



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0025880
(43) 공개일자 2024년02월27일

(51) 국제특허분류(Int. Cl.)

H04N 19/46 (2014.01) G06V 40/16 (2022.01)
H04N 19/119 (2014.01) H04N 19/13 (2014.01)
H04N 19/167 (2014.01) H04N 19/20 (2014.01)
H04N 19/50 (2014.01) H04N 19/625 (2014.01)
H04N 19/70 (2014.01)

(52) CPC특허분류

H04N 19/46 (2015.01)
G06V 40/161 (2022.01)

(21) 출원번호 10-2022-0104051

(22) 출원일자 2022년08월19일

심사청구일자 2022년08월19일

(71) 출원인

세종대학교산학협력단

서울특별시 광진구 능동로 209 (군자동, 세종대학교)

(72) 발명자

김영갑

서울특별시 광진구 능동로 209, 대양AI센터 701호(군자동)

유진용

서울특별시 광진구 능동로 209, 대양AI센터 732호(군자동)

(74) 대리인

양성보

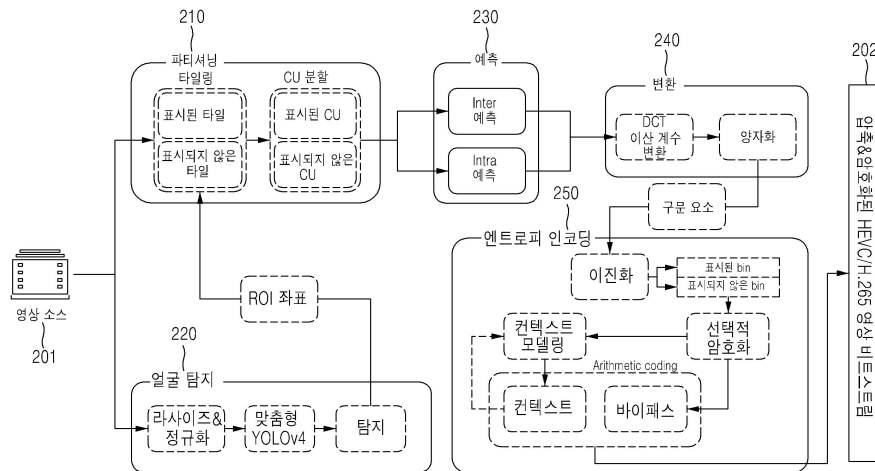
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 코딩 유닛 기반 HEVC/H.265 영상에서의 관심 영역 암호화 방법 및 장치

(57) 요약

코딩 유닛 기반 HEVC/H.265 영상에서의 관심 영역 암호화 방법 및 장치가 개시된다. 일 실시예에 따른 암호화 장치에 의해 수행되는 영상에서의 관심 영역 암호화 방법은, 영상을 구성하는 프레임들을 타일로 분할함에 따라 각 프레임마다 생성된 관심 영역과 관련된 코딩 유닛을 식별하는 단계; 및 상기 식별된 코딩 유닛에 대한 선택적 암호화를 수행하는 단계를 포함할 수 있다.

대표도



(52) CPC특허분류

H04N 19/119 (2015.01)

H04N 19/13 (2015.01)

H04N 19/167 (2015.01)

H04N 19/20 (2015.01)

H04N 19/50 (2015.01)

H04N 19/625 (2015.01)

H04N 19/70 (2015.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152582
과제번호	2019-0-00231-004
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(정진기금)
연구과제명	공공 인프라 안전을 위한 인공지능 기반 영상보안 기술 및 시스템 개발
기 여 율	1/1
과제수행기관명	세종대학교 산학협력단
연구기간	2022.01.01 ~ 2022.12.31

명세서

청구범위

청구항 1

암호화 장치에 의해 수행되는 영상에서의 관심 영역 암호화 방법에 있어서,

영상을 구성하는 프레임들을 타일로 분할함에 따라 각 프레임마다 생성된 관심 영역과 관련된 코딩 유닛을 식별하는 단계; 및

상기 식별된 코딩 유닛에 대한 선택적 암호화를 수행하는 단계;

를 포함하는 관심 영역 암호화 방법.

청구항 2

제1항에 있어서,

상기 코딩 유닛을 식별하는 단계는,

객체 탐지 모델을 이용하여 상기 영상으로부터 관심 영역을 탐지하고, 상기 탐지된 관심 영역의 좌표 데이터를 획득하는 단계

를 포함하는 관심 영역 암호화 방법.

청구항 3

제2항에 있어서,

상기 코딩 유닛을 식별하는 단계는,

상기 획득된 관심 영역의 좌표 데이터에 기초하여 상기 관심 영역과 관련있는 타일과 상기 관심 영역과 관련이 없는 타일을 구분하여 표시하는 단계

를 포함하는 관심 영역 암호화 방법.

청구항 4

제2항에 있어서,

상기 코딩 유닛을 식별하는 단계는,

상기 획득된 관심 영역의 좌표 데이터에 기초하여 상기 관심 영역과 관련 있는 코딩 유닛과 상기 관심 영역과 관련이 없는 코딩 유닛을 구분하여 표시하는 단계

를 포함하는 관심 영역 암호화 방법.

청구항 5

제2항에 있어서,

상기 객체 탐지 모델은,

YOLOv4 객체 탐지 알고리즘을 기반으로 객체 탐지를 위한 학습 데이터를 이용하여 객체로서 얼굴을 탐지하도록 학습된 것을 특징으로 하는 관심 영역 암호화 방법.

청구항 6

제1항에 있어서,

상기 코딩 유닛을 식별하는 단계는,

상기 식별된 코딩 유닛에 대한 인트라(intra) 예측 또는 인터(inter) 예측을 통해 상기 식별된 코딩 유닛으로부

터 적어도 하나 이상의 예측 유닛으로 분할하는 단계를 포함하는 관심 영역 암호화 방법.

