



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0063243  
(43) 공개일자 2015년06월09일

(51) 국제특허분류(Int. Cl.)  
H04N 19/625 (2014.01) A61B 6/00 (2006.01)  
(21) 출원번호 10-2013-0147784  
(22) 출원일자 2013년11월29일  
심사청구일자 2013년11월29일

(71) 출원인  
한국과학기술정보연구원  
대전광역시 유성구 대학로 245 (어은동)  
(72) 발명자  
윤희준  
대전 서구 대덕대로 150, 105동 1202호 (갈마동, 큰마을아파트)  
노서영  
대전 서구 도안동로 177, 116동 903호 (도안동, 도안신도시 수목토아파트)  
(74) 대리인  
특허법인 남앤드남

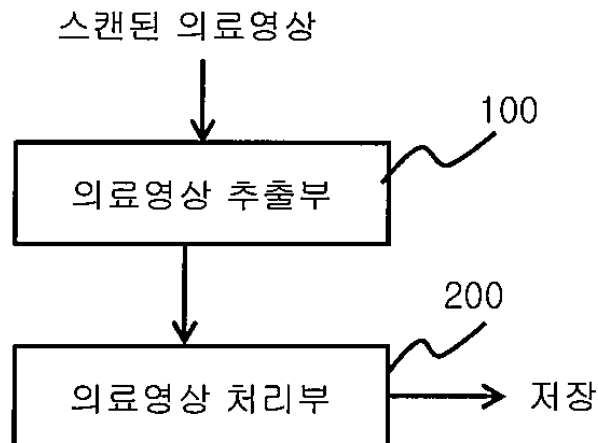
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 의료 영상 처리 방법 및 시스템

(57) 요약

본 발명은 의료 영상 처리 장치 및 방법이 개시된다. 본 발명에 따르면, DICOM 파일에 저장된 소정 포맷 형식의 의료 영상을 기 설정된 소정 단위로 추출하여 양자화 계수를 도출하고 도출된 양자화 계수를 기 설정된 소정 블록의 양자화 테이블로 나누어 양자화하여 의료 영상 데이터의 난독화를 실행함에 따라, 의료 영상 복원 시 양자화 테이블에 존재하는 의료 영상 데이터의 사이즈를 토대로 복원함에 있어 최소의 메모리 용량 및 향상된 속도로 의료 영상을 복원할 수 있으므로 의료 영상 해독 장비에 대한 의존도를 최소화할 수 있고, 기 설정된 소정 단위의 의료 영상을 AES 암호 알고리즘을 이용한 AES-CBC 모드를 통해 암호화함에 따라, 의료 영상 처리에 대한 무결성 검증이 가능하고, 비정상적인 의료 영상의 획득 및 암호화 복원 시 의료 영상의 복원이 불가능하여 암호화 기능을 향상시킬 수 있게 된다.

대표도 - 도1



(72) 발명자

**장행진**

대전 유성구 신성로84번길 33-16, 501호 (신성동, 벤처타운)

**류재철**

대전 유성구 어은로 57, 132동 801호 (어은동, 한빛아파트)

**신진섭**

대전 유성구 문화원로47번길 38, A동 302호 (궁동, 스위트빌)

**유성민**

대전 서구 계룡로326번길 33, A동 401호 (갈마동, 두원빌라)

**김상우**

대전 유성구 문화원로47번길 13, 204호 (궁동, 하나빌라)

## 명세서

### 청구범위

#### 청구항 1

소정 포맷의 의료 영상을 색상 변환 및 소정 단위로 샘플링하는 의료 영상 추출부;

상기 의료 영상 데이터를 이산 코사인 변환을 적용하여 생성된 양자화 계수를 기 설정된 소정 블록의 양자화 테이블로 나누어 양자화한 후 양자화 테이블의 양자화 계수를 토대로 압축 및 암호화하여 저장하는 의료 영상 처리부를 포함하는 것을 특징으로 하는 의료 영상 처리 장치.

#### 청구항 2

제1항에 있어서, 상기 양자화 테이블은

의료 영상 데이터의 휘도 테이블 및 광도 테이블로 설정되는 것을 특징으로 하는 의료 영상 처리 장치.

#### 청구항 3

제2항에 있어서, 상기 의료 영상 처리부는,

상기 이산 코사인 변환을 적용하여 소정 단위의 의료 영상에 대응되는 양자화 계수를 생성하고 생성된 양자화 계수를 기 설정된 소정 블록의 양자화 테이블로 나누어 양자화하는 의료 영상 양자화 모듈과,

소정 사이즈의 암호 키를 기반으로 상기 양자화 테이블의 양자화 계수를 암호화하여 저장하는 의료 영상 암호화 모듈을 포함하는 것을 특징으로 하는 의료 영상 처리 장치.

#### 청구항 4

제3항에 있어서, 상기 의료 영상 양자화 모듈은

상기 의료 영상 추출부의 의료 영상 데이터를 이산 코사인 변환을 통해 양자화 계수를 도출하는 양자화 계수 도출 소자와,

상기 양자화 계수 도출 소자의 양자화 계수를 기 설정된 양자화 테이블로 나누어 양자화하는 양자화 소자를 포함하는 것을 특징으로 하는 의료 영상 처리 장치.

