



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2015년04월08일

(11) 등록번호 10-1506934

(24) 등록일자 2015년03월24일

(51) 국제특허분류(Int. Cl.)

H04N 5/913 (2006.01) H04N 21/4408 (2011.01)

(21) 출원번호 10-2014-0042887

(22) 출원일자 2014년04월10일

심사청구일자 2014년04월10일

(56) 선행기술조사문헌

JP2005026970 A*

KR1020100102155 A*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

충남대학교산학협력단

대전광역시 유성구 대학로 99 (궁동, 충남대학교)

(72) 발명자

류재철

대전 유성구 어은로 57, 132동 801호 (어은동, 한빛아파트)

김상우

대전 유성구 대학로145번길 22

유성민

대전 서구 신갈마로 121-7, 401호 (갈마동, 한마음빌라)

(74) 대리인

권혁수, 송윤호

전체 청구항 수 : 총 19 항

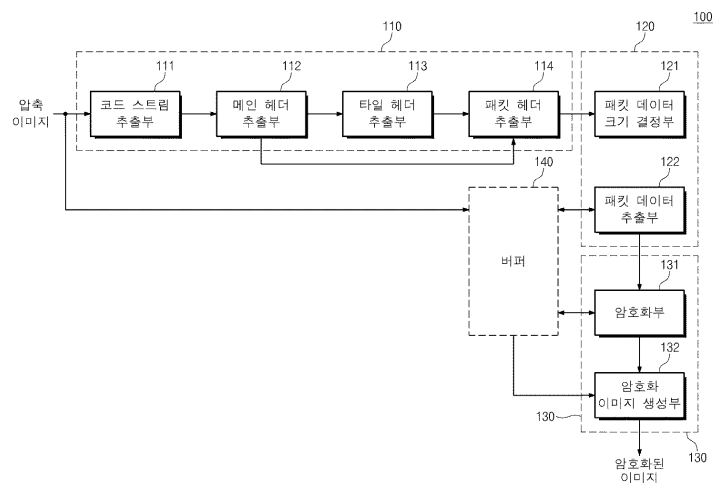
심사관 : 이성현

(54) 발명의 명칭 이미지 암호화 장치 및 그것의 이미지 암호화 방법

(57) 요약

본 발명은 이미지 암호화 장치에 관한 것이다. 본 발명의 이미지 암호화 장치는 압축 이미지로부터 헤더 정보를 추출하여 웨이블릿 변환에 따른 최저주파 영역의 데이터 추출을 위한 정보를 획득하는 헤더 추출부, 획득된 정보에 근거하여 최저주파 영역에 대응되는 데이터를 추출하는 암호화 데이터 추출부, 및 추출된 데이터를 암호화하고, 암호화된 데이터를 압축 이미지에 삽입하여 암호화된 압축 이미지를 생성하는 이미지 암호화부를 포함한다.

대표도



이 발명을 지원한 국가연구개발사업

과제고유번호 1711006475

부처명 미래창조과학부

연구관리전문기관 한국산업기술평가관리원

연구사업명 SW컴퓨팅산업원천기술개발

연구과제명 다양한 사용자 환경을 지원하기 위한 개인정보 대체기술 기반 개인정보보호 솔루션 개발

기 여 율 1/1

주관기관 (주)케이사인

연구기간 2013.06.01 ~ 2014.05.31

명세서

청구범위

청구항 1

압축 이미지로부터 헤더 정보를 추출하여 웨이블릿 변환에 따른 최저주파 영역의 데이터 추출을 위한 정보를 획득하는 헤더 추출부;

상기 획득된 정보에 근거하여 상기 최저주파 영역에 대응되는 데이터를 추출하는 암호화 데이터 추출부; 및

상기 추출된 데이터를 암호화하고, 상기 암호화된 데이터를 상기 압축 이미지에 삽입하여 암호화된 압축 이미지를 생성하는 이미지 암호화부를 포함하며,

상기 암호화 데이터 추출부는

상기 추출된 정보에 근거하여 결정된 패킷들 각각의 데이터 크기를 결정하는 패킷 데이터 크기 결정부; 및

상기 데이터 크기에 따라 상기 패킷들 각각으로부터 상기 최저주파 영역에 대응되는 데이터를 추출하는 패킷 데이터 추출부를 포함하는 이미지 암호화 장치.

청구항 2

제 1 항에 있어서,

상기 헤더 추출부는

상기 압축 이미지의 코드 스트림을 추출하는 코드 스트림 추출부;

상기 코드 스트림 내 메인 헤더를 추출하는 메인 헤더 추출부;

상기 코드 스트림 내 타일 헤더를 추출하는 타일 헤더 추출부; 및

상기 메인 헤더와 상기 타일 헤더에 포함된 정보를 이용하여 결정된 패킷들의 패킷 헤더를 추출하는 패킷 헤더 추출부를 포함하는 이미지 암호화 장치.

청구항 3

제 2 항에 있어서,

상기 메인 헤더 추출부는 상기 추출된 메인 헤더로부터 레이어 레벨을 획득하고, 상기 레이어 레벨에 따라 상기 최저주파 영역에 대응되는 패킷들을 결정하는 단계를 포함하는 이미지 암호화 장치.

청구항 4

제 3 항에 있어서,

상기 패킷 헤더 추출부는 상기 결정된 패킷들을 디코딩하여 패킷 헤더를 추출하는 이미지 암호화 장치.

청구항 5

압축 이미지로부터 헤더 정보를 추출하여 웨이블릿 변환에 따른 최저주파 영역의 데이터 추출을 위한 정보를 획득하는 헤더 추출부;

상기 획득된 정보에 근거하여 상기 최저주파 영역에 대응되는 데이터를 추출하는 암호화 데이터 추출부; 및

상기 추출된 데이터를 암호화하고, 상기 암호화된 데이터를 상기 압축 이미지에 삽입하여 암호화된 압축 이미지를 생성하는 이미지 암호화부를 포함하며,

상기 헤더 추출부는

상기 압축 이미지의 코드 스트림을 추출하는 코드 스트림 추출부;

상기 코드 스트림 내 메인 헤더를 추출하는 메인 헤더 추출부;

상기 코드 스트림 내 타일 헤더를 추출하는 타일 헤더 추출부; 및

상기 메인 헤더와 상기 타일 헤더에 포함된 정보를 이용하여 결정된 패킷들의 패킷 헤더를 추출하는 패킷 헤더 추출부를 포함하고,

상기 타일 헤더 추출부는 상기 타일 헤더로부터 패킷의 구성 정보를 포함하는 팩드 패킷 헤더(PPT)와 상기 패킷들의 길이를 나타내는 패킷 길이(PLT)를 추출하는 이미지 암호화 장치.

청구항 6

제 5 항에 있어서,

상기 패킷 헤더 추출부는 상기 결정된 패킷들을 상기 팩드 패킷 헤더(PPT)와 상기 패킷 길이(PLT) 정보를 이용하여 패킷으로부터 패킷 헤더를 추출하는 이미지 암호화 장치.

청구항 7

삭제

청구항 8

제 1 항에 있어서,

상기 추출된 정보는 패킷 헤더를 포함하고,

상기 패킷 데이터 크기 결정부는 상기 패킷 헤더에 포함된 비트 플레인 정보와 코딩 패스 정보를 이용하여 압축 데이터의 비트수를 결정하고, 상기 압축 데이터의 비트수에 대응되는 비트들이 나타내는 값을 통해 상기 패킷의 데이터 크기를 결정하는 이미지 암호화 장치.

청구항 9

제 8 항에 있어서,

상기 패킷 데이터 크기 결정부는 하기의 수학적식을 통해 상기 압축 데이터의 비트수를 결정하고,

[수학식]

$$Z=X+\log_2 Y$$

여기서, X는 상기 비트 플레인 정보에 따른 비트 플레인 값, Y는 상기 코딩 패스 정보에 따른 코딩 패스 값이고, Z는 압축 데이터의 비트수인 이미지 암호화 장치.

청구항 10

제 1 항에 있어서,

상기 이미지 암호화부는

상기 추출된 데이터를 암호화하는 암호화부;

상기 암호화된 데이터를 상기 압축 이미지에 삽입하여 암호화된 이미지를 생성하는 암호화 이미지 생성부를 포함하는 이미지 암호화 장치.

청구항 11

제 1 항에 있어서,

상기 압축 이미지는 제피이지2000(JPEG2000) 이미지인 이미지 암호화 장치.

청구항 12

제 1 항에 있어서,

상기 웨이블릿 변환은 이산 웨이블릿 변환을 포함하고,

상기 최저주파 영역은 상기 이산 웨이블릿 변환에 따른 레졸루션 레벨 0에 대응되는 영역인 이미지 암호화 장치.

청구항 13

이미지 암호화 장치의 이미지 암호화 방법에 있어서,

압축 이미지를 수신하는 단계;

상기 압축 이미지로부터 코드 스트림을 추출하고, 코드 스트림에서 헤더 정보를 추출하여 웨이블릿 변환에 따른 최저주파 영역의 추출을 위한 정보를 획득하는 단계;

상기 획득된 정보에 근거하여 상기 최저주파 영역에 대응되는 패킷들을 결정하는 단계;

상기 결정된 패킷들의 데이터를 추출하는 단계;

상기 추출된 데이터를 암호화하는 단계; 및

상기 암호화된 데이터를 상기 압축 이미지에 삽입하여 암호화된 압축 이미지를 생성하는 단계를 포함하며,

상기 결정된 패킷들의 데이터를 추출하는 단계는,

상기 획득된 정보에 근거하여 결정된 패킷들 각각의 데이터 크기를 결정하고, 상기 데이터 크기에 따라 상기 최저주파 영역에 대응되는 데이터를 추출하는 이미지 암호화 방법.