청구항 7

제6항에 있어서,
상기 코딩 유닛을 식별하는 단계는,
상기 식별된 코딩 유닛에 대해 이산 계수 변환(DCT; discrete coefficient transform) 및 양자화를 거쳐 엔트로피 인코딩을 수행하는 단계를 포함하는 관심 영역 암호화 방법.

청구항 8

제1항에 있어서,
상기 선택적 암호화를 수행하는 단계는,
상기 식별된 코딩 유닛에 대한 엔트로피 인코딩 과정 중에 적응적 산술 부호화 기반으로 선택적 암호화를 수행하는 단계를 포함하는 관심 영역 암호화 방법.

청구항 9

제8항에 있어서,
상기 선택적 암호화를 수행하는 단계는,
상기 식별된 코딩 유닛에 기초하여 코텍의 파라미터들에 대한 적응형 산술 부호화(CABAC; context-adaptive binary arithmetic coding)를 기반으로 선택적 암호화를 수행하는 단계를 포함하는 관심 영역 암호화 방법.

청구항 10

제9항에 있어서,
상기 코텍은, HEVC/H.264인 것을 특징으로 하는 관심 영역 암호화 방법.

청구항 11

제9항에 있어서,
상기 선택적 암호화를 수행하는 단계는,
상기 코텍의 파라미터들에 대응하는 구문 요소에 대한 선택적 암호화를 수행하고, 상기 수행된 선택적 암호화를 통해 압축 및 암호화된 영상 비트스트림을 도출하는 단계를 포함하는 관심 영역 암호화 방법.

청구항 12

제11항에 있어서,
상기 구문 요소는,
비이진화된 구문 요소에 대하여 이진화를 통해 bin 으로 변환하고, 상기 변환된 bin 중 코딩 유닛에 대응하는 bin의 접미사 부분에 대해서 암호화가 수행되는 것을 특징으로 하는 관심 영역 암호화 방법.

청구항 13

제1항에 있어서,

상기 코딩 유닛을 식별하는 단계는, 코딩 트리 유닛(CTU; coding tree unit) 수준에서 암호화 전파를 제한하는 단계

를 포함하는 관심 영역 암호화 방법.

청구항 14

제1항 내지 제13항 중 어느 한 항의 관심 영역 암호화 방법을 상기 암호화 장치에 실행시키기 위해 비-일시적인 컴퓨터 판독가능한 기록 매체에 저장되는 컴퓨터 프로그램.

청구항 15

암호화 장치에 있어서,

영상을 구성하는 프레임들을 타일로 분할함에 따라 각 프레임마다 생성된 관심 영역과 관련된 코딩 유닛을 식별하는 코딩 유닛 식별부; 및

상기 식별된 코딩 유닛에 대한 선택적 암호화를 수행하는 선택적 암호화부;

를 포함하는 암호화 장치.

발명의 설명

기술 분야

[0001]

아래의 설명은 영상의 암호화 기술에 관한 것이다.

배경 기술

[0003]

기존의 HEVC/H.265에서의 관심 영역(ROI; region of interest) 암호화는 대부분이 HEVC/H.265에서 제공하는 기능 중 하나인 타일(Tile)을 기반으로 수행한다. 이는 관심 영역과 공통 영역을 가지는 모든 타일에 대하여 암호화를 수행하는 것으로, 실제 탐지된 관심 영역보다 넓은 영역을 암호화한다. 영상 도메인에서 관심 영역 암호화의 이점은 사용자가 지정한 영역에 대해서만 암호화 알고리즘을 적용하여 계산의 복잡도를 줄이고 암호화 속도를 향상하는 것인데, 타일 기반의 관심 영역 암호화는 이러한 이점을 얻기 힘들다. 또한, 보존되어야 할 관심 영역의 주변까지 불규칙하게 암호화되기 때문에 암호화된 영상을 활용할 수 있는 도메인이 국한된다. 이러한 문제가 발생하는 주된 이유는 HEVC/H.265가 AVC/H.264와 다르게 독립적으로 처리될 수 있는 영역을 지정하기 어렵기 때문이다. 인코딩 및 디코딩의 특성상, 사용자가 지정한 범위에만 암호화를 적용하더라도 암호화 효과가 주변 픽셀에까지 영향을 끼치는 암호화 전파(encryption propagation)가 일어나기 때문에 영상 도메인에서 관심 영역 암호화를 수행하기 위해서는 독립된 영역이 필요하다. 그러나 HEVC/H.265가 매 프레임마다 서로 다른 크기의 영상처리유닛(CU; coding unit)으로 분할되어 독립된 영역을 지정하기 어려우며 독립된 영역을 지정한다고 하더라도 압축 성능이 크게 저하된다. 이에 따라 HEVC/H.265와 AVC/H.264에서의 관심 영역 암호화는 도 1과 같이 암호화된 영역의 차이가 나타난다.

발명의 내용

해결하려는 과제

[0005]

영상을 구성하는 프레임들을 타일로 분할함에 따라 각 프레임마다 생성된 관심 영역과 관련된 코딩 유닛을 식별하고, 식별된 코딩 유닛에 대한 선택적 암호화를 수행하는 방법 및 장치를 제공할 수 있다.

[0006]

선택적 암호화가 수행된 코딩 유닛을 통해 암호화된 관심 영역의 암호화 전파를 제한하는 방법 및 장치를 제공할 수 있다.