#### 청구항 5

청구항 4에 있어서, 상기 의료 영상 암호화 모듈은,

상기 의료 영상 양자화 소자의 2차 압축된 의료 영상을 암호화하기 위한 키를 설정하는 키 생성 소자와,

상기 생성된 키를 이용하여 상기 양자화된 의료 영상을 AES(Advanced Encryption Standard) 암호 알고리즘의 AES-CBC(Cipher Block Changing) 모드를 통해 암호화하는 암호화 소자를 포함하는 것을 특징으로 하는 의료 영상 처리 장치.

#### 청구항 6

제5항에 있어서, 상기 의료 영상 암호화 모듈은,

상기 양자화 소자의 양자화 테이블의 양자화 계수를 암호화하기 위한 소정 사이즈의 암호 키를 설정하는 키 생성 소자와,

상기 생성된 암호 키를 이용하여 상기 양자화된 의료 영상을 AES(Advanced Encryption Standard) 암호 알고리즘의 AES-CBC(Cipher Block Changing) 모드를 통해 암호화하는 암호화 소자를 포함하는 것을 특징으로 하는 의료 영상 처리 장치.

#### 청구항 7

제1항 내지 제6항 중 한 항에 있어서, 상기 소정 단위는,

입력된 의료 영상 당 64 바이트 이상 256 바이트 이하인 것을 특징으로 하는 의료 영상 처리 장치.

**청구항 8**

입력된 의료 영상의 색상 변환 및 소정 단위로 샘플링하여 의료 영상의 일부분을 추출하는 의료 영상 추출부와,  
상기 의료 영상 추출부의 소정 단위의 의료 영상 데이터를 영상 주파수 데이터로 변환하기 위해 이산 코사인 변환을 적용하여 의료 영상 데이터의 양자화 계수를 도출하고 도출된 양자화 계수를 토대로 상기 의료 영상 데이터를 기 설정된 양자화 테이블로 나누어 양자화하는 의료 영상 양자화 모듈과,

상기 의료 영상 양자화 모듈의 양자화 테이블을 탐색하여 기 생성된 키를 기반으로 AES(Advanced Encryption Standard) 암호 알고리즘의 AES-CBC(Cipher Block Changing) 모드를 통해 암호화하여 저장하는 의료 영상 암호화 모듈을 포함하는 것을 특징으로 하는 의료 영상 처리 서버.

**청구항 9**

외부로부터 공급되는 의료 영상을 색상 변환 후 기 설정된 소정 단위로 샘플링하는 의료 영상 추출 단계와,

추출된 의료 영상 데이터를 이산 코사인 변환하여 양자화 계수를 도출하고 도출된 양자화 계수를 기 설정된 양자화 테이블로 나누어 양자화하는 의료 영상 양자화 단계와,

상기 양자화 테이블을 탐색하여 기 소정 사이즈로 생성된 암호 키를 기반으로 암호화하여 저장하는 의료 영상 암호화 단계를 포함하는 것을 특징으로 하는 의료 영상 처리 방법.

**청구항 10**

제9항에 있어서, 상기 의료 영상 양자화 단계는,

기 설정된 소정 단위의 의료 영상 데이터를 이산 코사인 변환을 적용하여 영상 주파수 데이터로 변환하여 양자화 계수를 도출하고,

도출된 양자화 계수를 기 설정된 양자화 테이블로 나누어 양자화하도록 구비되는 것을 특징으로 하는 의료 영상 처리 방법.

**청구항 11**

제9항에 있어서, 상기 소정 단위는,

수신된 의료 영상 데이터를 64 바이트 이상 256 바이트 이하로 구비되는 것을 특징으로 하는 의료 영상 처리 방법.

**청구항 12**

제9항에 있어서, 상기 양자화 테이블은,

상기 의료 영상 데이터의 휘도 테이블과 광도 테이블로 구비되는 것을 특징으로 하는 의료 영상 처리 방법.

**청구항 13**

제9항에 있어서, 상기 의료 영상 암호화 단계는,

상기 의료 영상 양자화 모듈의 양자화 테이블을 탐색하여 기 생성된 소정 사이즈의 암호 키를 기반으로 AES(Advanced Encryption Standard) 암호 알고리즘의 AES-CBC(Cipher Block Changing) 모드를 통해 암호화하여 저장하도록 구비되는 것을 특징으로 하는 의료 영상 처리 방법.

**발명의 설명**

**기술 분야**

[0001] 본 발명은 의료 영상 처리 시스템 및 방법에 관한 것으로, 보다 상세하게는 DICOM 파일 내에 저장된 소정 포맷의 의료 영상을 기 설정된 소정 단위로 압축 및 암호화할 수 있도록 한 장치 및 방법에 관한 것이다.

**배경 기술**

[0002] 의료영상저장전송시스템(Picture Archiving and Communication System, PACS)이 보급되면서, MRI, CT, X-ray와 같은 디지털화 된 의료영상정보들이 많이 사용되고 있다.

[0003] 이러한 의료영상정보들은 시스템 간 호환성을 위해 DICOM(Digital Imaging and Communications in Medicine) 표준을 준수하도록 되어 있다.

[0004] DICOM 표준형식의 의료영상정보 파일에는 환자 개인정보들과 함께 다수의 의료 영상이 포함되어 있다. 따라서 적절한 보호조치 없이 의료영상정보가 관리될 경우, 개인정보 유출, 환자 동의 없는 의료영상의 재사용 등의 문제들이 발생할 수 있다.