청구항 14

제 13 항에 있어서,

상기 최저주파 영역의 추출을 위한 정보를 획득하는 단계는

상기 코드 스트림을 추출하는 단계;

상기 코드 스트림 내 메인 헤더를 추출하고, 상기 메인 헤더로부터 상기 패킷들을 결정하기 위한 레이어 레벨에 대한 정보를 추출하는 단계; 및

상기 코드 스트림 내 타일 헤더를 추출하는 단계를 포함하는 이미지 암호화 방법.

청구항 15

제 14 항에 있어서,

상기 패킷들을 결정하는 단계는

상기 레이어 레벨에 근거하여 상기 암호화를 위한 패킷들을 결정하는 단계를 포함하는 이미지 암호화 방법.

청구항 16

이미지 암호화 장치의 이미지 암호화 방법에 있어서,

압축 이미지를 수신하는 단계;

상기 압축 이미지로부터 코드 스트림을 추출하고, 코드 스트림에서 헤더 정보를 추출하여 웨이블릿 변환에 따른 최저주파 영역의 추출을 위한 정보를 획득하는 단계;

상기 획득된 정보에 근거하여 상기 최저주파 영역에 대응되는 패킷들을 결정하는 단계;

상기 결정된 패킷들의 데이터를 추출하는 단계;

상기 추출된 데이터를 암호화하는 단계; 및

상기 암호화된 데이터를 상기 압축 이미지에 삽입하여 암호화된 압축 이미지를 생성하는 단계를 포함하고,

상기 최저주파 영역의 추출을 위한 정보를 획득하는 단계는,

상기 코드 스트림을 추출하는 단계;

상기 코드 스트림 내 메인 헤더를 추출하고, 상기 메인 헤더로부터 상기 패킷들을 결정하기 위한 레이어 레벨에 대한 정보를 추출하는 단계; 및

상기 코드 스트림 내 타일 헤더를 추출하는 단계를 포함하며,

상기 패킷들을 결정하는 단계는,

상기 레이어 레벨에 근거하여 상기 암호화를 위한 패킷들을 결정하는 단계를 포함하고,

상기 결정된 패킷들의 데이터를 추출하는 단계는,

상기 타일 헤더 내에 패킷들의 구성 정보를 포함하는 팩드 패킷 헤더와 상기 패킷들의 길이를 나타내는 패킷 길이를 포함하면, 상기 팩드 패킷 헤더와 상기 패킷 길이 정보를 이용하여 패킷 헤더를 추출하는 단계; 및

상기 타일 헤더 내에 상기 팩드 패킷 헤더와 상기 패킷 길이를 포함하지 않으면, 상기 패킷들을 디코딩하여 상기 패킷 헤더를 추출하는 단계를 포함하는 이미지 암호화 방법.

청구항 17

제 16 항에 있어서,

상기 패킷들의 데이터를 추출하는 단계는

상기 추출된 패킷 헤더에 포함된 비트 플레인 정보와 코딩 패스 정보를 이용하여 압축 데이터의 비트수를 결정하는 단계; 및

상기 압축 데이터의 비트수에 대응되는 비트들이 나타내는 값을 통해 상기 패킷의 데이터 크기를 결정하는 단계를 더 포함하는 이미지 암호화 방법.

청구항 18

제 17 항에 있어서,

상기 압축 데이터의 비트수는 하기의 수학적식을 통해 결정되고,

[수학적식]

$$Z=X+\log_2 Y$$

여기서, X는 상기 비트 플레인 정보에 따른 비트 플레인 값, Y는 상기 코딩 패스 정보에 따른 코딩 패스 값이고, Z는 압축 데이터의 비트수인 이미지 암호화 방법.

청구항 19

제 13 항에 있어서,

상기 압축 이미지는 제피이지2000(JPEG2000) 이미지인 이미지 암호화 방법.

청구항 20

제 13 항에 있어서,

상기 웨이블릿 변환은 이산 웨이블릿 변환을 포함하고,

상기 최저주파 영역은 상기 이산 웨이블릿 변환에 따른 레졸루션 레벨 0에 대응되는 영역인 이미지 암호화 방법.

발명의 설명

기술 분야

[0001] 본 발명은 이미지 처리 시스템에 관한 것으로서, 특히 압축 완료된 이미지를 암호화하는 이미지 암호화 장치 및 그것의 이미지 암호화 방법에 관한 것이다.

[0002] 본 발명은 미래창조과학부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)의 일환으로 수행된 연구로부터 도출된 것이다[과제번호: 10041579, 과제명: 다양한 사용자 환경을 지원하기 위한 개인정보 대체 기술 기반 개인정보보호 솔루션 개발](This work was supported by the IT R&D program of MSIP/KEIT. [10041579, Development the Personal Information Security service solution using tokenization technology]).

배경 기술

[0003] 현재 이미지 압축 방식은 이산 코사인 변환(DCT: Discrete Cosine Transform)에서 이산 웨이블릿 변환(DWT: Discrete Wavelet Transform)으로 점차 변화하고 있다. 그러므로, 이미지 암호화 및 난독화 기술도 이산 웨이블릿 변환에 관련되어 있다. 따라서, 이미지 암호화 기술은 이산 웨이블릿 변환 동작에서 이미지를 부분 암호화하거나 이미지의 중요 요소를 암호화하는 기술들이 이용되고 있다.

[0004] 이러한 이미지 암호화 기술들은 이미지 압축 동작 중에 수행될 수 있다. 하지만, 이미지 압축 동작에 개입이 불가능한 경우, 이미지 암호화가 불가능하다는 문제점이 있었다.

[0005] 또한, 이미지 압축이 완료된 이후에 다시 이미지 암호화를 수행할 수 있다. 하지만, 이미지 암호화를 압축 완료 이후에 수행함에 따라 이산 웨이블릿 변환을 추가로 다시 수행하여야 하는 문제점이 있었다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 목적은 압축 완료된 이미지를 추가적인 변환 동작없이 암호화할 수 있는 이미지 암호화 장치 및 그것의 암호화 방법을 제공함에 있다.

과제의 해결 수단

[0007] 본 발명에 따른 이미지 암호화 장치는 압축 이미지로부터 헤더 정보를 추출하여 웨이블릿 변환에 따른 최저주파 영역의 데이터 추출을 위한 정보를 획득하는 헤더 추출부, 상기 획득된 정보에 근거하여 상기 최저주파 영역에 대응되는 데이터를 추출하는 암호화 데이터 추출부, 및 상기 추출된 데이터를 암호화하고, 상기 암호화된 데이터를 상기 압축 이미지에 삽입하여 암호화된 압축 이미지를 생성하는 이미지 암호화부를 포함한다.

[0008] 이 실시예에 있어서, 상기 헤더 추출부는 상기 압축 이미지의 코드 스트림을 추출하는 코드 스트림 추출부, 상기 코드 스트림 내 메인 헤더를 추출하는 메인 헤더 추출부, 상기 코드 스트림 내 타일 헤더를 추출하는 타일 헤더 추출부, 및 상기 메인 헤더와 상기 타일 헤더에 포함된 정보를 이용하여 결정된 패킷들의 패킷 헤더를 추출하는 패킷 헤더 추출부를 포함한다.

[0009] 이 실시예에 있어서, 상기 메인 헤더 추출부는 상기 추출된 메인 헤더로부터 레이어 레벨을 획득하고, 상기 레이어 레벨에 따라 상기 최저주파 영역에 대응되는 패킷들을 결정하는 단계를 포함한다.

[0010] 이 실시예에 있어서, 상기 패킷 헤더 추출부는 상기 결정된 패킷들을 디코딩하여 패킷 헤더를 추출한다.

[0011] 이 실시예에 있어서, 상기 타일 헤더 추출부는 상기 타일 헤더로부터 패킷의 구성 정보를 포함하는 팩드 패킷 헤더(PPT)와 상기 패킷들의 길이를 나타내는 패킷 길이(PLT)를 추출한다.

[0012] 이 실시예에 있어서, 상기 패킷 헤더 추출부는 상기 결정된 패킷들을 상기 팩드 패킷 헤더와 상기 패킷 길이 정보를 이용하여 패킷으로부터 패킷 헤더를 추출한다.

[0013] 이 실시예에 있어서, 상기 암호화 데이터 추출부는 상기 추출된 정보에 근거하여 결정된 패킷들 각각의 데이터 크기를 결정하는 패킷 데이터 크기 결정부, 및 상기 데이터 크기에 따라 상기 패킷들 각각으로부터 상기 최저주파 영역에 대응되는 데이터를 추출하는 패킷 데이터 추출부를 포함한다.

[0014] 이 실시예에 있어서, 상기 추출된 정보는 패킷 헤더를 포함하고, 상기 패킷 데이터 크기 결정부는 상기 패킷 헤더에 포함된 비트 플레인 정보와 코딩 패스 정보를 이용하여 압축 데이터의 비트수를 결정하고, 상기 압축 데이터의 비트수에 대응되는 비트들이 나타내는 값을 통해 상기 패킷의 데이터 크기를 결정한다.

