(130), 비트 블럭 반전부(150), 은닉 여부 결정부(170), 및 정보 은닉부(190)를 포함한다. 가역 정보 은닉 장치(101)의 구조 및 동작에 관한 설명 중 도 2를 통하여 설명된 구조 및 동작에 관한 설명과 중복되는 부분에 관하여는 그 상세한 설명을 생략하기로 한다.

[0076] 암호화부(120)는 영상 압축부(110)로부터 출력된 압축 영상 파일의 비트 스트림을 기존에 알려진 암호화 기법(예컨대, RSA 암호화 기법)을 이용하여 암호화 할 수 있다.

[0077] 비트 블럭 분할부(130)는 암호화부(120)에 의해 암호화된 파일의 비트 스트림을 미리 정해진 길이(L비트)를 갖는 복수의 비트 블럭들로 분할한다.

[0078] 은닉 여부 결정부(170)는 비트 블럭 반전부(150)로부터 반전된 비트 블럭($\bar{Y}_k$)을 수신하고, 비트 블럭(Y_k)에 은닉 정보(b_k)를 은닉할지 여부를 결정하고, 은닉 여부에 대한 정보를 출력한다.

[0079] 즉, 은닉 여부 결정부(170)는 반전된 비트 블럭($\bar{Y}_k$)을 대상으로 미리 복호화 동작을 수행하고, 복호화 성공 여부에 따라 비트 블럭(Y_k)에 은닉 정보(b_k)를 은닉할지 여부를 결정한다. 구체적으로 은닉 여부 결정부(170)는 반전된 비트 블럭($\bar{Y}_k$)이 성공적으로 복호화된 경우 비트 블럭(Y_k)에 은닉 정보(b_k)를 은닉하지 않기로 결정한다. 또한, 은닉 여부 결정부(170)는 반전된 비트 블럭($\bar{Y}_k$)이 성공적으로 복호화되지 못한 경우 비트 블럭(Y_k)에 은닉 정보(b_k)를 은닉하기로 결정한다.

[0080] 실시 예에 따라, 암호화부(120)는 정보 은닉부(190)의 후단에 위치하여, 정보 은닉부(190)로부터 출력된 은닉된 비트 블럭(Z_k)을 암호화하는 동작을 수행할 수도 있다.

[0081] 도 8은 도 1에 도시된 가역 정보 추출 장치의 다른 실시 예를 도시한다.

[0082] 도 8을 참조하면, 가역 정보 추출 장치(301)는 은닉 영상 입력부(310), 비트 블럭 반전부(330), 복호화부(340), 은닉 정보 추출부(370), 및 디코딩부(380)를 포함한다. 가역 정보 추출 장치(301)의 구조 및 기능을 설명함에 있어서 도 4를 통하여 설명된 가역 정보 추출 장치(300)의 구조 및 기능에 대한 설명과 중복되는 내용에 관하여는 구체적인 설명을 생략하기로 한다.

[0083] 복호화부(340)는 은닉 영상 입력부(310)로부터 출력된 비트 스트림(Z_k) 및/또는 비트 블럭 반전부(330)로부터 출력된 반전된 비트 스트림($\bar{Z}_k$)을 복호화할 수 있다. 복호화 동작의 성공 여부와 복호화 결과는 암호화부(340)에 의해 은닉 정보 추출부(370)로 출력될 수 있다.

[0084] 은닉 정보 추출부(370)는 비트 스트림(Z_k)에 은닉 정보(b_k)가 은닉되었는지 여부, 즉 은닉 여부를 결정하고, 은닉된 은닉 정보(b_k)를 비트 스트림(Z_k)으로부터 추출할 수 있다.

[0085] 구체적으로, 은닉 정보 추출부(370)는 다음과 같이 3가지 경우에 따라 은닉 여부를 결정하고 은닉 정보(b_k)를 추출할 수 있다.