과제의 해결 수단

- [0008] 암호화 장치에 의해 수행되는 영상에서의 관심 영역 암호화 방법은, 영상을 구성하는 프레임들을 타일로 분할함에 따라 각 프레임마다 생성된 관심 영역과 관련된 코딩 유닛을 식별하는 단계; 및 상기 식별된 코딩 유닛에 대한 선택적 암호화를 수행하는 단계를 포함할 수 있다.
- [0009] 상기 코딩 유닛을 식별하는 단계는, 객체 탐지 모델을 이용하여 상기 영상으로부터 관심 영역을 탐지하고, 상기 탐지된 관심 영역의 좌표 데이터를 획득하는 단계를 포함할 수 있다.
- [0010] 상기 코딩 유닛을 식별하는 단계는, 상기 획득된 관심 영역의 좌표 데이터에 기초하여 상기 관심 영역과 관련있는 타일과 상기 관심 영역과 관련이 없는 타일을 구분하여 표시하는 단계를 포함할 수 있다.
- [0011] 상기 코딩 유닛을 식별하는 단계는, 상기 획득된 관심 영역의 좌표 데이터에 기초하여 상기 관심 영역과 관련있는 코딩 유닛과 상기 관심 영역과 관련이 없는 코딩 유닛을 구분하여 표시하는 단계를 포함할 수 있다.
- [0012] 상기 객체 탐지 모델은, YOLOv4 객체 탐지 알고리즘을 기반으로 객체 탐지를 위한 학습 데이터를 이용하여 객체로서 얼굴을 탐지하도록 학습된 것일 수 있다.
- [0013] 상기 코딩 유닛을 식별하는 단계는, 상기 식별된 코딩 유닛에 대한 인트라(intra) 예측 또는 인터(inter) 예측을 통해 상기 식별된 코딩 유닛으로부터 적어도 하나 이상의 예측 유닛으로 분할하는 단계를 포함할 수 있다.
- [0014] 상기 코딩 유닛을 식별하는 단계는, 상기 식별된 코딩 유닛에 대해 이산 계수 변환(DCT; discrete coefficient transform) 및 양자화를 거쳐 엔트로피 인코딩을 수행하는 단계를 포함할 수 있다.
- [0015] 상기 선택적 암호화를 수행하는 단계는, 상기 식별된 코딩 유닛에 대한 엔트로피 인코딩 과정 중에 적응적 산술 부호화 기반으로 선택적 암호화를 수행하는 단계를 포함할 수 있다.
- [0016] 상기 선택적 암호화를 수행하는 단계는, 상기 식별된 코딩 유닛에 기초하여 코텍의 파라미터들에 대한 적응형 산술 부호화(CABAC; context-adaptive binary arithmetic coding)를 기반으로 선택적 암호화를 수행하는 단계를 포함할 수 있다.
- [0017] 상기 코텍은, HEVC/H.264인 것일 수 있다.
- [0018] 상기 선택적 암호화를 수행하는 단계는, 상기 코텍의 파라미터들에 대응하는 구문 요소에 대한 선택적 암호화를 수행하고, 상기 수행된 선택적 암호화를 통해 압축 및 암호화된 영상 비트스트림을 도출하는 단계를 포함할 수 있다.
- [0019] 상기 구문 요소는, 비이진화된 구문 요소에 대하여 이진화를 통해 bin 으로 변환하고, 상기 변환된 bin 중 코딩 유닛에 대응하는 bin의 접미사 부분에 대해서 암호화가 수행되는 것일 수 있다.
- [0020] 상기 코딩 유닛을 식별하는 단계는, 코딩 트리 유닛(CTU; coding tree unit) 수준에서 암호화 전파를 제한하는 단계를 포함할 수 있다.
- [0021] 관심 영역 암호화 방법을 상기 암호화 장치에 실행시키기 위해 비-일시적인 컴퓨터 판독가능한 기록 매체에 저장되는 컴퓨터 프로그램을 포함할 수 있다.
- [0022] 암호화 장치는, 영상을 구성하는 프레임들을 타일로 분할함에 따라 각 프레임마다 생성된 관심 영역과 관련된 코딩 유닛을 식별하는 코딩 유닛 식별부; 및 상기 식별된 코딩 유닛에 대한 선택적 암호화를 수행하는 선택적 암호화부를 포함할 수 있다.

발명의 효과

- [0024] 탐지된 객체의 좌표를 기반으로 암호화를 수행하는 경량적인 방법을 채택하여 AVC/H.264에서와 같이 독립적인 영역을 지정하기 위해 FMO(flexible macroblock ordering)과 같은 도구를 사용하지 않아도 된다.
- [0025] 또한, 탐지된 관심 영역에 대하여 유사한 암호화 성능(즉, PSNR; peak signal to noise ratio, SSIM; structural similarity index measure)을 나타내면서 전체적인 암호화 속도를 개선할 수 있다.

[0026] 이와 관련하여 CTU수준에서 암호화 전과를 제한함으로써 영상에 대한 암호화 비율(ER; encryption ratio) 및 IOU(intersection over union)가 개선되고 암호화된 관심 영역 주변의 원본 이미지를 보존할 수 있다.