[0015] 이 실시예에 있어서, 상기 패킷 데이터 크기 결정부는 하기의 수학적식을 통해 상기 압축 데이터의 비트수를 결정하고,

[0016] [수학식]

$$Z=X+\log_2 Y$$

[0017]

[0018] 여기서, X는 상기 비트 플레인 정보에 따른 비트 플레인 값, Y는 상기 코딩 패스 정보에 따른 코딩 패스 값이고, Z는 압축 데이터의 비트수이다.

[0019] 이 실시예에 있어서, 상기 이미지 암호화부는 상기 추출된 데이터를 암호화하는 암호화부, 상기 암호화된 데이터를 상기 압축 이미지에 삽입하여 암호화된 이미지를 생성하는 암호화 이미지 생성부를 포함한다.

[0020] 이 실시예에 있어서, 상기 압축 이미지는 제피이지2000(JPEG2000) 이미지이다.

[0021] 이 실시예에 있어서, 상기 웨이블릿 변환은 이산 웨이블릿 변환을 포함하고, 상기 최저주파 영역은 상기 이산 웨이블릿 변환에 따른 레졸루션 레벨 0에 대응되는 영역이다.

[0022] 본 발명에 따른 이미지 암호화 장치의 이미지 암호화 방법은 압축 이미지를 수신하는 단계, 상기 압축 이미지로부터 코드 스트림을 추출하고, 코드 스트림에서 헤더 정보를 추출하여 웨이블릿 변환에 따른 최저주파 영역의 추출을 위한 정보를 획득하는 단계, 상기 획득된 정보에 근거하여 상기 최저주파 영역에 대응되는 패킷들을 결정하는 단계, 상기 결정된 패킷들의 데이터를 추출하는 단계, 상기 추출된 데이터를 암호화하는 단계, 및 상기 암호화된 데이터를 상기 압축 이미지에 삽입하여 암호화된 압축 이미지를 생성하는 단계를 포함한다.

[0023] 이 실시예에 있어서, 상기 최저주파 영역의 추출을 위한 정보를 획득하는 단계는 상기 코드 스트림을 추출하는 단계, 상기 코드 스트림 내 메인 헤더를 추출하고, 상기 메인 헤더로부터 상기 패킷들을 결정하기 위한 레이어 레벨에 대한 정보를 추출하는 단계, 및 상기 코드 스트림 내 타일 헤더를 추출하는 단계를 포함한다.

[0024] 이 실시예에 있어서, 상기 패킷들을 결정하는 단계는 상기 레이어 레벨에 근거하여 상기 암호화를 위한 패킷들을 결정하는 단계를 포함한다.

[0025] 이 실시예에 있어서, 상기 결정된 패킷들의 데이터를 추출하는 단계는 상기 타일 헤더 내에 패킷들의 구성 정보를 포함하는 팩트 패킷 헤더와 상기 패킷들의 길이를 나타내는 패킷 길이를 포함하면, 상기 팩트 패킷 헤더와 상기 패킷 길이 정보를 이용하여 패킷 헤더를 추출하는 단계, 및 상기 타일 헤더 내에 상기 팩트 패킷 헤더와 상기 패킷 길이를 포함하지 않으면, 상기 패킷들을 디코딩하여 상기 패킷 헤더를 추출하는 단계를 포함한다.

[0026] 이 실시예에 있어서, 상기 패킷들의 데이터를 추출하는 단계는 상기 추출된 패킷 헤더에 포함된 비트 플레인 정보와 코딩 패스 정보를 이용하여 압축 데이터의 비트수를 결정하는 단계, 및 상기 압축 데이터의 비트수에 대응되는 비트들이 나타내는 값을 통해 상기 패킷의 데이터 크기를 결정하는 단계를 더 포함한다.

[0027] 이 실시예에 있어서, 상기 압축 데이터의 비트수는 하기의 수학적식을 통해 결정되고,

[0028] [수학식]

$$Z=X+\log_2 Y$$

[0029]

[0030] 여기서, X는 상기 비트 플레인 정보에 따른 비트 플레인 값, Y는 상기 코딩 패스 정보에 따른 코딩 패스 값이고, Z는 압축 데이터의 비트수이다.

[0031] 이 실시예에 있어서, 상기 압축 이미지는 제피이지2000(JPEG2000) 이미지이다.

[0032] 이 실시예에 있어서, 상기 웨이블릿 변환은 이산 웨이블릿 변환을 포함하고, 상기 최저주파 영역은 상기 이산 웨이블릿 변환에 따른 레졸루션 레벨 0에 대응되는 영역이다.

발명의 효과

[0033] 본 발명의 이미지 암호화 장치는 압축 이미지의 웨이블릿 변환에 따른 최저주파 영역을 암호화함으로써, 이산 웨이블릿 변환과 같은 추가적인 변환 동작없이 압축 이미지를 암호화할 수 있다.

도면의 간단한 설명

- [0034] 도 1은 본 발명에 따른 이미지 암호화 장치를 예시적으로 도시한 도면,
 도 2는 본 발명에 따른 JPEG2000 파일의 구조를 예시적으로 도시한 도면,
 도 3은 본 발명에 따른 코드 스트림의 구조를 예시적으로 도시한 도면,
 도 4는 본 발명에 따른 이차원 이산 웨이블릿 변환을 예시적으로 도시한 도면,
 도 5는 본 발명에 따른 이차원 이미지의 3레벨의 이산 웨이블릿 변환에 따른 결과를 예시적으로 도시한 도면,
 도 6은 본 발명에 따른 3레벨 이산 웨이블릿 변환에 따라 분해된 이미지 데이터를 예시적으로 도시한 도면,
 도 7은 본 발명에 따른 레졸루션 레벨에 따른 레이어들을 예시적으로 도시한 도면,
 도 8은 도 1에 도시된 이미지 암호화 장치의 이미지 암호화 방법을 예시적으로 도시한 도면,
 도 9는 본 발명에 따른 이미지 암호화 동작을 수행하기 이전의 압축 이미지를 예시적으로 도시한 도면, 및
 도 10은 도 9에 도시된 압축 이미지를 암호화 완료한 이후 압축 해제한 이미지를 예시적으로 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0035] 이하, 본 발명에 따른 바람직한 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 하기의 설명에서는 본 발명에 따른 동작을 이해하는데 필요한 부분만이 설명되며 그 이외 부분의 설명은 본 발명의 요지를 모호하지 않도록 하기 위해 생략될 것이라는 것을 유의하여야 한다.
- [0036] 본 발명은 압축 완료된 압축 이미지를 이용하여 웨이블릿 변환의 최저주파 영역의 데이터(일례로, 레졸루션 레벨 0(resolution level 0)에 대응되는 데이터)를 암호화하는 이미지 암호화 장치를 제공한다.
- [0037] 하기에서는 압축 이미지를 제피이지2000(이하 'JPEG2000'이라 칭하기로 함) 이미지를 기준으로 설명하지만, 웨이블릿 변환을 이용한 다른 압축 이미지에도 본 발명을 적용할 수 있다. JPEG2000을 사용함에 따라, 본 발명의 이미지 암호화 장치는 이산 웨이블릿 변환(DWT: Discrete Wavelet Transform)과 같은 웨이블릿 변환을 통해 생성된 압축 이미지를 암호화할 수 있다.
- [0038] 도 1은 본 발명에 따른 이미지 암호화 장치를 예시적으로 도시한 도면이다.
- [0039] 도 1을 참조하면, 이미지 암호화 장치(100)는 헤더 추출부(110), 암호화 데이터 추출부(120), 이미지 암호화부(130), 및 버퍼(140)를 포함한다.
- [0040] 헤더 추출부(110)는 압축 이미지(JPEG2000)를 수신하고, 수신된 압축 이미지로부터 헤더 정보를 추출하여 이산 웨이블릿 변환에 따른 최저주파 영역의 데이터 추출을 위한 정보를 획득한다. 이를 통해, 헤더 추출부(110)는 암호화된 이미지를 포함한 패킷들을 결정할 수 있다.
- [0041] 헤더 추출부(110)는 코드 스트림 추출부(111), 메인 헤더 추출부(112), 및 타일 헤더 추출부(113), 및 패킷 헤더 추출부(114)를 포함한다.
- [0042] 코드 스트림 추출부(111)는 압축 이미지, 일례로 JPEG2000 이미지의 코드 스트림(code stream)을 추출한다. 코드 스트림은 메인 헤더와 복수의 타일들로 구성된다. 이때, 복수의 타일들에는 이미지 데이터들이 패킷과 같은 형태로 포함될 수 있다. 코드 스트림 추출부(111)는 추출된 코드 스트림을 메인 헤더 추출부(112)로 출력한다.
- [0043] 메인 헤더 추출부(112)는 코드 스트림 내 포함된 메인 헤더를 추출한다. 메인 헤더 추출부(112)는 메인 헤더의 코드 스타일 디폴트(Code style default, 이하 'COD'라 칭하기로 함)를 이용하여 레이어 레벨(layer level)에 관련된 정보를 획득한다. 이를 통해, 패킷 헤더 추출부(114)에서 타일에 포함된 패킷들의 디코딩 동작을 수행할 수 있다. 메인 헤더 추출부(112)는 획득된 레이어 레벨을 패킷 헤더 추출부(114)로 출력한다.
- [0044] 타일 헤더 추출부(113)는 타일들에 포함된 타일 헤더를 추출한다. 타일 헤더 추출부(113)는 타일 헤더의 추출을 통해 타일에 포함된 패킷들의 스트림 즉, 데이터(패킷) 스트림을 획득할 수 있다.
- [0045] 한편, 타일 헤더는 하기의 표 1에 예시적으로 나타내었다.