[0005] 이러한 문제를 해결하기 위해 DICOM 파일 전체를 암호화하게 되면 안전성 면에서 매우 효과적이다.

[0006] 하지만 최근에는 의료영상 촬영기기의 성능향상으로 HD급 의료영상 1장이 6MB에 이르며, DICOM 파일에는 이러한 의료영상이 다량으로 포함되어 있기 때문에 파일크기가 대용량화되는 추세이다.

[0007] 이로 인해, 의료 영상의 암호화 장비 및 해독 장비에 대한 성능 상의 문제로 DICOM 파일 전체에 이러한 암호화를 적용하기에는 어려움이 있다.

[0008] 따라서, 의료 영상의 복원율을 증가하고 의료 영상 해독 장비의 성능의 의존도를 최소화할 수 있는 의료 영상의 암호화 장치 및 로직이 요구된다.

**발명의 내용**

**해결하려는 과제**

[0009] 따라서, 본 발명은 상기의 문제점을 해결하기 위해 창출된 것으로, 본 발명의 목적은 DICOM 파일에 저장된 소정 포맷 형식의 의료 영상을 기 설정된 소정 단위로 추출하여 양자화 계수를 도출하고 도출된 양자화 계수를 기 설정된 소정 블록의 양자화 테이블로 나누어 양자화하여 의료 영상 데이터의 난독화를 실행함에 따라, 의료 영상 복원 시 양자화 테이블에 존재하는 의료 영상 데이터의 사이즈를 토대로 복원함에 있어 최소의 메모리 용량 및 향상된 속도로 의료 영상을 복원할 수 있으므로 의료 영상 해독 장비에 대한 의존도를 최소화할 수 있는 의료 영상 처리 방법 및 시스템을 제공하고자 함에 있다.

[0010] 본 발명의 다른 목적은, 기 설정된 소정 단위의 의료 영상 데이터를 양자화 테이블을 탐색한 후 생성된 암호 키를 토대로 AES 암호 알고리즘을 이용한 AES-CBC 모드를 통해 암호화함에 따라, 의료 영상 처리에 대한 무결성 검증이 가능하고, 비정상적인 의료 영상의 획득 및 암호화 해지 시 의료 영상의 복원이 불가능한 의료 영상 처리 방법 및 시스템을 제공하고자 함에 있다.

**과제의 해결 수단**

[0011] 상기 목적을 달성하기 위한 본 발명의 제1 관점에 따른 의료 영상 처리 시스템은,

[0012] 소정 포맷의 의료 영상을 색상 변환 및 소정 단위로 샘플링하는 의료 영상 추출부; 및

[0013] 상기 의료 영상 데이터를 이산 코사인 변환을 적용하여 생성된 양자화 계수를 기 설정된 소정 블록의 양자화 테이블로 나누어 양자화한 후 양자화 테이블의 양자화 계수를 토대로 압축 및 암호화하여 저장하는 의료 영상 처리 부를 포함하는 것을 특징으로 한다.

[0014] 바람직하게 상기 양자화 테이블은

[0015] 의료 영상 데이터의 휘도 테이블 및 광도 테이블로 설정되는 것을 특징으로 한다.

[0016] 바람직하게 상기 의료 영상 처리부는,

[0017] 상기 이산 코사인 변환을 적용하여 소정 단위의 의료 영상에 대응되는 양자화 계수를 생성하고 생성된 양자화 계수를 기 설정된 소정 블록의 양자화 테이블로 나누어 양자화하는 의료 영상 양자화 모듈과,