도면의 간단한 설명

[0028] 도 1은 AVC/H.264 및 HEVC/H.265에서의 관심 영역 암호화 차이를 나타낸 도면이다.
 도 2는 일 실시예에 있어서, 코딩 유닛 기반 관심 영역 암호화 동작을 설명하기 위한 도면이다.
 도 3은 일 실시예에 있어서, 암호화 장치의 구성을 설명하기 위한 블록도이다.
 도 4는 일 실시예에 있어서, 관심 영역 암호화 방법을 설명하기 위한 흐름도이다.
 도 5는 일 실시예에 있어서, 관심 영역과 코딩 유닛 간의 관계 유형을 설명하기 위한 도면이다.
 도 6은 일 실시예에 있어서, 적응적 산술 부호화 기반 선택적 구문 요소를 암호화하는 동작을 설명하기 위한 도면이다.
 도 7은 일 실시예에 있어서, 참조 영역 제한 범위에 따른 디코딩된 영상을 나타낸 도면이다.
 도 8은 일 실시예에 있어서, 타일 기반 관심 영역 암호화와 코딩 유닛 기반 관심 영역 암호화를 비교한 결과를 나타낸 도면이다.
 도 9는 일 실시예에 있어서, 타일 기반 관심 영역 암호화, 코딩 유닛 기반 관심 영역 암호화, ground truth에 대한 암호화 비율 및 IOU 비교 결과를 나타낸 그래프이다.
 도 10은 일 실시예에 있어서, 전체 프레임 암호화, 타일 기반 관심 영역 암호화, 코딩 유닛 기반 관심 영역 암호화에 대한 암호화 속도를 나타낸 그래프이다.

발명을 실시하기 위한 구체적인 내용

[0029] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0031] 도 3은 일 실시예에 있어서, 암호화 장치의 구성을 설명하기 위한 블록도이고, 도 4는 일 실시예에 있어서, 관심 영역 암호화 방법을 설명하기 위한 흐름도이다.

[0032] 암호화 장치(100)의 프로세서는 코딩 유닛 식별부(310) 및 선택적 암호화부(320)를 포함할 수 있다. 이러한 프로세서의 구성요소들은 암호화 장치에 저장된 프로그램 코드가 제공하는 제어 명령에 따라 프로세서에 의해 수행되는 서로 다른 기능들(different functions)의 표현들일 수 있다. 프로세서 및 프로세서의 구성요소들은 도 4의 관심 영역 암호화 방법이 포함하는 단계들(410 내지 420)을 수행하도록 암호화 장치를 제어할 수 있다. 이때, 프로세서 및 프로세서의 구성요소들은 메모리가 포함하는 운영체제의 코드와 적어도 하나의 프로그램의 코드에 따른 명령(instruction)을 실행하도록 구현될 수 있다.

[0033] 프로세서는 관심 영역 암호화 방법을 위한 프로그램의 파일에 저장된 프로그램 코드를 메모리에 로드할 수 있다. 예를 들면, 암호화 장치에서 프로그램이 실행되면, 프로세서는 운영체제의 제어에 따라 프로그램의 파일로부터 프로그램 코드를 메모리에 로드하도록 암호화 장치를 제어할 수 있다. 이때, 프로세서의 코딩 유닛 식별부(310) 및 선택적 암호화부(320)의 각각은 메모리에 로드된 프로그램 코드 중 대응하는 부분의 명령을 실행하여 이후 단계들(410 내지 430)을 실행하기 위한 프로세서의 서로 다른 기능적 표현들일 수 있다.

[0034] 단계(410)에서 코딩 유닛 식별부(310)는 영상을 구성하는 프레임들을 타일로 분할함에 따라 각 프레임마다 생성된 관심 영역과 관련된 코딩 유닛을 식별할 수 있다. 코딩 유닛 식별부(310)는 객체 탐지 모델을 이용하여 영상으로부터 관심 영역을 탐지하고, 탐지된 관심 영역의 좌표 데이터를 획득할 수 있다. 코딩 유닛 식별부(310)는 획득된 관심 영역의 좌표 데이터에 기초하여 관심 영역과 관련있는 타일과 관심 영역과 관련이 없는 타일을 구분하여 표시할 수 있다. 코딩 유닛 식별부(310)는 획득된 관심 영역의 좌표 데이터에 기초하여 관심 영역과 관련 있는 코딩 유닛과 관심 영역과 관련이 없는 코딩 유닛을 구분하여 표시할 수 있다. 코딩 유닛 식별부(310)는 식별된 코딩 유닛에 대한 인트라(intra) 예측 또는 인터(inter) 예측을 통해 식별된 코딩 유닛으로부터 적어도 하나 이상의 예측 유닛으로 분할할 수 있다. 코딩 유닛 식별부(310)는 식별된 코딩 유닛에 대해 이산

계수 변환(DCT; discrete coefficient transform) 및 양자화를 거쳐 엔트로피 인코딩을 수행할 수 있다. 또한, 코딩 유닛 식별부(310)는 코딩 트리 유닛(CTU; coding tree unit) 수준에서 암호화 전파를 제한할 수 있다.

[0035] 단계(420)에서 선택적 암호화부(320)는 식별된 코딩 유닛에 대한 선택적 암호화를 수행할 수 있다. 선택적 암호화부(320)는 식별된 코딩 유닛에 대한 엔트로피 인코딩 과정 중에 적응적 산술 부호화 기반으로 선택적 암호화를 수행할 수 있다. 선택적 암호화부(320)는 식별된 코딩 유닛에 기초하여 코덱의 파라미터들에 대한 적응형 산술 부호화(CABAC; context-adaptive binary arithmetic coding)를 기반으로 선택적 암호화를 수행할 수 있다. 선택적 암호화부(320)는 코덱의 파라미터들에 대응하는 구문 요소에 대한 선택적 암호화를 수행할 수 있다. 선택적 암호화부(320)는 코덱의 파라미터들에 대응하는 구문 요소에 대한 선택적 암호화를 수행함에 따라 압축 및 암호화된 영상 비트스트림을 도출할 수 있다.

[0036] 이하에서는, 도 2를 통해 코딩 유닛 기반 HEVC/H.265 영상에서의 관심 영역 암호화 동작에 대하여 보다 상세하게 설명하기로 한다.