표 1

Tile Header Markers			
Mnemonic	Value	Description	Required
SOT	FF90	Start of tile	Y
SOD	FF93	start of data	Y
COD	FF52	Coding style default	N
QCD	FF5C	Quantization default	N
COC	FF53	Coding style component	N
QCC	FF5D	Quantization component	N
RGN	FF5E	Region of interest	N
POC	FF5F	Progressing order Change	N
PPT	FF61	Packed packet header:tile	N
PLT	FF58	Packet lengths:tile	N
COM	FF64	Comment	N

[0046]

[0047]

표 1에 나타난 바와 같이, 타일 헤더 추출부(113)에서 팩드 패킷 헤더(Packed packet header, 이하, 'PPT'라 칭하기로 함)와 패킷 길이(Packet length, 이하 'PLT'라 칭하기로 함)를 포함할 수 있다. 이때, PPT와 PLT는 선택적으로 타일 헤더에 포함될 수 있는 정보이다. 또한, PPT는 각 레졸루션 레벨 내의 패킷들의 배치 구조(또는, 배치 순서)를 나타낸다. 또한, PLT는 각 레졸루션 레벨 내의 패킷들 각각의 길이를 나타낸다.

[0048]

따라서, 타일 헤더 추출부(113)에서 타일 헤더로부터 PPT와 PLT를 획득하면, 패킷 헤더 추출부(114)(또는 패킷 데이터 추출부(122))는 패킷의 디코딩 동작을 수행하지 않고도, 암호화된 패킷들을 획득할 수 있다. 이를 통해, 패킷 헤더 추출부(114)는 패킷 헤더 또는 패킷 데이터를 추출할 수 있다.

[0049]

만약, 타일 헤더 추출부(113)에서 PPT와 PLT를 획득하지 못하면, 패킷 헤더 추출부(114)(또는 패킷 데이터 추출부(122))는 패킷의 디코딩을 통해 패킷 헤더 또는 패킷 데이터를 추출할 수 있다.

[0050]

패킷 헤더 추출부(114)는 메인 헤더 추출부(112)로부터 레이어 레벨을 수신한다. 레이어 레벨은 이산 웨이블릿 변환(DWT)에 따라 구분되는 레졸루션 레벨들 각각에 포함된 패킷들의 개수를 나타낸다. 따라서, 레이어 레벨을 수신한 패킷 헤더 추출부(114)는 레졸루션 레벨 0에 대응되는 패킷들의 개수를 확인할 수 있고, 확인된 패킷들을 암호화할 패킷으로 결정한다.

[0051]

패킷 헤더 추출부(114)는 이산 웨이블릿 변환(DWT)에 따른 최저주파 영역, 즉 레졸루션 레벨 0에 대응되는 패킷들의 패킷 헤더를 추출한다. 패킷 헤더 추출부(114)는 레이어 레벨에 따른 패킷 개수만큼 레졸루션 레벨 0의 패킷들에 대해 패킷 헤더들을 추출할 수 있다.

[0052]

패킷 헤더 추출부(114)는 추출된 패킷 헤더를 암호화 데이터 추출부(120)로 출력한다.

[0053]

암호화 데이터 추출부(120)는 최저주파 영역의 데이터 추출을 위한 정보, 일례로, 패킷 헤더를 이용하여 암호화를 위한 최저주파 영역의 데이터를 추출한다. 암호화 데이터 추출부(120)는 패킷 데이터 크기 결정부(121)와 패킷 데이터 추출부(122)를 포함한다.

[0054]

패킷 데이터 크기 결정부(121)는 암호화가 결정된 패킷들의 패킷 헤더를 이용하여 패킷들 각각의 데이터 크기를 결정한다. 패킷 데이터 크기 결정부(121)는 패킷 헤더에 포함된 정보를 이용하여 패킷의 데이터 크기를 결정한다.

[0055]

여기서, 패킷 헤더의 구조는 하기의 표 2에 예시적으로 나타내었다.

표 2

Bitstream bytes	Bit used	Comments
0xC7	1	Nonzero length packet
	1	Only code-block is included
0xD4	0001	3 zero bit-planes
	11 1101010	16 coding passes for this code-block
	0	Lblock remains3
0x0C	0000110	6byte of compress data
	0	padding bit

[0056]

[0057]

패킷 데이터 크기 결정부(121)는 비트 플레인(bit plane)을 확인한다. 제로가 3개이므로 비트 플레인 값은 3으로 결정된다. 패킷 데이터 크기 결정부(121)는 코딩 패스(coding pass)를 확인한다. 코딩 패스의 값은 16이다.

[0058]

패킷 데이터 크기 결정부(121)는 압축 데이터의 비트수(Z)를 비트 플레인 값과 코딩 패스 값을 이용하여 하기의 수학적 식 1로부터 획득할 수 있다.

수학적 식 1

$$Z=X+\log_2 Y$$

[0059]

[0060]

여기서, X는 비트 플레인값이고, Y는 코딩 패스 값이다. 예를 들어, 표 2에 도시된 바와 같이, X를 3으로 설정하고, Y를 16으로 설정하면, 압축 데이터의 비트수(Z)는 7이 된다. 따라서, 표 2에 도시된 압축 데이터들(compress data)로 표기된 7개의 비트들(0000110)이 패킷 데이터의 크기를 나타낸다. 이를 통해, 패킷 데이터의 크기는 7개의 비트들이 나타내는 이진수(0000110)를 십진수로 변환하면 6을 획득할 수 있으므로, 6바이트가 패킷 데이터의 크기가 된다.

[0061]

패킷 데이터 크기 결정부(121)는 결정된 패킷의 데이터 크기를 패킷 데이터 추출부(122)로 출력한다.

[0062]

패킷 데이터 추출부(122)는 패킷 데이터 크기를 이용하여 패킷들 내에서 패킷 데이터를 추출한다. 패킷 데이터 추출부(122)는 패킷들로부터 추출된 데이터들을 이미지 암호화부(130)로 출력한다. 또한, 패킷 데이터 추출부(122)는 추출된 데이터를 버퍼(140)에 저장할 수도 있다.

[0063]

이미지 암호화부(130)는 추출된 데이터를 암호화하고, 암호화된 데이터를 압축 이미지에 삽입하여 암호화된 압축 이미지를 생성할 수 있다.

[0064]

이미지 암호화부(130)는 암호화부(131)와 암호화 이미지 생성부(132)를 포함한다.

[0065]

암호화부(131)는 추출된 데이터를 수신하면, 추출된 데이터를 암호화한다. 암호화부(131)는 에이이에스(AES: Advanced Encryption Standard)(일예로, 씨티알(CTR: Counter), 오프비(OFB: Output Feedback))와 같은 암호화 알고리즘이 사용될 수 있다. 암호화부(131) 추출된 데이터를 버퍼(140)를 통해 수신할 수도 있다. 암호화부(131)는 암호화된 데이터(또는, 패킷)를 암호화 이미지 생성부(132)로 출력한다.

[0066]

암호화 이미지 생성부(132)는 암호화된 데이터(또는 패킷)를 압축 이미지에 삽입하여 암호화된 이미지를 생성한다. 암호화 이미지 생성부(132)는 압축 이미지를 저장한 버퍼(140)로부터 수신하고, 최저주파 영역, 즉 레졸루션 레벨 0에 대응되는 데이터를 암호화하여 압축 이미지에 삽입한다. 이를 통해, 암호화 이미지 생성부(132)는 암호화된 압축 이미지를 출력할 수 있다.

[0067]

버퍼(140)는 이미지 암호화 장치(100)의 전반적인 동작 중에 발생하는 데이터를 저장하거나, 저장된 데이터를 이미지 암호화 장치로 제공할 수 있다.