[0086] 첫째, 비트 스트림(Z_k)에 대한 복호화가 실패한 경우, 은닉 정보 추출부(370)는 "0"과 "1" 중 어느 하나(예컨대, "1")를 은닉 정보(b_k)로 추출할 수 있다. 이 경우 디코딩부(380)는 반전된 비트 스트림($\bar{Z}_k$)의 복호화 결과를 디코딩함으로써 원본 영상을 획득할 수 있다.

[0087] 둘째, 비트 스트림(Z_k)에 대한 복호화는 성공하였으나 반전된 비트 스트림($\bar{Z}_k$)에 대한 복호화는 실패한 경우, 은닉 정보 추출부(370)는 "0"과 "1" 중 다른 하나(예컨대, "0")을 은닉 정보(b_k)로 추출할 수 있다. 이 경우 디코딩부(380)는 비트 스트림(Z_k)의 복호화 결과를 디코딩함으로써 원본 영상을 획득할 수 있다.

[0088] 셋째, 비트 스트림(Z_k)에 대한 복호화와 반전된 비트 스트림($\bar{Z}_k$)에 대한 복호화가 모두 성공한 경우, 은닉 정보 추출부(370)는 비트 스트림(Z_k)에 은닉 정보(b_k)가 은닉되어 있지 않은 것으로 결정할 수 있다. 이 경우 디코딩부(380)는 비트 스트림(Z_k)의 복호화 결과를 디코딩함으로써 원본 영상을 획득할 수 있다.

[0089] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0090] 10 : 가역 정보 은닉 시스템