- [0018] 소정 사이즈의 암호 키를 기반으로 상기 양자화 테이블의 양자화 계수를 암호화하여 저장하는 의료 영상 암호화 모듈을 포함하는 것을 특징으로 한다.
- [0019] 바람직하게 상기 의료 영상 양자화 모듈은
- [0020] 상기 의료 영상 추출부의 의료 영상 데이터를 이산 코사인 변환을 통해 양자화 계수를 도출하는 양자화 계수 도출 소자와,
- [0021] 상기 양자화 계수 도출 소자의 양자화 계수를 기 설정된 양자화 테이블로 나누어 양자화하는 양자화 소자를 포함하는 것을 특징으로 한다.
- [0022] 바람직하게 상기 의료 영상 암호화 모듈은,
- [0023] 상기 양자화 소자의 양자화 테이블의 양자화 계수를 암호화하기 위한 소정 사이즈의 암호 키를 설정하는 키 생성 소자와,
- [0024] 상기 생성된 암호 키를 이용하여 상기 양자화 테이블을 탐색하여 AES(Advanced Encryption Standard) 암호 알고리즘의 AES-CBC(Cipher Block Changing) 모드를 통해 암호화하는 암호화 소자를 포함하는 것을 특징으로 한다.
- [0025] 바람직하게 상기 소정 단위는,
- [0026] 입력된 의료 영상 당 64 바이트 이상 256 바이트 이하인 것을 특징으로 한다.
- [0027] 상기 목적을 달성하기 위한 본 발명의 제2 관점에 따른 의료 영상 처리 서버는,
- [0028] 입력된 의료 영상의 색상 변환 및 소정 단위로 샘플링하여 의료 영상의 일부분을 추출하는 의료 영상 추출부와,
- [0029] 상기 의료 영상 추출부의 소정 단위의 의료 영상 데이터를 영상 주파수 데이터로 변환하기 위해 이산 코사인 변환을 적용하여 의료 영상 데이터의 양자화 계수를 도출하고 도출된 양자화 계수를 토대로 상기 의료 영상 데이터를 기 설정된 양자화 테이블로 나누어 양자화하는 의료 영상 양자화 모듈과,
- [0030] 상기 의료 영상 양자화 모듈의 양자화 테이블을 탐색하여 기 생성된 암호 키를 기반으로 AES(Advanced Encryption Standard) 암호 알고리즘의 AES-CBC(Cipher Block Changing) 모드를 통해 암호화하여 저장하는 의료 영상 암호화 모듈을 포함하는 것을 특징으로 한다.
- [0031] 상기 목적을 달성하기 위한 본 발명의 제3관점에 따른 의료 영상 처리 방법은,
- [0032] 외부로부터 공급되는 의료 영상을 색상 변환 후 기 설정된 소정 단위로 샘플링하는 의료 영상 추출 단계와,
- [0033] 추출된 의료 영상 데이터를 이산 코사인 변환하여 양자화 계수를 도출하고 도출된 양자화 계수를 기 설정된 양자화 테이블로 나누어 양자화하는 의료 영상 양자화 단계와,
- [0034] 상기 양자화 테이블을 탐색하여 기 소정 사이즈로 생성된 암호 키를 기반으로 암호화하여 저장하는 의료 영상 암호화 단계를 포함하는 것을 특징으로 한다.
- [0035] 바람직하게 상기 의료 영상 양자화 단계는,
- [0036] 기 설정된 소정 단위의 의료 영상 데이터를 이산 코사인 변환을 적용하여 영상 주파수 데이터로 변환하여 양자화 계수를 도출하고,
- [0037] 도출된 양자화 계수를 기 설정된 양자화 테이블로 나누어 양자화하도록 구비되는 것을 특징으로 한다.
- [0038] 바람직하게 상기 소정 단위는,
- [0039] 수신된 의료 영상 데이터를 64 바이트 이상 256 바이트 이하로 구비되는 것을 특징으로 한다.
- [0040] 바람직하게 상기 양자화 테이블은,
- [0041] 상기 의료 영상 데이터의 휘도 테이블과 광도 테이블로 구비되는 것을 특징으로 한다.
- [0042] 바람직하게 상기 의료 영상 암호화 단계는,
- [0043] 상기 의료 영상 양자화 모듈의 양자화 테이블을 탐색하여 기 생성된 소정 사이즈의 암호 키를 기반으로 AES(Advanced Encryption Standard) 암호 알고리즘의 AES-CBC(Cipher Block Changing) 모드를 통해 암호화하여 저장하도록 구비되는 것을 특징으로 한다.

**발명의 효과**

[0044] 이상에서 설명한 바와 같이, 본 발명에 따른 의료 영상 처리 방법 및 장치는, DICOM 파일에 저장된 소정 포맷 형식의 의료 영상을 기 설정된 소정 단위로 추출하여 양자화 계수를 도출하고 도출된 양자화 계수를 기 설정된 소정 블록의 양자화 테이블로 나누어 양자화하여 의료 영상 데이터의 단독화를 실행함에 따라, 의료 영상 복원 시 양자화 테이블에 존재하는 의료 영상 데이터의 사이즈를 토대로 복원함에 있어 최소의 메모리 용량 및 향상된 속도로 의료 영상을 복원할 수 있으므로 의료 영상 해독 장비에 대한 의존도를 최소화할 수 있게 된다.

[0045] 또한 본 발명에 따르면, 기 설정된 소정 단위의 의료 영상 데이터를 양자화 테이블을 탐색한 후 생성된 암호 키를 토대로 AES 암호 알고리즘을 이용한 AES-CBC 모드를 통해 암호화함에 따라, 의료 영상 처리에 대한 무결성 검증이 가능하고, 비정상적인 의료 영상의 획득 및 암호화 해지 시 의료 영상의 복원이 불가능하여 암호화 기능을 향상시킬 수 있는 효과를 얻는다.

**도면의 간단한 설명**

[0046] 본 명세서에서 첨부되는 다음의 도면들은 본 발명의 바람직한 실시 예를 예시하는 것이며, 후술하는 발명의 상세한 설명과 함께 본 발명의 기술사상을 더욱 이해시키는 역할을 하는 것이므로, 본 발명은 그러한 도면에 기재된 사항에만 한정되어 해석되어서는 아니된다.

- 도 1은 본 발명의 실시 예에 따른 의료 영상 처리 장치의 구성을 보인 도이다.
- 도 2는 본 발명의 실시 예에 따른 의료 영상 처리 장치의 의료 영상 처리부의 구성을 보인 도이다.
- 도 3은 본 발명의 실시 예에 따른 의료 영상부의 의료 영상 압축 모듈의 구성을 보인 도이다.
- 도 4는 본 발명의 실시 예에 따른 의료 영상 처리 장치의 의료 영상 암호화 모듈의 구성을 보인 도이다.
- 도 5는 본 발명의 실시 예에 따른 의료 영상 처리 장치의 의료 영상 데이터를 보인 예시도이다.
- 도 6은 본 발명의 실시 예에 따른 의료 영상 처리 장치에 의해 암호화된 의료 영상 데이터를 복원하기 위해 비교 연산을 보인 도이다.
- 도 7은 본 발명의 다른 실시 예에 따른 의료 영상 처리 과정을 보인 흐름도이다.