- [0068] 한편, 버퍼(140)는 압축 이미지를 저장할 수 있고, 암호화된 압축 이미지의 생성을 위해 압축 이미지를 암호화 이미지 생성부(132)로 제공할 수 있다. 또한, 버퍼(140)는 암호화부(131)에서 암호화한 이미지를 저장할 수도 있다.
- [0069] 본 발명에서, 암호화 이미지 장치(100)는 압축 이미지 내에서 저주파 필터로만 필터링된 최저주파 영역의 이미지 데이터만을 암호화한다. 여기서, 최저주파 영역은 레졸루션 레벨 0의 영역이므로, 암호화 이미지 장치(100)는 전체 압축 이미지의 데이터 대비 매우 작은 크기의 데이터만을 압축할 수 있다. 이를 통해, 암호화 이미지 장치(100)는 압축 완료된 이미지를 추가적인 변환 동작없이 암호화할 수 있다.
- [0070] 이를 통해, 암호화 이미지 장치(100)는 이미지 압축 과정의 변경없이 이미지를 암호화할 수 있고, 이미지 크기의 증가를 최소화할 수 있다.
- [0071] 도 2는 본 발명에 따른 JPEG2000 파일의 구조를 예시적으로 도시한 도면이다.
- [0072] 도 2를 참조하면, JPEG2000 파일(10)은 이산 웨이블릿 변환을 통해 생성된 압축 이미지이다.
- [0073] JPEG2000 파일(10)은 JPEG2000 시그니처(JPEG2000 Signature) 박스(11), 파일 타입(file type) 박스(12), JP2 헤더(JP2 Header) 박스(13), 및 연속된 코드 스트림 박스들(14)을 포함한다.
- [0074] JPEG2000 시그니처 박스(11)는 일례로, "0x6A7032"의 값을 가질 수 있다.
- [0075] 파일 타입 박스(12)는 파일 타입을 정의하는 4바이트의 데이터로 구성될 수 있다.
- [0076] JP2 헤더 박스(13)는 JPEG2000에 관련된 다양한 정보를 포함한다.
- [0077] 코드 스트림 박스(14)는 m개의 연속된 코드 스트림들이 연속된다.
- [0078] 여기서, JP2 헤더 박스(13)는 하위 박스들을 포함하고 있는 슈퍼 박스(super box)이지만, JP2 헤더 박스(13)가 존재하지 않더라도 이미지의 실행이 가능하다. 예를 들어, 의료용 디지털 이미지 및 통신 표준(DICOM: Digital Imaging and Communications in Medicine) 파일에는 JP2 헤더 박스(13)가 존재하지 않고, 코드 스트림 박스(13)만이 존재할 수도 있다.
- [0079] 이미지 압축 장치(100)는 코드 스트림 추출부(111)를 이용하여 코드 스트림 박스(14)의 코드 스트림들을 추출할 수 있다.
- [0080] 도 3은 본 발명에 따른 코드 스트림의 구조를 예시적으로 도시한 도면이다.
- [0081] 도 3을 참조하면, 이미지 압축 장치(100)에서 JPEG2000 파일(10)로부터 추출된 하나의 코드 스트림(200)은 메인 헤더(210)와 복수의 타일들(220-1, 220-n)을 포함한다.
- [0082] 메인 헤더(210)는 코드 스트림 시작(Start of code stream, 이하 'SOC'라 칭하기로 함)(211), 크기(Size)(212), COD(213), 및 양자화 디폴트(Quantization Default, 이하 'QCD'라 칭하기로 함)를 포함한다.
- [0083] SOC(211)은 코드 스트림의 시작을 나타낸다.
- [0084] 크기(SIZE)(212)는 이미지와 타일의 크기를 나타낸다.
- [0085] COD(213)는 JPEG2000 이미지의 코딩과 디코딩에 필요한 파라미터들을 포함한다.
- [0086] QCD(214)는 JPEG2000 이미지 양자화에 대한 정보, 양자화된 데이터 복원에 필요한 파라미터, 및 각 서브밴드에 대한 정보를 포함한다. QCD(214)는 마커(marker)를 포함하며, 약 17바이트 내지 23바이트의 크기를 가질 수 있다.
- [0087] 이때, 메인 헤더 추출부(112)는 메인 헤더(210)에 포함된 COD(213)를 추출할 수 있고, 추출된 COD(213)를 패킷 데이터의 디코딩에 이용할 수 있다.
- [0088] 복수의 타일들(220-1~220-n) 중에서 제 1 타일(220-1)을 기준으로 구조를 살펴보면 다음과 같다.
- [0089] 제 1 타일(220-1)은 타일 헤더(221)와 데이터(또는 패킷) 스트림(231)을 포함한다.
- [0090] 타일 헤더(221)는 타일 시작(Start of tile part, 이하 'SOT'라 칭하기로 함)(2211), 선택적 마커들(2212), 및 데이터 시작(Start of data, 이하 'SOD'라 칭하기로 함)(2213)을 포함한다.
- [0091] SOT(2211)은 타일의 시작을 나타낸다.

- [0092] 선택적 마커들(2212)은 선택적으로 포함될 수 있는 정보들을 포함한다. 여기서, 선택적으로 포함될 수 있는 정보들은 상술한 표 1을 통해 확인할 수 있다.
- [0093] SOD(2213)은 타일에 포함된 데이터의 시작을 나타낸다.
- [0094] 이때, 타일 헤더 추출부(113)는 선택적 마커들(2212)을 통해 이산 웨이블릿 변환 레벨(DWT level)과 레이어 레벨(Layer level)을 획득할 수 있다.
- [0095] 데이터 스트림(231)은 복수의 패킷들을 포함한다. 여기서, 하나의 패킷(2311)은 패킷 헤더와 패킷 데이터를 포함한다.
- [0096] 이때, 패킷 헤더 추출부(114)는 암호화가 결정된 패킷들에 대해 패킷 헤더를 추출할 수 있다. 패킷 헤더는 패킷 데이터의 크기에 대한 정보를 포함한다.
- [0097] 하기에서는 패킷 데이터의 구조를 설명하기 위한 이산 웨이블릿 변환을 예시적으로 살펴보기로 한다.
- [0098] 도 4는 본 발명에 따른 이차원 이산 웨이블릿 변환을 예시적으로 도시한 도면이다.
- [0099] 도 4를 참조하면, 이산 웨이블릿 변환은 높은 압축률을 획득하고, 확장 가능한 전송을 지원하기 위해 사용되며, JPEG2000 이미지를 획득하는데 이용된다.
- [0100] 이러한, 이산 웨이블릿 변환을 위해서는 고주파 필터(H(z))와 저주파 필터(L(z))를 로우(row) 방향과 컬럼(column) 방향으로 필터링하여 사용한다.
- [0101] 이산 웨이블릿 변환을 위해서 고주파 필터들(311, 321, 333)과 저주파 필터들(312, 322, 324)이 사용될 수 있다.
- [0102] 원본 이미지(20)는 로우 방향에서 제 1 고주파 필터(311)와 제 2 저주파 필터(312)를 통해 필터링된다.
- [0103] 이후, 제 1 고주파 필터(311)를 통해 필터링된 이미지는 컬럼 방향의 제 2 고주파 필터(321)와 제 2 저주파 필터(322)를 통해 각각 필터링된다. 제 2 고주파 필터(321)를 통해 제 1 이산 웨이블릿 이미지(HH1)를 획득할 수 있고, 제 2 저주파 필터(322)를 통해 제 2 이산 웨이블릿 이미지(HL1)를 획득할 수 있다.
- [0104] 저주파 필터(312)를 통해 필터링된 이미지는 컬럼 방향의 제 3 고주파 필터(323)와 제 3 저주파 필터(324)를 통해 각각 필터링된다. 제 3 고주파 필터(323)를 통해 제 3 이산 웨이블릿 이미지(LH1)를 획득할 수 있고, 제 3 저주파 필터(324)를 통해 제 4 이산 웨이블릿 이미지(LL1)를 획득할 수 있다.
- [0105] 한편, 고주파 필터들(311, 321, 333)과 저주파 필터들(312, 322, 324) 이후에 다운 샘플러(DS: Down Sampler)가 위치할 수 있으며, 다운 샘플러(DS)들은 필터링된 이미지를 다운 샘플링할 수 있다.
- [0106] 이와 같이, 하나의 이미지가 로우 방향과 컬럼 방향으로 각각 한 번씩 고주파 필터링과 저주파 필터링을 수행하는 것이 1레벨의 이산 웨이블릿 변환에 해당한다.
- [0107] 여기는, 제 1 레벨의 이산 웨이블릿 변환을 도시하고 있으나, 로우 방향과 컬럼 방향으로 고주파 필터링과 저주파 필터링을 각각 복수의 횟수로 반복하여 수행할 수도 있다.
- [0108] 도 5는 본 발명에 따른 이차원 이미지의 3레벨의 이산 웨이블릿 변환에 따른 결과를 예시적으로 도시한 도면이다.
- [0109] 도 5를 참조하면, 하나의 원본 이미지(410)를 이용한 3레벨 웨이블릿 변환을 수행한다.
- [0110] 원본 이미지를 1레벨의 이산 웨이블릿 변환을 수행하여 제 1 이미지(420)를 획득할 수 있다. 제 1 이미지(420)는 HH1, HL1, LH1, LL1의 이미지들로 구성될 수 있다. 제 1 이미지(420)에서 최저주파 영역은 LL1(421)이다.
- [0111] 1레벨 이산 웨이블릿 변환된 이미지(420)를 이산 웨이블릿 변환을 추가로 수행하면, 제 2 이미지(430)를 획득할 수 있다. 제 2 이미지(430)는 HH1, HL1, LH1, HH2, HL2, LH2, LL2의 이미지들로 구성될 수 있다. 제 2 이미지(430)에서 최저주파 영역은 LL2(431)이다.
- [0112] 2레벨 이산 웨이블릿 변환된 이미지(430)를 이산 웨이블릿 변환을 추가로 수행하면, 제 3 이미지(440)를 획득할 수 있다. 제 3 이미지(440)는 HH1, HL1, LH1, HH2, HL2, LH2, HH3, HL3, LH3, LL3의 이미지들로 구성될 수 있다. 제 3 이미지(440)에서 최저주파 영역은 LL3(441)이다.
- [0113] 따라서, 이미지 암호화 장치(100)는 1레벨 이산 웨이블릿 변환일 때, LL1(421)을 암호화할 수 있고, 2레벨 이산

웨이블릿 변환일 때, LL2(431)을 암호화할 수 있다. 또한, 이미지 암호화 장치(100)는 3레벨 이산 웨이블릿 변환일 때, LL3(441)을 암호화할 수 있다.