100, 101 : 가역 정보 은닉 장치

110 : 영상 압축부

120 : 암호화부

130 : 비트 블럭 분할부

150 : 비트 블럭 반전부

170 : 은닉 여부 결정부

190 : 정보 은닉부

300, 301 : 가역 정보 추출 장치

310 : 은닉 영상 입력부

330 : 비트 블럭 반전부

340 : 복호화부

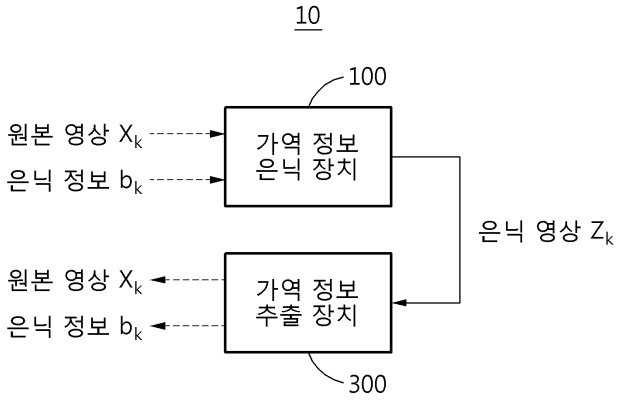
350 : 디코딩부

370 : 은닉 정보 추출부

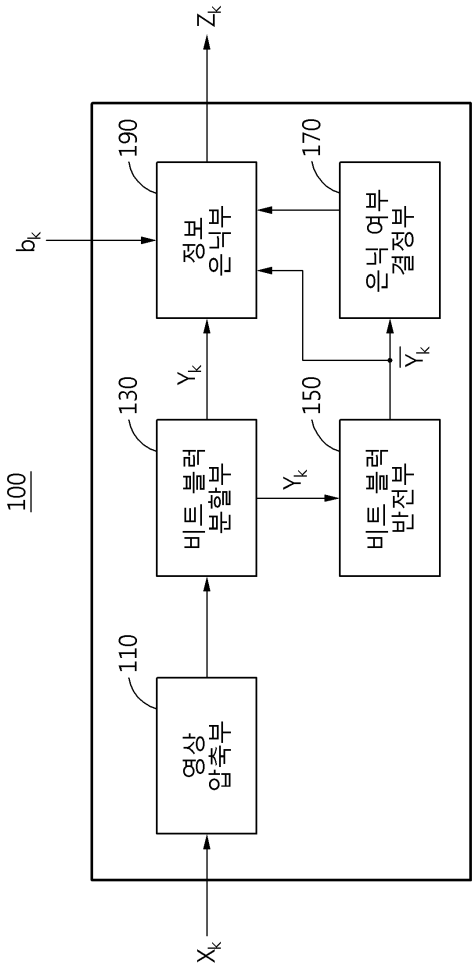
380 : 디코딩부

도면

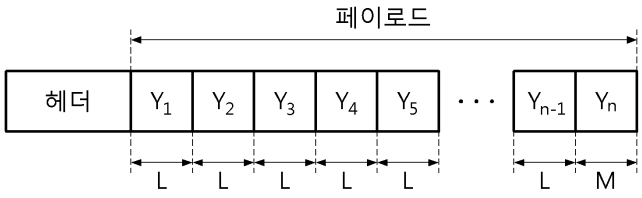
도면1


10
100
원본 영상 X_k
은닉 정보 b_k
가역 정보 은닉 장치
은닉 영상 Z_k
원본 영상 X_k
은닉 정보 b_k
가역 정보 추출 장치
300

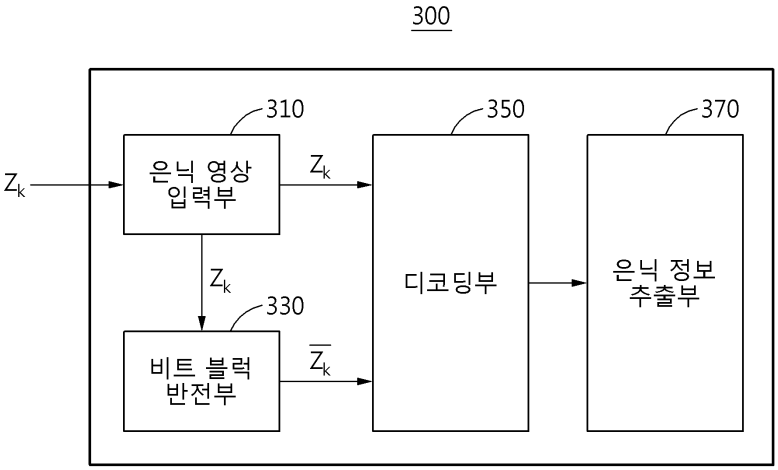
도면2


Z_k
190
170
b_k
정보 은닉부
은닉 여부 결정부
Y_k
$\overline{Y}_k$
130
150
100
비트 블럭 분할부
Y_k
비트 블럭 반전부
110
영상 압축부
X_k