**발명을 실시하기 위한 구체적인 내용**

[0047] 본 발명과 본 발명의 동작상의 잇점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시 예를 예시하는 첨부 도면 및 도면에 기재된 내용을 참조하여야 한다.

[0048] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시 예를 설명함으로써, 본 발명을 상세히 설명한다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0049] 도 1은 본 발명의 실시 예에 따른 의료 영상 처리 장치의 구성을 보인 도이고, 도 2는 도 1에 도시된 의료 영상 처리 장치의 의료 영상 처리부의 구성을 보인 도이고, 도 3은 도 2에 도시된 의료 영상 처리부의 압축 모듈의 구성을 보인 도이며, 도 4는 도 2에 도시된 의료 영상 처리 장치의 의료 영상 암호화 모듈의 구성을 보인 도이다.

[0050] 본 발명의 실시 예에 따른 의료 영상 처리 장치는, 도 1 내지 도 3에 도시된 바와 같이, 수신된 다수의 의료 영상을 기 설정된 소정 단위로 추출한 후 양자화 계수에 따라 압축하고 압축된 소정 단위의 의료 영상을 암호화하여 저장하도록 구비된다.

[0051] 즉, 상기 의료 영상 처리 장치는, 도 1에 도시된 바와 같이, 의료 영상 추출부(100)와, 의료 영상 처리부(200)로 구비된다.

[0052] 여기서, 상기 의료 영상 추출부(110)는 스캔된 소정 포맷의 다수의 의료 영상 중 하나의 의료 영상의 색상 변환 후 소정 단위의 의료 영상을 샘플링하도록 구비된다. 상기 소정 포맷은, DICOM(Digital Imaging and Communication In Medicine) 파일의 JPEG(Joint photographic Expert Group)를 말한다.

[0053] 또한 소정 단위는 DICOM 파일의 JPEG 표준의 의료 영상 당 62 바이트 이상 256 바이트 단위이다.

[0054] 즉, 상기 의료 영상 추출부(110)는 소정의 DICOM 파일의 JPEG 표준의 의료 영상을 색상 변환 후 64 바이트 이상

256 바이트 이하의 소정 단위로 샘플링하여 의료 영상 처리부(200)로 전달한다.

[0055] 여기서, 상기 의료 영상 처리부(200)는, 도 2에 도시된 바와 같이, 의료 영상 압축 모듈(210) 및 의료 영상 암호화 모듈(230)을 포함한다.

[0056] 여기서, 상기 의료 영상 양자화 모듈(210)은 소정 단위로 샘플링된 영상을 이산 코사인 변환을 적용하여 양자화 계수를 산출하고 산출된 양자화 계수를 토대로 기 설정된 양자화 테이블로 나누어 저장한 후 양자화 테이블을 이용하여 의료 영상 추출부(100)의 의료 영상을 양자화하도록 구비된다.

[0057] 즉, 상기 의료 영상 양자화 모듈(210)은, 도 3에 도시된 바와 같이, 소정 단위로 샘플링된 영상을 이산 코사인 변환을 적용하여 양자화 계수를 산출하는 양자화 계수 산출 소자(211)와, 산출된 양자화 계수를 토대로 기 설정된 양자화 테이블로 나누어 저장한 후 저장된 양자화 테이블을 이용하여 의료 영상을 양자화하는 양자화 소자(213)로 구비된다.

[0058] 여기서, 상기 양자화 테이블은, 샘플링된 의료 영상의 휘도 테이블 및 광도 테이블을 포함하고, 상기 양자화 계수를 8x8의 블록으로 나누어 저장하는 구조를 가진다.

[0059] 따라서, 양자화 계수 산출 소자(211)는 상기 의료 영상 추출부(100)의 소정 단위로 샘플링된 의료 영상의 이산 코사인 변환을 적용하여 양자화 계수를 산출하고, 산출된 양자화 계수는 양자화 소자(213)에 전달된다.

[0060] 그리고, 상기 양자화 소자(213)는 수신된 양자화 계수를 기반으로 의료 영상을 8x8 블록 단위의 양자화 테이블로 나누어 양자화하고, 양자화된 의료 영상 데이터는 상기 의료 영상 암호화 모듈(230)로 전달된다. 이때 상기 양자화 테이블에 포함되는 데이터는 도 5에 도시된 바와 같다.

[0061] 즉, 상기 이산 코사인 변환을 적용하여 양자화 계수는 다음 연산 식 1을 기반으로 도출되며, 상기 양자화 계수는 다음 연산 식 1을 만족한다.

$$F(i, j) = C(i, j) \sum_{n=0}^{M-1} \sum_{m=0}^{M-1} f(n, m) \cos \frac{(2n+1)j\pi}{2N} \cos \frac{(2m+1)i\pi}{2N},$$

$$C(0,0) = \frac{1}{N}, C(i, j) = \frac{2}{N} (i \neq 0, j \neq 0) \quad \dots \text{식 1}$$

[0062] 여기서, C(i, j)는 진폭이고, n, m, i, j, n, N, M 는 모두 자연수이며, 기존의 배열 f(n, m)을 이용하여 새로운 배열F(i, j) 을 구하는 양자화를 실행한다.