- [0114] 이와 같이, 이산 웨이블릿 레벨의 수행 횟수에 따라 이미지 암호화 장치(100)는 최저주파 영역의 데이터를 추출하고, 추출된 데이터를 암호화할 수 있다. 또한, 3레벨 이산 웨이블릿 변환 이상에 대해서도 위와 유사한 방식으로 최저주파 영역을 결정할 수 있다.
- [0115] 도 6은 본 발명에 따른 3레벨 이산 웨이블릿 변환에 따라 분해된 이미지 데이터를 예시적으로 도시한 도면이다.
- [0116] 도 6을 참조하면, 원본 이미지를 이용한 3레벨 이산 웨이블릿 변환을 수행하면, 3레벨 이산 웨이블릿 변환을 수행하면, 4개의 레졸루션 레벨이 형성된다.
- [0117] 첫 번째 이산 웨이블릿 변환에 따른 HH2, HL2, LH1을 포함한 이미지는 레졸루션 레벨 3(R3)이 된다.
- [0118] 두 번째 이산 웨이블릿 변환에 따른 HH2, HL2, LH2를 포함한 이미지는 레졸루션 레벨 2(R2)가 된다.
- [0119] 세 번째 이산 웨이블릿 변환에 따른 HH3, HL3, LH3을 포함한 이미지는 레졸루션 레벨 1(R1)이 된다. 또한, LL3을 포함한 이미지는 레졸루션 레벨 0(R0)이 된다.
- [0120] 본 발명에서는, 레졸루션 레벨(0)에 대응되는 LL3의 이미지를 암호화한다. LL3의 이미지는 저주파 필터로만 필터링된 이미지로서, 사람의 눈이 민감한 데이터들이 포함된다. 따라서, 이미지 암호화 장치(100)는 레졸루션 레벨 0에 대응되는 데이터들을 암호화하면, JPEG2000 이미지의 형태를 식별 불가능하게 한다.
- [0121] 도 7은 본 발명에 따른 레졸루션 레벨에 따른 레이어들을 예시적으로 도시한 도면이다.
- [0122] 도 7을 참조하면, 레졸루션 레벨에 따른 레이어들이 도시된다. 레졸루션 레벨 0, 레졸루션 레벨 1, 레졸루션 레벨 2, 레졸루션 레벨 3 각각은 일예로 4개의 레이어들로 구성될 수 있고, L0, L1, L2, L3 각각은 레졸루션 레벨 0에 대응되는 패킷들을 나타낸다. 이때, 레졸루션 레벨(resolution level)은 4가 될 수 있다.
- [0123] 따라서, 레이어들 각각은 패킷들에 순서대로 포함될 수 있다.
- [0124] 이미지 암호화 장치(100)는 최저주파 영역인 레졸루션 레벨 0에 대응되는 빗금친 4개의 레이어들, 즉 패킷들(L0, L1, L2, L3)을 암호화한다.
- [0125] 도 8은 도 1에 도시된 이미지 암호화 장치의 이미지 암호화 방법을 예시적으로 도시한 도면이다.
- [0126] 도 8을 참조하면, 코드 스트림 추출부(111)는 압축 이미지를 수신한다(S101단계).
- [0127] 코드 스트림 추출부(111)는 압축 이미지로부터 코드 스트림을 추출한다(S103단계). 코드 스트림 추출부(111)는 추출된 코드 스트림을 메인 헤더 추출부(112)로 출력한다.
- [0128] 메인 헤더 추출부(112)는 코드 스트림으로부터 메인 헤더를 추출한다(S105단계). 메인 헤더 추출부(112)는 메인 헤더 내의 COD를 이용하여 레이어 레벨을 결정할 수 있다.
- [0129] 타일 헤더 추출부(113)는 코드 스트림으로부터 타일 헤더를 추출한다(S107단계). 타일 헤더 추출부(113)는 타일 헤더를 추출하여 데이터 스트림을 추출할 수 있다.
- [0130] 패킷 헤더 추출부(114)는 암호화될 패킷들의 패킷 헤더를 추출한다(S109단계). 패킷 헤더 추출부(114)는 메인 헤더 추출부(112)의 레이어 레벨에 따라 암호화될 패킷들을 결정할 수 있다. 여기서, 암호화될 패킷은 레졸루션 레벨 0에 대응되는 데이터를 포함한 패킷들이다. 레이어 레벨은 하나의 레졸루션 레벨에 포함된 패킷의 개수를 나타낸다. 예를 들어, 레이어 레벨이 4의 값을 가지면, 레졸루션 레벨에 포함된 패킷의 개수는 4개가 된다. 따라서, 레졸루션 레벨 0의 4개의 패킷이 암호화될 패킷이다. 따라서, 패킷 헤더 추출부(114)는 4개의 패킷의 패킷 헤더를 추출할 수 있다.
- [0131] 또한, 패킷 헤더 추출부(114)는 패킷 헤더를 추출하기 위해 패킷을 디코딩한다. 하지만, 패킷 헤더 추출부(114)는 타일 헤더 추출부(113)를 통해 PPT와 PLT를 수신하면, 디코딩없이 패킷들을 선택하고, 선택된 패킷으로부터 패킷 헤더를 추출할 수 있다. 패킷 헤더 추출부(114)는 추출된 패킷 헤더를 패킷 데이터 크기 결정부(121)로 출력한다.
- [0132] 패킷 데이터 크기 결정부(121)는 패킷 헤더에 포함된 비트 플레인 정보를 확인한다(S111단계).
- [0133] 패킷 데이터 크기 결정부(121)는 패킷 헤더에 포함된 코딩 패스 정보를 확인한다(S113단계).

- [0134] 패킷 데이터 크기 결정부(121)는 비트 플레인 정보와 코딩 패스 정보를 이용하여 압축 데이터의 비트수를 결정하고, 결정된 압축 데이터의 비트수들이 나타내는 값을 이용하여 패킷 데이터의 크기를 결정한다(S115단계). 패킷 데이터 크기 결정부(121)는 패킷 데이터 크기를 패킷 데이터 추출부(122)로 출력한다.
- [0135] 패킷 데이터 추출부(122)는 결정된 패킷 데이터의 크기에 따라 패킷 데이터를 추출한다(S117단계). 패킷 데이터 추출부(122)는 추출된 패킷 데이터를 암호화부(131)로 출력한다.
- [0136] 암호화부(131)는 추출된 패킷 데이터를 미리 결정된 방식으로 암호화한다(S119단계).
- [0137] 암호화부(131)는 레이어 레벨의 개수에 대응되는 패킷들의 암호화가 완료되었는지 확인한다(S121단계).
- [0138] S121단계의 확인결과, 레이어 레벨의 개수에 대응되는 패킷들의 암호화가 완료되면, 암호화 이미지 생성부(132)는 암호화된 패킷들을 수신된 압축 이미지에 삽입하여 암호화된 압축 이미지를 생성한다.
- [0139] 하지만, S121단계의 확인결과, 레이어 레벨의 개수에 대응되는 패킷들의 암호화가 완료되지 못하면, S109단계로 진행하여 다음 패킷의 패킷 데이터를 암호화한다.
- [0140] 도 9는 본 발명에 따른 이미지 암호화 동작을 수행하기 이전의 압축 이미지를 예시적으로 도시한 도면이다.
- [0141] 도 9를 참조하면, 암호화되기 전의 압축 이미지를 나타낸다. 의료용 이미지를 예시적으로 도시한다.
- [0142] 도 10은 도 9에 도시된 압축 이미지를 암호화 완료한 이후 압축 해제한 이미지를 예시적으로 도시한 도면이다.
- [0143] 도 10을 참조하면, 이미지 암호화 장치가 최저주파 영역의 데이터를 암호화한 이미지의 압축을 해제한다. 이때, 압축 해제된 이미지는 암호화를 통해 도 9에서 도시된 이미지를 식별할 수 없을 정도로 암호화된 것을 확인할 수 있다.
- [0144] 본 발명의 이미지 암호화 장치는 최저주파 영역의 이미지 데이터를 압축을 기재하고 있으나, 이미지 압축 장치에 대응되는 이미지 암호해제 장치는 암호화 기능(또는, 암호화부)을 암호화 해제 기능(또는, 암호해제부)으로의 대체를 통해 간단히 구현할 수 있다.
- [0145] 이를 통해, 본 발명에서 제안된 이미지 암호화 장치는 사람의 눈에 민감한 저주파 대역, 즉 웨이블릿 변환에 따른 최저주파 영역(레졸루션 레벨 0)에 대응되는 데이터를 암호화한다. 이와 같이, 이미지 암호화 장치는 압축 이미지를 이용하여 직접 암호화를 수행함에 따라 웨이블릿 변환과 같은 추가적인 변환 동작을 필요로 하지 않으며, 이미지 압축 과정에 개입할 수 없더라도 이미지의 암호화가 가능하다.
- [0146] 이때, 암호화된 데이터는 원본 이미지 대비 매우 작은 부분의 데이터로서, 메모리와 같은 자원을 효율적으로 사용할 수 있다. 암호화되는 이미지의 크기가 전체 이미지 대비 작은 부분에 해당하므로 이미지 압축 과정을 변경할 필요가 없다. 또한, AES-CTR과 같은 암호화 방식을 사용하면, 암호화에 따른 전체 이미지의 크기 변화가 없이 암호화가 가능하다.
- [0147] 본 발명의 이미지 암호화 장치는 예를 들면, 의료 영상 저장 전송 시스템(PACS: Picture archiving and communication system)과 같이 보호가 필요한 의료 이미지 파일들의 암호화에 적용될 수 있다.
- [0148] 제안된 이미지 암호화 장치는 전체 의료 이미지 파일의 암호화를 할 필요가 없으므로, 낮은 컴퓨팅 성능 및 낮은 메모리 성능을 갖는 병원에서 활용될 수 있다. 이는, 이미지 암호화 장치의 사용 예를 설명하기 위한 것으로 병원 이외의 다른 다양한 이미지를 사용하는 다른 분야에서도 이미지의 암호화에 활용될 수 있다.
- [0149] 한편, 본 발명의 상세한 설명에서는 구체적인 실시 예에 관하여 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 상술한 실시 예에 국한되어 정해져서는 안되며 후술하는 특허청구범위뿐만 아니라 이 발명의 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