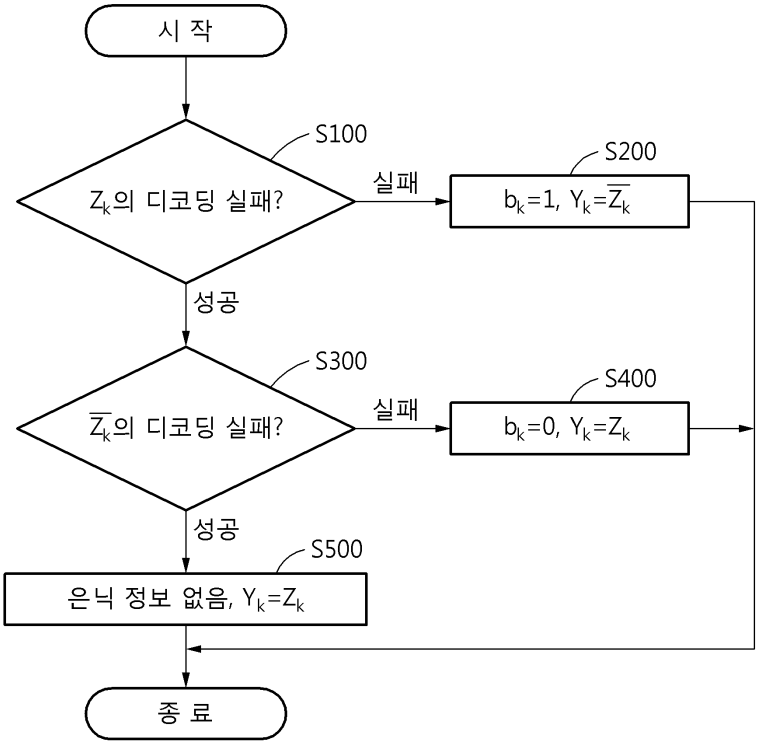
도면3


페이로드
헤더
Y_1
Y_2
Y_3
Y_4
Y_5
Y_{n-1}
Y_n
L
L
L
L
L
L
M

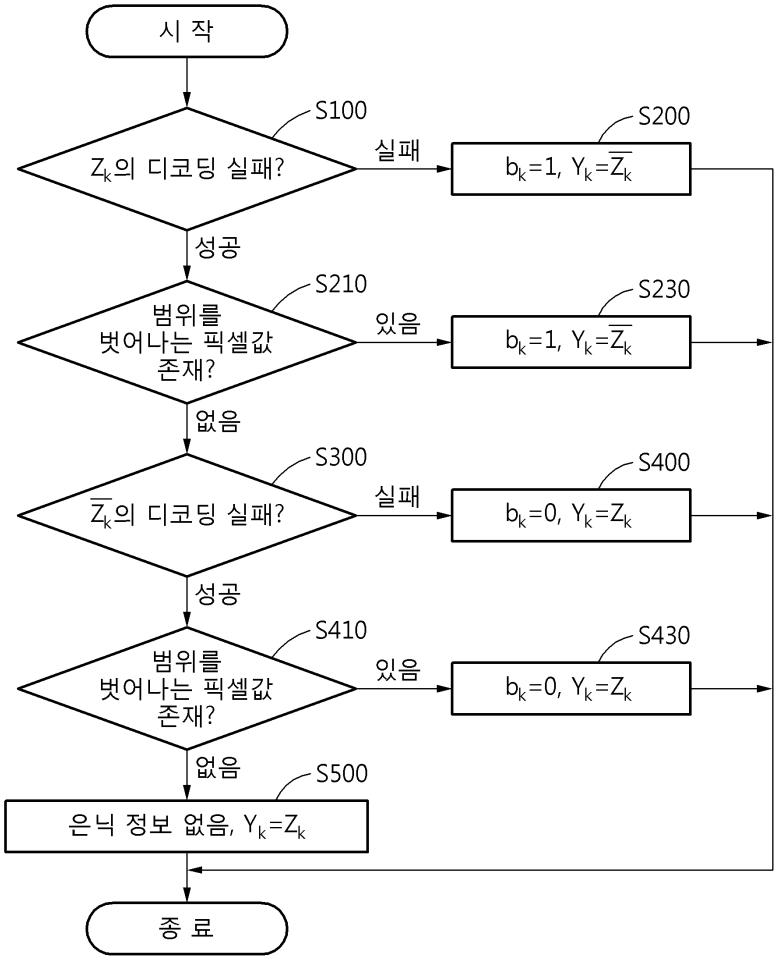
도면4


300
310
350
370
Z_k
은닉 영상 입력부
Z_k
Z_k
디코딩부
은닉 정보 추출부
330
비트 블럭 반전부
$\overline{Z_k}$