[0063] 여기서 상기 소정 단위로 샘플링된 의료 영상 데이터를 상기 연산식을 기반으로 양자화하는 일련의 과정은 널리 알려진 영상 데이터를 상기 연산식을 토대로 양자화 계수를 도출하는 일련의 과정과 유사 또는 동일하므로 이에 대한 상세한 설명은 생략한다.

[0064] 또한 양자화 테이블이 비정상적으로 변조되면 의료 영상 데이터의 복원 시 상기 양자화 계수의 복원이 정상적으로 이루어지지 아니하므로, 원래의 의료 영상이 복원되지 않는다.

[0065] 즉, 하기 식2에서 도시된 바와 같이, 비정상적인 양자화 계수(E(i, j))로 인해 정상적인 양자화 테이블의 배열 f(n, m)과 다른 T(n, m)이 출력된다.

$$T(n, m) = \sum_{i=0}^{M-1} \sum_{j=0}^{M-1} E(i, j) F(i, j) \cos \frac{(2n+1)j\pi}{2N} \cos \frac{(2m+1)i\pi}{2N} \quad \dots \text{식 2}$$

[0066] 따라서, 양자화 소자(213)는 의료 영상의 크기와 무관하게 64 바이트 이상 256 바이트 이하의 의료 영상 데이터만으로 양자화 테이블을 이용하여 양자화된다.

[0067] 이때 양자화 테이블에 저장된 정보는 도 6에 도시된 바와 같다.

[0070] 상기 의료 영상 암호화 모듈(230)은 상기 양자화 소자(213)로부터 공급되는 양자화 테이블의 양자화 계수의 사이즈, 등을 탐색하여 기 설정된 소정 사이즈의 암호 키를 토대로 암호화하도록 구비된다.

[0071] 즉, 상기 의료 영상 암호화 모듈(230)은, 도 4에 도시된 바와 같이, 소정 사이즈의 키를 생성하는 키 생성 소자(231)과 키 생성 소자의 키를 기반으로 상기 의료 영상의 일부분을 양자화하는 양자화 테이블의 양자화 계수의 사이즈 등을 탐색하여 AES(Advanced Encryption Standard) 암호 알고리즘의 AES-CBC(Cipher Block Changing) 모드를 통해 암호화하는 암호화 소자(233)를 포함한다.

[0072] 여기서, 상기 소정 사이즈는 128 비트로 설정되고, 상기 AES(Advanced Encryption Standard) 암호 알고리즘의 AES-CBC(Cipher Block Changing) 모드를 통해 암호화하는 일련

- [0073] 의 과정은 널리 알려진 AES 암호 알고리즘의 CBC(Cipher Block Changing) 모드를 통해 암호화하는 과정과 동일 또는 유사하게 실행되므로 이에 대한 상세한 설명은 생략한다.
- [0074] 따라서, 상기 키 생성 소자(231)는 양자화 테이블의 데이터를 암호화하기 위한 128 비트의 암호 키를 생성하여 상기 암호화 소자(233)로 전달하고 상기 암호화 소자(233)는 생성된 암호 키를 토대로 양자화 테이블에 저장된 데이터를 탐색하여 AES(Advanced Encryption Standard) 암호 알고리즘의 AES-CBC(Cipher Block Changing) 모드를 통해 암호화하여 저장한다. 이때 암호화된 의료 영상 데이터의 포맷은 // 도 5에 도시된 바와 같이 정보들을 포함한다.
- [0075] 이러한 구성에 의하면, 의료 영상 추출부(100)에서 소정 단위로 샘플링한 의료 영상 데이터는 의료 영상 양자화 모듈(210)의 양자화 계수 도출 소자(211)에 제공되고, 상기 양자화 계수도출 소자(211)는 수신된 소정 단위의 샘플링된 의료 영상 데이터를 이산 코사인 변환을 적용하여 양자화 계수를 도출하고, 도출된 양자화 계수는 양자화 소자(213)로 전달한다.
- [0076] 그리고, 상기 양자화 소자(213)는 양자화 계수 도출 소자(211)의 양자화 계수를 기 설정된 사이즈 블록의 양자화 테이블로 나누어 저장하며 저장된 양자화 테이블을 이용하여 양자화하여 의료 영상 암호화 모듈(230)로 전달한다.
- [0077] 따라서 의료 영상 복원 과정에서 양자화 테이블에 존재하는 양자화 계수의 사이즈를 참조하여 비교함에 따라 불필요한 데이터 간의 비교를 배제함으로써, 도 6에 도시된 바와 같이, 2 바이트씩 비교 수행하여 1킬로바이트에 양자화 계수가 존재할 경우 기존의 영상의 난독화를 해지하기 위한 비교 연산이 500회인데 반해 본 발명에 따른 비교 횟수는 기존의 비교 연산 횟수에 비해 약 90% 이상 감소할 수 있고, 전체 의료 영상 처리 속도의 향상이 가능하다.
- [0078] 한편, 상기 의료 영상 암호화 모듈(230)의 키 생성 소자(231)는 수신된 양자화 계수를 암호화하기 위한 소정 사이즈의 암호 키를 생성하고, 생성된 암호 키는 암호화 소자(233)로 전달한다.
- [0079] 상기 암호화 소자(233)는 상기 생성된 소정 사이즈의 암호 키를 기반으로 양자화 계수를 AES(Advanced Encryption Standard) 암호 알고리즘의 AES-CBC(Cipher Block Changing) 모드를 통해 암호화하여 저장한다.
- [0080] 이상에서 설명한 바와 같이, 소정 크기로 추출된 의료 영상을 이산 코사인 변환을 적용하여 양자화 계수를 도출하고 양자화 계수를 기 설정된 소정 블록의 양자화 테이블로 양자화한 후 암호화하여 저장하는 일련의 과정을 도 6을 참조하여 설명한다.
- [0081] 도 7 본 발명의 다른 실시 예에 따른 의료 영상 처리 과정을 보인 흐름도로서, 도 1 내지 도 7 참조하여 본 발명의 다른 실시 예에 따른 의료 영상 처리 과정을 설명한다.
- [0082] 우선, 상기 의료 영상 추출부(100)는, 단계(501)를 통해 외부로부터 공급되는 의료 영상을 색상 변환 후 소정 단위로 샘플링하여 저장한 후 의료 영상 처리부(200)의 의료 영상 양자화 모듈(210)로 제공한다.
- [0083] 상기 의료 영상 양자화 모듈(210)은 단계(503)를 통해 소정 단위로 추출된 의료 영상을 이산 코사인 변환을 적용하여 양자화 계수를 도출하고 이어 단계(505)를 통해 양자화 계수를 소정 블록의 양자화 테이블로 나누어 양자화한다.
- [0084] 그리고, 상기 양자화 테이블로 나누어 양자화된 의료 영상 데이터는 의료 영상 암호화 모듈(230)로 전달한다.
- [0085] 상기 의료 영상 암호화 모듈(230)은 기 설정된 소정 사이즈의 암호 키를 생성한 후 생성된 암호 키를 기반으로 AES(Advanced Encryption Standard) 암호 알고리즘의 AES-CBC(Cipher Block Changing) 모드를 통해 암호화하여 저장한다(단계 507, 509).
- [0086] 본 발명의 실시 예에 따르면, DICOM 파일에 저장된 소정 포맷 형식의 의료 영상을 기 설정된 소정 단위로 추출하여 양자화 계수를 도출하고 도출된 양자화 계수를 기 설정된 소정 블록의 양자화 테이블로 나누어 양자화하여 의료 영상 데이터의 난독화를 실행함에 따라, 의료 영상 복원 시 양자화 테이블에 존재하는 의료 영상 데이터의 사이즈를 토대로 복원함에 있어 최소의 메모리 용량 및 향상된 속도로 의료 영상을 복원할 수 있으므로 의료 영상 해독 장비에 대한 의존도를 최소화할 수 있게 된다.
- [0087] 또한 본 발명에 따르면, 기 설정된 소정 단위의 의료 영상을 AES 암호 알고리즘을 이용한 AES-CBC 모드를 통해 암호화함에 따라, 의료 영상 처리에 대한 무결성 검증이 가능하고, 비정상적인 의료 영상의 획득 및 암호화 복