- | | | |
|--------|------------------|----------------|
| [0150] | 100: 이미지 암호화 장치 | 110: 헤더 추출부 |
| | 120: 암호화 데이터 추출부 | 130: 이미지 암호화부 |
| | 111: 코드 스트림 추출부 | 112: 메인 헤더 추출부 |
| | 113: 타일 헤더 추출부 | 114: 패킷 헤더 추출부 |

121: 패킷 데이터 크기 결정부

122: 패킷 데이터 추출부

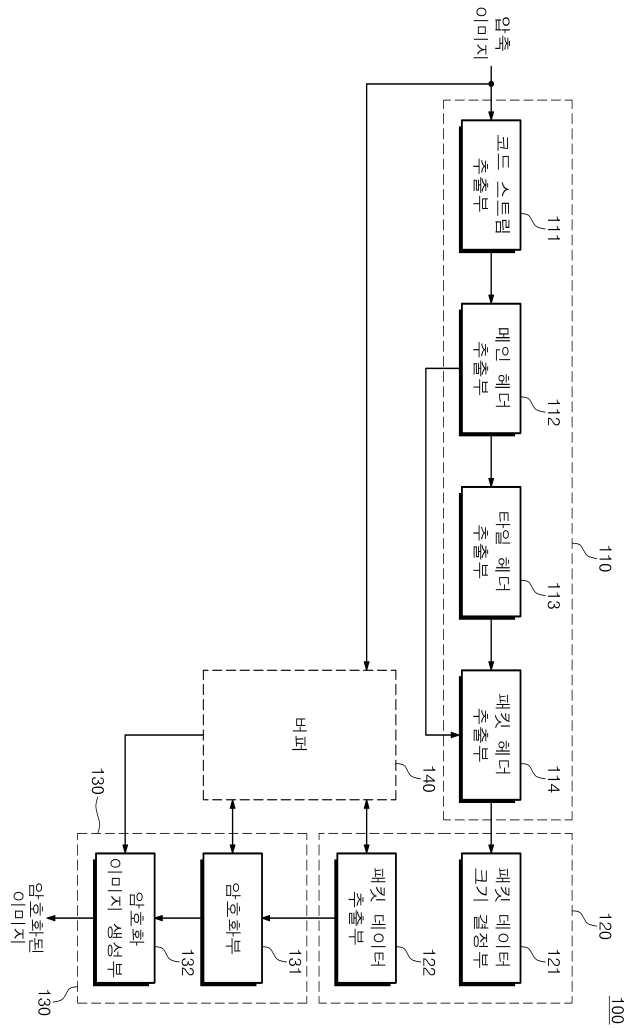
131: 암호화부

132: 암호화 이미지 생성부

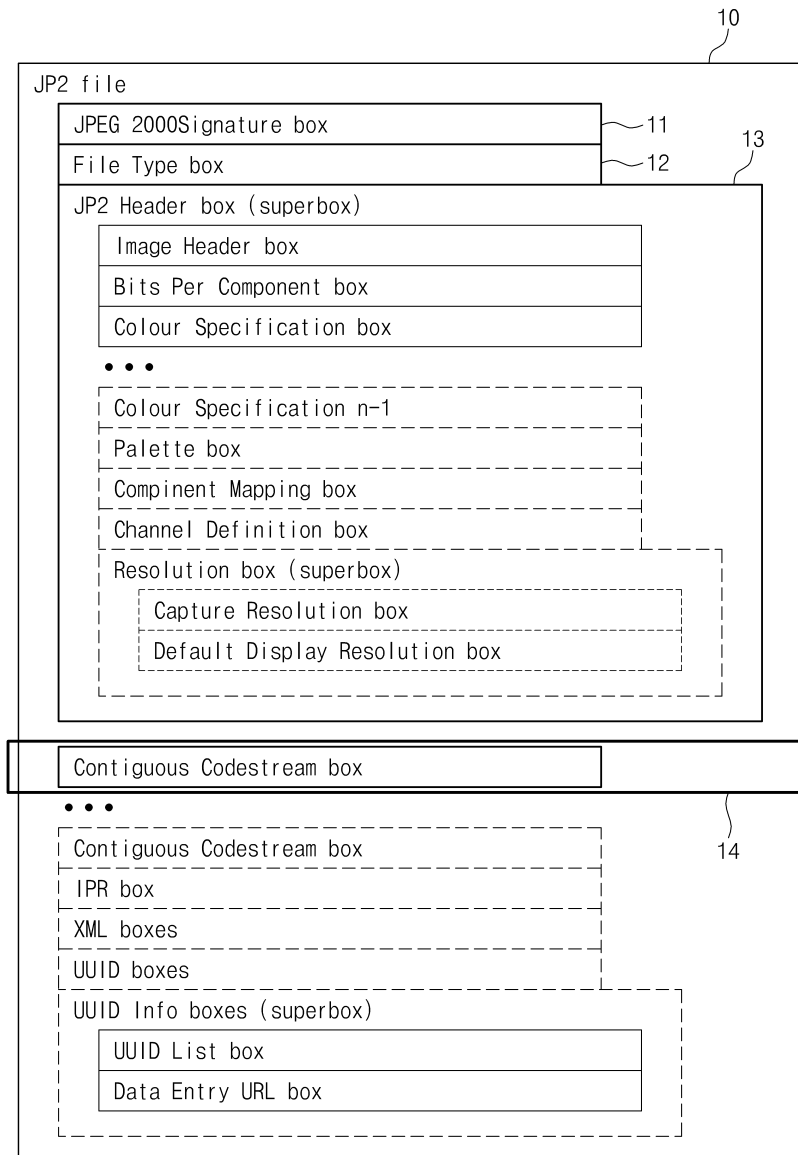
140: 버퍼

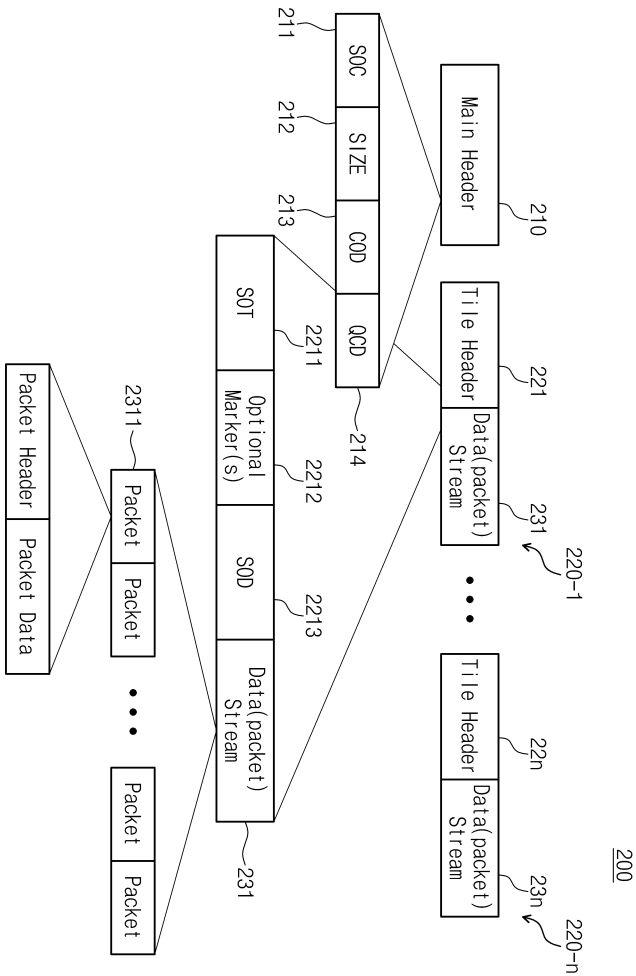