[0037] 암호화 장치는 객체 탐지 모델을 이용하여 영상 소스(201)로부터 관심 영역을 탐지하고, 탐지된 관심 영역의 좌표를 획득할 수 있다. 예를 들면, 암호화 장치는 객체 탐지 모델을 이용하여 영상 소스(201)로부터 객체를 탐지하고, 탐지된 객체를 포함하는 관심 영역의 좌표 데이터를 획득할 수 있다. 실시예에서는 관심 영역을 얼굴이라고 가정하여 설명하기로 한다. 일반적으로, 사람의 얼굴에 다양한 식별 정보가 나타나기 때문에 개인 정보 보호를 위한 관심 영역으로 많이 선택된다. 암호화 장치는 관심 영역을 탐지하기 위해 실시간 객체 탐지가 가능한 얼굴 탐지 모델로 YOLOv4를 채택할 수 있다. 그러나, 기존의 학습 데이터로 얼굴을 탐지할 수 없어, "WIDER FACE" 데이터를 활용하여 얼굴을 학습시키고 얼굴을 탐지하기 위한 맞춤형 YOLOv4를 생성할 수 있다. 암호화 장치는 맞춤형 YOLOv4를 통해 얼굴을 탐지하고, 탐지된 얼굴(관심 영역)을 포함하는 경계(boundary)와 좌표 데이터를 표시할 수 있다. 암호화 장치는 추출된 관심 영역(ROI)의 좌표 데이터를 파티셔닝(210) 단계에 전달할 수 있다.

[0038] 암호화 장치는 파티셔닝(210) 단계에서 수신된 관심 영역의 좌표 데이터에 기초하여 관심 영역의 좌표 데이터를 포함하는 타일(표시된 타일)과 관심 영역의 좌표 데이터를 포함하지 않는 타일(표시되지 않은 타일)의 분류할 수 있다. 마찬가지로, 암호화 장치는 수신된 관심 영역의 좌표 데이터에 기초하여 관심 영역의 좌표 데이터를 포함하는 코딩 유닛(표시된 코딩 유닛)과 관심 영역의 좌표 데이터를 포함하지 않는 코딩 유닛(표시되지 않은 코딩 유닛)으로 분류할 수 있다. 이를 통해 암호화 알고리즘이 적용될 코딩 유닛과 적용되지 않을 코딩 유닛이 분류될 수 있다.

[0039] 암호화 장치는 각 코딩 유닛을 적어도 하나 이상의 예측 유닛(PU; prediction unit)으로 분할할 수 있고, 예측(230) 단계에서 인트라(intra) 또는 인터(inter) 예측을 통해 예측 유닛값을 획득할 수 있다. 암호화 장치는 디코딩 예측 과정에서 지정된 관심 영역 밖의 픽셀이 복사되지 않고 암호화된 영역을 참조하는 작업이 수행되지 않도록 예측을 제한해야 한다. 이는, 예측 작업이 전체 처리 단위(예를 들면, 타일, 프레임)에 영향을 미치기 때문에 작은 영역에 암호화를 적용하더라도 이미지 전체에 암호화 전파가 발생할 수 있기 때문이다.

[0040] 암호화 장치는 변환(240) 단계에서 이산 계수 변환(DCT; discrete coefficient transform) 및 양자화를 거쳐 엔트로피 인코딩(250) 단계를 수행할 수 있다. 암호화 장치는 엔트로피 인코딩(250) 단계에서 이전 단계에서 변환된 구문 요소(syntax elements) 중 시각적으로 영향을 많이 끼치는 일부(motion vector(MV), MV sign, transform coefficient(TC), TC sign, intra prediction mode(IPM))를 선택적으로 암호화하여 압축 및 암호화된 HEVC/H.265 영상 비트스트림(202)을 도출할 수 있다.

[0041] 도 5를 참고하면, 관심 영역과 코딩 유닛 간의 관계 유형을 설명하기 위한 도면이다. 암호화 장치는 관심 영역과 관련이 있는 코딩 유닛만을 암호화하여 암호화 영역을 줄일 수 있다. 암호화 장치는 파티셔닝 과정에서 관심 영역과 관련된 코딩 유닛을 식별할 수 있다. 파티셔닝 과정에서 식별된 코딩 유닛이 표시될 수 있으며, 이후, 암호화 장치는 관심 영역과 관련없는 코딩 유닛과 관심 영역과 관련있는 코딩 유닛을 구별할 수 있다. 암호화 장치는 2차원에서 두 개의 직사각형 공통 영역이 존재하는지 여부에 따라 코딩 유닛을 식별할 수 있다. 암호화 장치는 탐지된 객체를 포함하는 관심 영역의 좌표 데이터를 기반으로 관심 영역과 상관 관계가 있는 코딩 유닛을 식별할 수 있다.

[0042] 도 5(a)는 두 관심 영역과 코딩 유닛의 관계를 나타낸 것이고, 도 5(b)는 두 관심 영역과 코딩 유닛이 관계가 없을 때의 유형을 나타낸 것이다. 관심 영역과 코딩 유닛이 관계가 없을 때에 대하여 중점적으로 분석될 수 있

으며, 관심 영역과 코딩 유닛이 관계가 없을 때의 유형을 4가지로 분류될 수 있다.