원 시 의료 영상의 복원이 불가능하여 암호화 기능을 향상시킬 수 있다.

[0088] 여기에 제시된 실시 예들과 관련하여 설명된 방법 또는 알고리즘의 단계들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

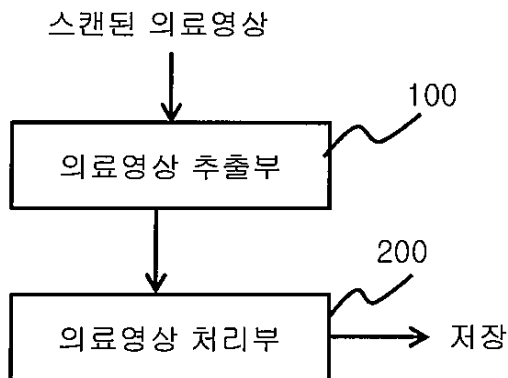
[0089] 지금까지 본 발명을 바람직한 실시 예를 참조하여 상세히 설명하였지만, 본 발명이 상기한 실시 예에 한정되는 것은 아니며, 이하의 특허청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 또는 수정이 가능한 범위까지 본 발명의 기술적 사상이 미친다 할 것이다.

**산업상 이용가능성**

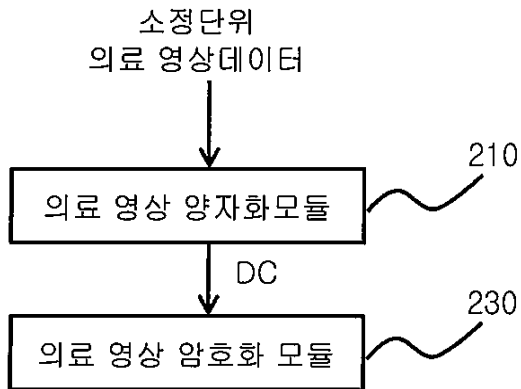
[0090] DICOM 파일에 저장된 소정 포맷 형식의 의료 영상을 기 설정된 소정 단위로 추출하여 양자화 계수를 도출하고 도출된 양자화 계수를 기 설정된 소정 블록의 양자화 테이블로 나누어 양자화하여 의료 영상 데이터의 난독화를 실행함에 따라, 의료 영상 복원 시 양자화 테이블에 존재하는 의료 영상 데이터의 사이즈를 토대로 복원함에 있어 최소의 메모리 용량 및 향상된 속도로 의료 영상을 복원할 수 있으므로 의료 영상 해독 장비에 대한 의존도를 최소화할 수 있고, 기 설정된 소정 단위의 의료 영상을 AES 암호 알고리즘을 이용한 AES-CBC 모드를 통해 암호화함에 따라, 의료 영상 처리에 대한 무결성 검증이 가능하고, 비정상적인 의료 영상의 획득 및 암호화 복원 시 의료 영상의 복원이 불가능하여 암호화 기능을 향상시킬 수 있는 의료 영상 처리 장치 및 방법에 대한 운용의 정확성 및 신뢰도 측면, 더 나아가 성능 효율 면에 매우 큰 진보를 가져올 수 있으며, 적용되는 데이터 전송 장치의 시판 또는 영업의 가능성이 충분할 뿐만 아니라 현실적으로 명백하게 실시할 수 있는 정도이므로 산업상 이용가능성이 있는 발명이다.