도면

도면1



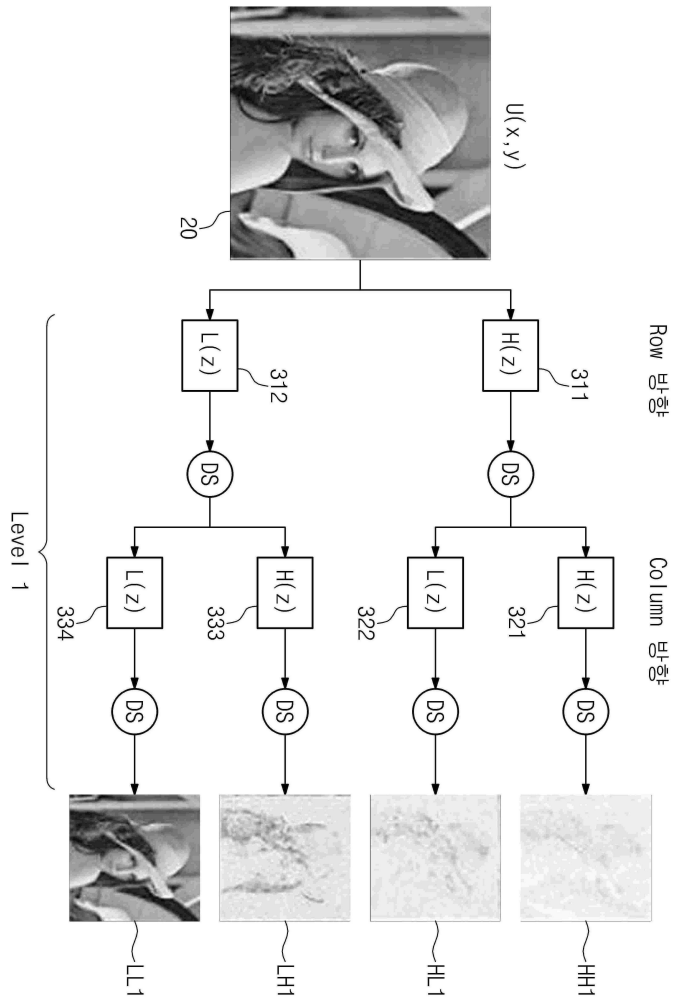
도면2



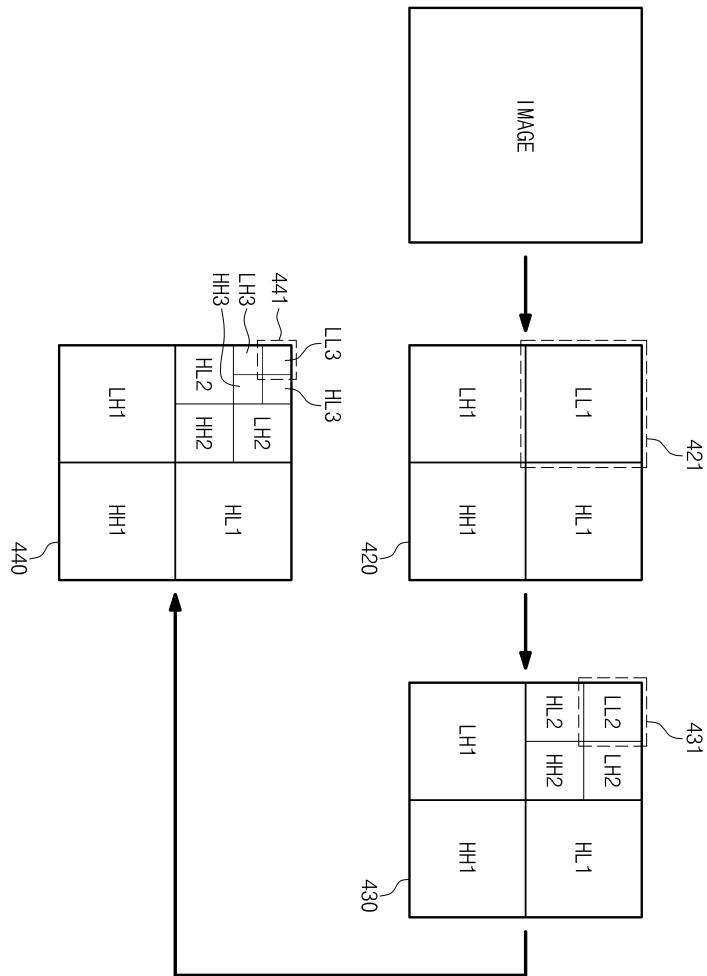


도면3

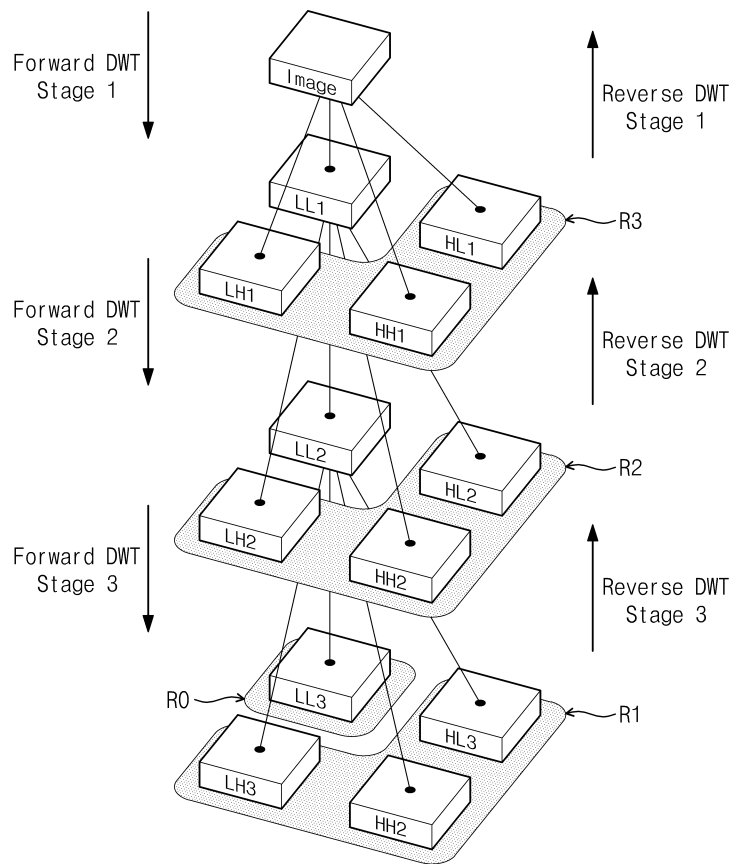
도면4



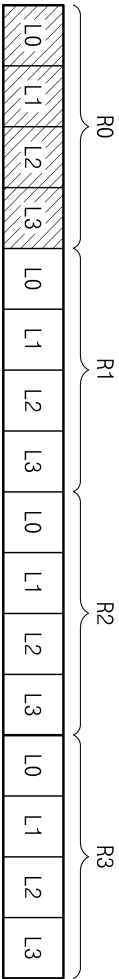
도면5



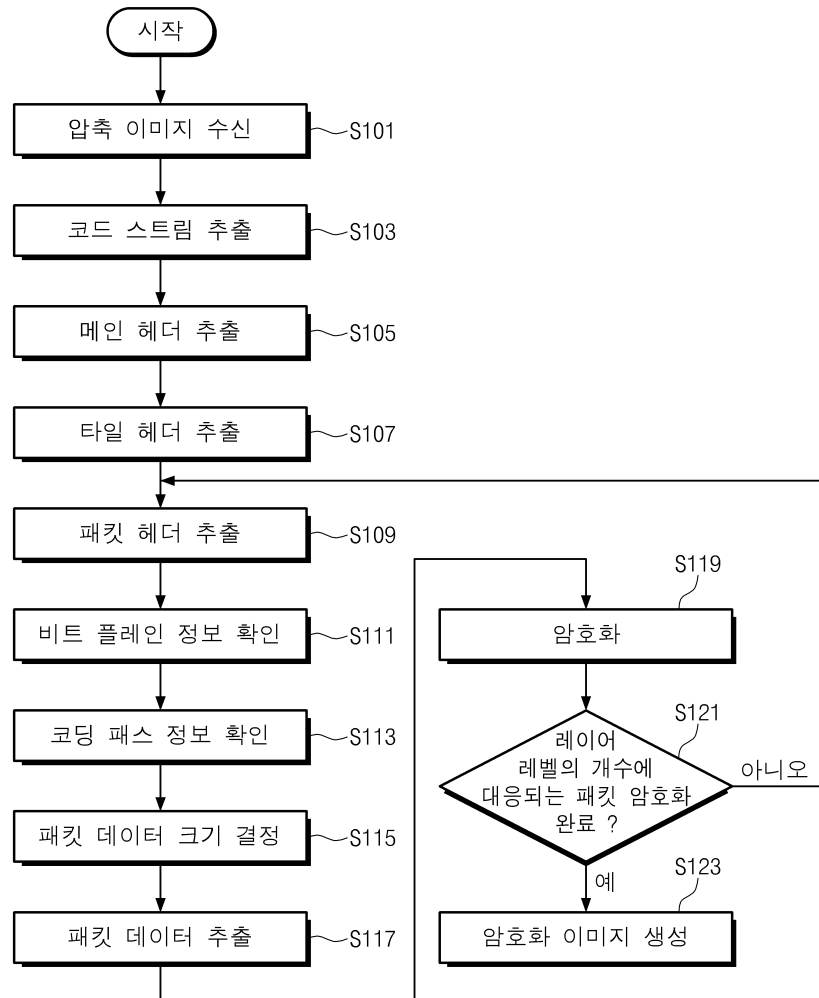
도면6



도면7



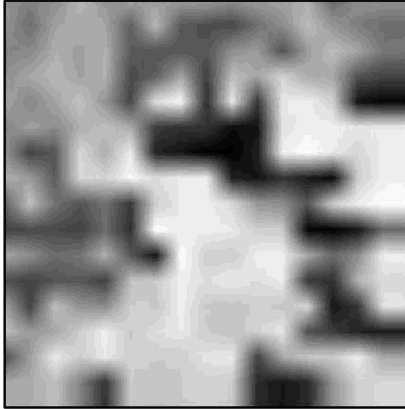
도면8



도면9



도면10



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 20

【변경전】

상기 웨이블릿 변환은

【변경후】

상기 웨이블릿 변환은