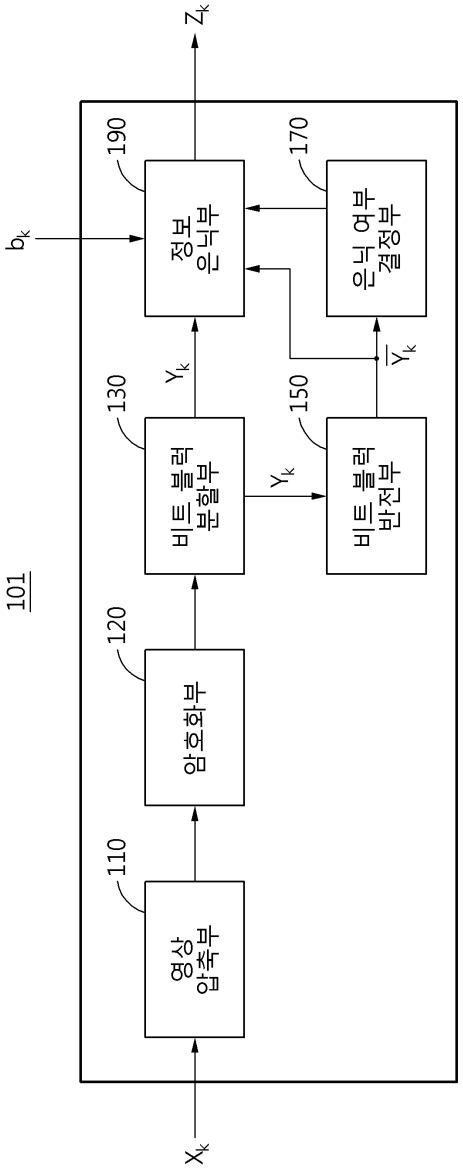
도면5


시 작
S100
Z_k의 디코딩 실패?
실패
S200
$b_k=1$, $Y_k=\overline{Z_k}$
성공
S300
$\overline{Z_k}$의 디코딩 실패?
실패
S400
$b_k=0$, $Y_k=Z_k$
성공
S500
은닉 정보 없음, $Y_k=Z_k$
종 료

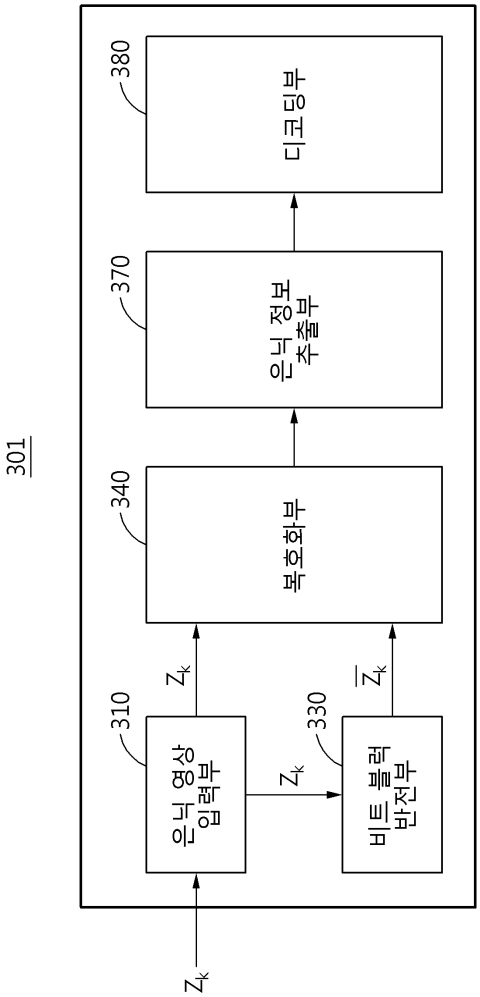
도면6


시 작
S100
Z_k의 디코딩 실패?
실패
S200
b_k=1, $Y_k=\overline{Z_k}$
성공
S210
범위를 벗어나는 픽셀값 존재?
있음
S230
b_k=1, $Y_k=\overline{Z_k}$
없음
S300
$\overline{Z_k}$의 디코딩 실패?
실패
S400
b_k=0, $Y_k=Z_k$
성공
S410
범위를 벗어나는 픽셀값 존재?
있음
S430
b_k=0, $Y_k=Z_k$
없음
S500
은닉 정보 없음, $Y_k=Z_k$
종 료

도면7


101
영상 압축부
110
암호화부
120
비트 블럭 분할부
130
비트 블럭 반전부
150
은닉 여부 결정부
170
정보 은닉부
190
X_k
Y_k
Y_k
$\overline{Y_k}$
b_k
Z_k

도면8


301
310
은닉 영상 입력부
330
비트 블럭 반전부
340
복호화부
370
은닉 정보 추출부
380
디코딩부
Z_k
Z_k
$\overline{Z_k}$
Z_k