**도면**

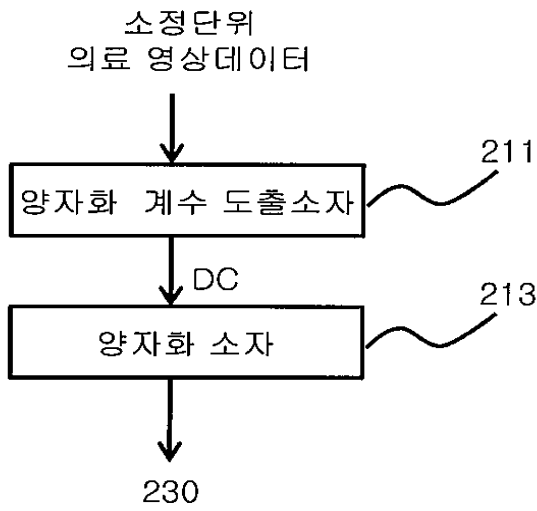
**도면1**



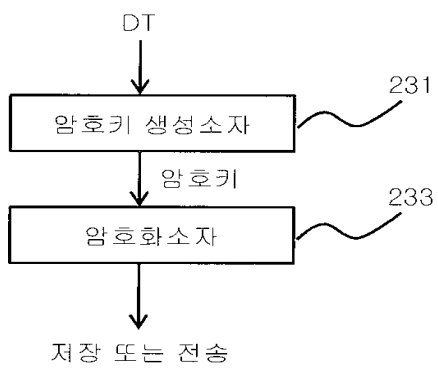
도면2



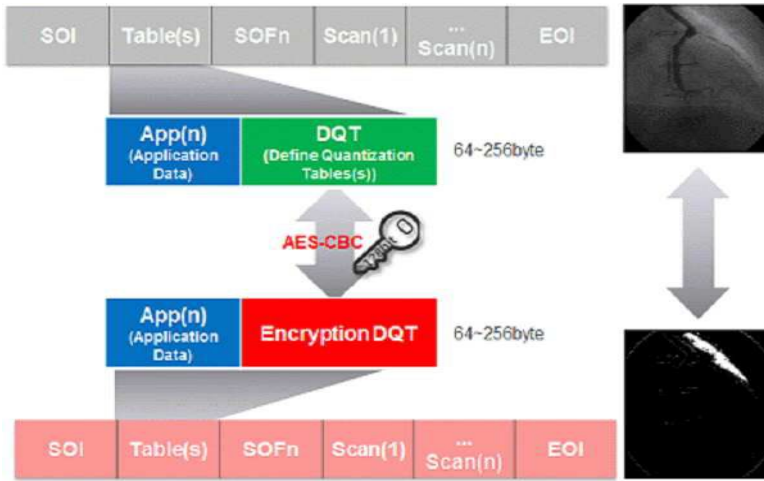
도면3



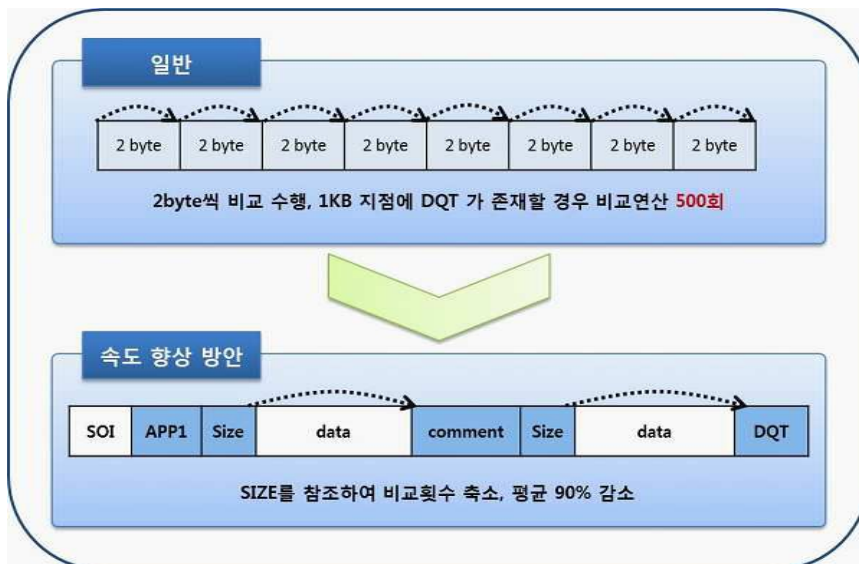
도면4



도면5



도면6



도면7