[0043] 코딩 유닛의 좌측상단 좌표(절대 좌표)를 (CU_x , CU_y)라 하고, 각 코딩 유닛의 너비를 CU_{width} 라고 할 때, 오른쪽 하단 모서리의 좌표는 ($CU_x + CU_{width}$, $CU_y + CU_{width}$)이다. 관심 영역의 좌측상단 좌표를 (ROI_x , ROI_y)라 하고, 너비와 높이를 w 와 h 로 가정할 때, 오른쪽 하단 모서리의 좌표는 ($ROI_x + w$, $ROI_y + h$)이다. 코딩 유닛과 관심 영역이 관계없는 4가지의 조건은 다음과 같이 표현될 수 있다.

$$\text{Case 1:} \quad ROI_y \geq CU_y + CU_{width} \quad (1)$$

$$\text{Case 2:} \quad ROI_x + w \leq CU_x \quad (2)$$

$$\text{Case 3:} \quad ROI_x > CU_x + CU_{width} \quad (3)$$

$$\text{Case 4:} \quad ROI_y + h < CU_y \quad (4)$$

[0044]

[0045] 위 조건(case)을 만족하는 경우, 암호화 장치는 코딩 유닛과 관심 영역이 관련이 없는 것으로 판단하여 암호화를 적용하지 않는 코딩 유닛으로 식별하고, 위 조건을 만족하지 않는 경우, 코딩 유닛과 관심 영역이 관련이 있는 것으로 판단하여 암호화를 적용해야 하는 코딩 유닛으로 식별할 수 있다.

[0046] 도 6을 참고하면, 적응적 산술 부호화 기반 선택적 구문 요소를 암호화하는 동작을 설명하기 위한 도면이다. 식별된 코딩 유닛은 예측 과정과 변환 과정을 거쳐 엔트로피 인코딩을 수행하는데 표현법이 다소 변화하였더라도 여전히 식별될 수 있어야 한다. 암호화 장치는 식별된 코딩 유닛에 대해 예측과 변환 과정을 거쳐 엔트로피 인코딩을 수행할 수 있다. 암호화 장치는 엔트로피 인코딩 과정 중 적응형 산술 부호화를 기반으로 암호화를 수행하며, 시각적 영향이 큰 HEVC/H.264 파라미터 MV, MV sign, TC, TC sign, IPM와 대응하는 구문 요소만을 선택적으로 암호화를 수행할 수 있다. 암호화하기 앞서, 도 6에 도시된 바와 같이, 암호화 장치는 비이진화된 구문 요소에 대하여 이진화를 통해 식별된 코딩 유닛에 대응하는 bin에 대해서만 암호화를 수행할 수 있다. 비이진 구문 요소는 unary, truncated unary, fixed-length, truncated rice code 및 k^{th} -order exp-Golomb(EG) codes와 같은 이진화 방법을 통해 bin 문자열로 변환될 수 있다. 그런 다음, 암호화 장치는 이진화된 구문 요소 중 식별된 코딩 유닛에 해당하는 bin 문자열에 대해 CABAC bin string 레벨에서 암호화를 수행할 수 있다. AES-CFB는 이진화된 구문 요소의 실시간 암호화를 위해 사용되며 초기 벡터(IV)는 의사 난수 생성기를 통해 설정될 수 있다. 암호화 키를 E_k 라고 하고, 초기 벡터에 의해 생성된 키 스트림 S는 구문 요소 P와의 XOR 연산을 통해 암호화된 구문 요소 C가 생성될 수 있다. 키 스트림은 다음과 같이 생성될 수 있다.

[0047] 수학적 식 1:

$$S_i = E_k(C_{i-1}), i \geq 1$$

[0048]

[0049] 선택된 구문 요소는 암호화로 인한 포맷 준수(format compliance) 문제를 초래해서는 안 된다. 이에 따라, 암호화 장치는 포맷 준수를 해칠 수 있는 일부 구문 요소에 대해서 포맷 준수를 해치지 않도록 접미사(suffix) 부분만을 암호화하여 인코딩을 수행할 수 있다.

[0050] 암호화 장치는 포맷 준수를 보장하고 CABAC의 바이패스 모드를 사용하여 선택한 일부 bin의 접미사(suffix) 부분을 암호화하여 비트 전송률을 유지할 수 있다. 예를 들면, 구문 요소 양자화 TC(QTC)의 암호화 프로세스는 QTC가 truncated rice 코드와 k번째 EG 코드에 의해 이진화되고 부호 비트(TC 부호)와 0이 아닌 QTC 값(TC)을 사용하여 별도로 암호화될 수 있다. 부호 비트는 바이패스 모드로 인코딩되기 전에 암호화될 수 있다. 이 값은 EGO 코드를 사용하여 이진화된 다음 이진 산술 코드로 인코딩하기 전에 암호화될 수 있다. QTC 구문 요소 P(Q) 암호화는 다음과 같다.

[0051] 수학적 식 2:

$$C(Q)_i = P(Q)_i \oplus S_i, i \geq 1$$

[0052]

[0053] 파라미터 MV를 인코딩 및 암호화하는 것은 구문 요소 MV 차이(MVD)를 인코딩 및 암호화하는 것을 의미한다.

MVD는 윤곽선 및 모션과 밀접한 관련이 있기 때문에 시각적 품질에 상당한 영향을 미친다. 따라서, MVD는 높은 암호화 성능을 보인다. 또한, MVD 암호화는 QTC 암호화와 같이 부호 및 값의 암호화를 별도로 수행할 수 있다. MVD 부호는 XOR 계산을 통해 암호화되고 바이패스 모드로 인코딩될 수 있다. MVD 값은 EG1 코드로 이진화되며, 암호화는 접미사 비트 및 키 스트림 S의 XOR 계산에 의해 수행될 수 있다. 그런 다음 바이패스 모드로 인코딩될 수 있다. luma IPM 암호화는 후보 모드 리스트의 수와 키 스트림 S 사이의 XOR 계산을 통해 수행될 수 있다. IPM 암호화로 인해 복호화가 어려울 수 있으므로 계수 스캐닝 모드는 마지막 계수의 위치를 매핑하여 동기화해야 한다. HEVC/H.265에는 5개의 (평면, 수직, 수평, DC 및 해당 luma IPM) 크로마(chroma) IPM이 있다. 일반적으로 크로마 IPM 암호화는 luma IPM 암호화의 영향을 받기 때문에 chroma IPM 리스트의 숫자가 영향을 받지 않는 경우에만 XOR 연산에 의해 암호화될 수 있다.

[0054] 도 7를 참고하면, 참조 영역 제한 범위에 따른 디코딩된 영상을 나타낸 도면이다. 도 7(a)는 타일과 같은 병렬 처리없이 관심 영역과 관련된 코딩 유닛에 암호화 알고리즘을 적용하였을 때 나타나는 영상이고, 도 7(b)는 타일 레벨에서 참조 영역이 제한되었을 때 나타나는 영상이고, 도 7(c)는 CTU 레벨에서 참조 영역이 제한되었을 때 나타나는 영상을 나타낸 것이다.

[0055] 암호화 장치에서 관심 영역과 관련된 코딩 유닛을 식별하고, 식별된 코딩 유닛에 대응하는 bin에만 암호화를 수행할지라도 도 7(a)와 도 7(b)처럼 넓은 영역에 걸쳐 암호화 전파가 나타날 수 있다. 비록, 엔트로피 인코딩 과정에서는 식별된 코딩 유닛에만 암호화를 적용하지만, 디코딩 예측 과정에서 정상적으로 이미지가 생성되어야 하는 영역에서 암호화된 영역을 참조하여 예측하기 때문에 발생하는 문제이다. 따라서, 디코딩 예측 수준에서 관심 영역 이외의 영역들이 암호화된 영역을 참조하지 못하게 해야 하는데, 이는 계산량을 늘리고 프로세스를 복잡하게 만들어 성능을 떨어뜨리기 때문에 인코딩 수준에서 독립된 영역을 설정하여 암호화 전파를 일정 수준에서 제한하는 것이 바람직하다. 이에 따라, 암호화 장치는 코딩 트리 유닛(CTU; coding tree unit) 수준에서 암호화 전파를 제한하여 도 7(c)와 같이 비교적 주변 이미지를 보존할 수 있는 결과를 나타낼 수 있다. 다시 말해서, 암호화 장치는 파티셔닝 단계(210)에서 코딩 트리 유닛(CTU; coding tree unit) 수준에서 암호화 전파를 제한할 수 있다. 일반적으로, HEVC/H.265에서 제공하는 타일의 최소 높이(height)는 128픽셀이나, CTU는 HEVC/H.265에서 제공하는 타일의 최소 높이의 절반인 64픽셀이다. 이에 따라, 따라서 암호화 전파 현상을 보다 세부적으로 제한할 수 있다.

[0056] 실시예에 따르면, 타일에 기반한 기존의 HEVC/H.265에서의 관심 영역 암호화 방법이 탐지된 관심 영역에 비해 지나치게 큰 영역을 암호화하고 리소스 낭비하는 문제를 완화시킬 수 있다.

[0057] 도 8은 일 실시예에 있어서, 타일 기반 관심 영역 암호화와 코딩 유닛 기반 관심 영역 암호화를 비교한 결과를 나타낸 도면이다.

[0058] 실시예에 따른 코딩 유닛 기반 관심 영역 암호화의 성능을 도출하기 위한 실험 환경은 64GB 메인 메모리와 3.90GHz에서 실행되는 64비트 16코어 AMD Threadripper PRO 3955WX이며 Ubuntu 20.04 운영체제이다. HEVC/H.265 인코더로 kvazaar를 기반으로 코딩 유닛 기반 관심 영역 암호화가 구현될 수 있다.

[0059] 도 8에서는 기존 타일 기반 관심 영역의 암호화와 제안된 방법을 비교함으로써 실시예에서 제안된 제안된 방법(코딩 유닛 기반 관심 영역 암호화)의 우수성을 나타낸다. 우선, 도 8에서 볼 수 있듯이 디코딩된 영상에서 기존 방법은 탐지된 관심 영역에 비해 지나치게 큰 범위에 대해 암호화를 수행하고 있는 것을 확인할 수 있다. 반면, 실시예에서 제안된 방법은 탐지된 관심 영역과 유사한 암호화 영역을 나타내면 주변 이미지를 명확히 보존하고 있다. 이와 관련한 구체적인 성능(즉, 암호화 비율, IOU)은 도 9에서 확인할 수 있듯이 코딩 유닛 기반 관심 영역 암호화 방법이 전체 프레임 대비 적은 비율을 암호화하면서 IOU가 ground truth(즉, IOU = 1)에 가깝다는 것을 보여준다. 또한, 관심 영역에 대한 암호화 성능(즉, PSNR, SSIM)이 기존의 방식과 비교하여 유사함을 표 1과 같이 보인다.

[0060] 표 1: 전체 프레임 암호화, 타일 기반 관심 영역 암호화, 코딩 유닛 기반 관심 영역 암호화에 대한 PSNR 및 SSIM 비교

Sequence	Whole-frame encryption		Tile-based ROI encryption		CU-based ROI encryption	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
vidyo 1	9.36	0.21	9.49	0.23	9.29	0.19
vidyo 3	6.42	0.21	6.64	0.22	6.73	0.20
vidyo 4	8.19	0.23	8.26	0.22	8.22	0.24

[0061]

[0062]

마지막으로, 암호화 시간 측면에서도 도 10과 같이 제안된 방법이 기존의 방식보다 우수하다는 것을 확인할 수 있다.

[0063]

이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0064]

소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0065]

실시예에 따른 방법은 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 실시예를 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.

[0066]

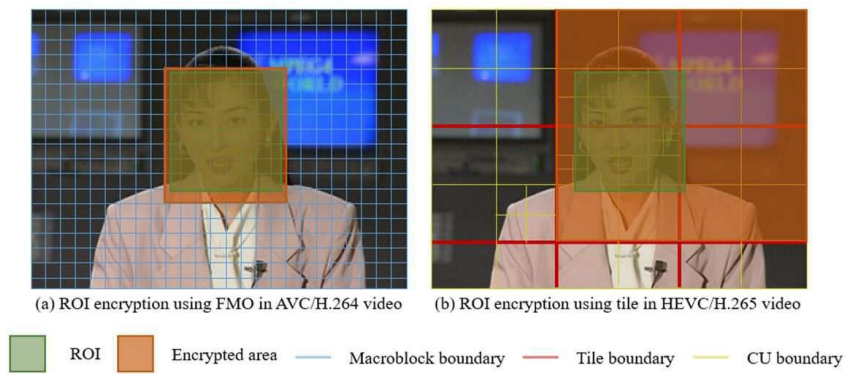
이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0067]

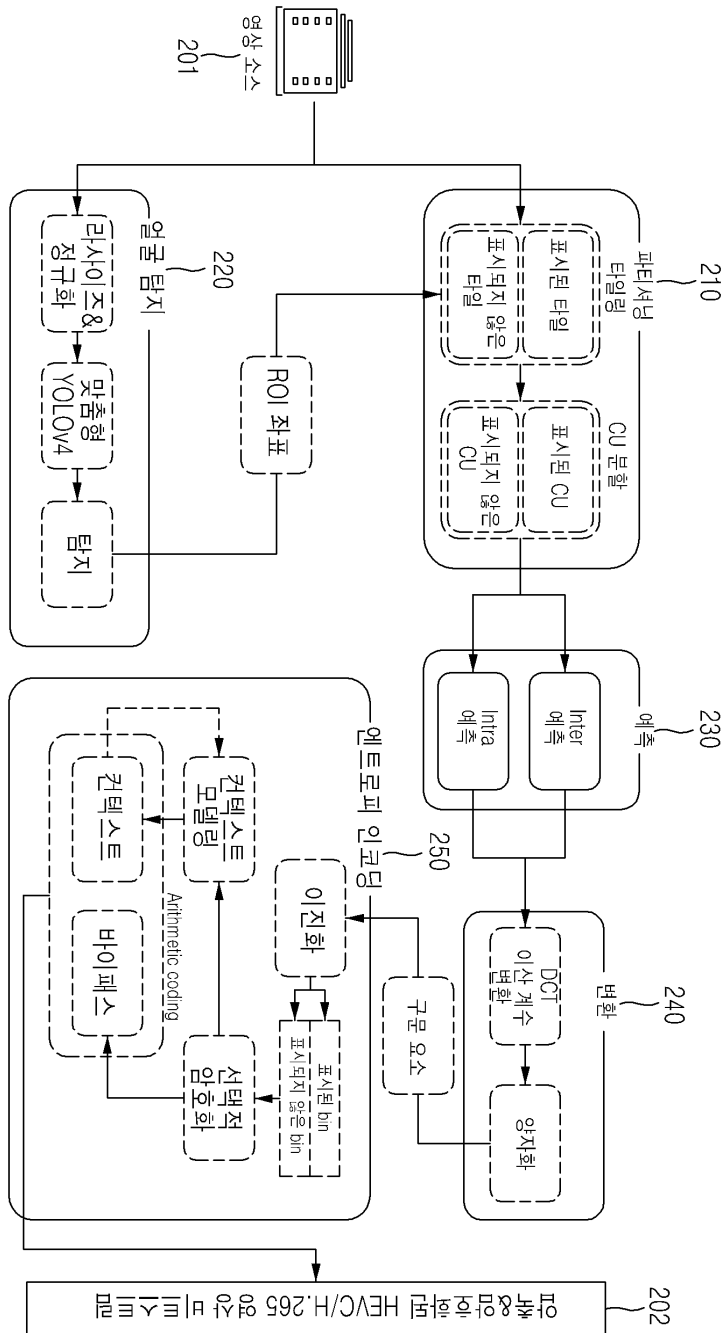
그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

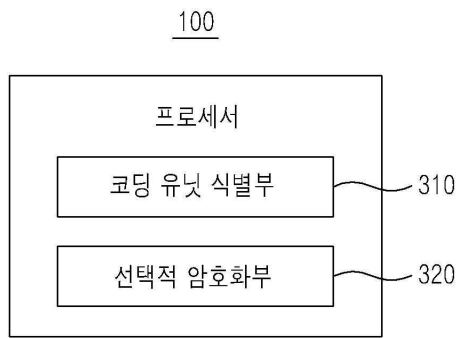
도면1



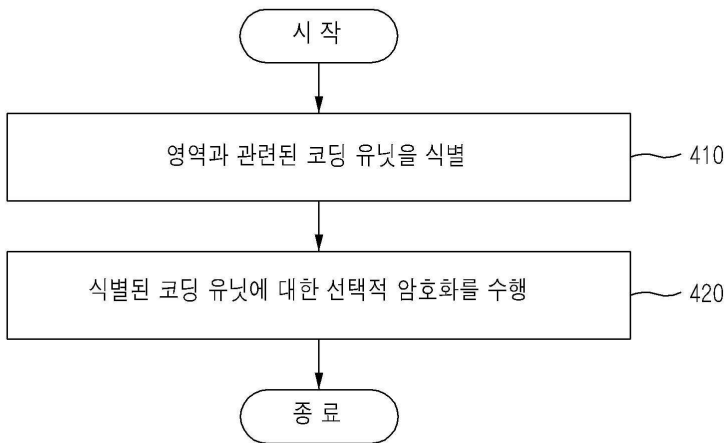
도면2



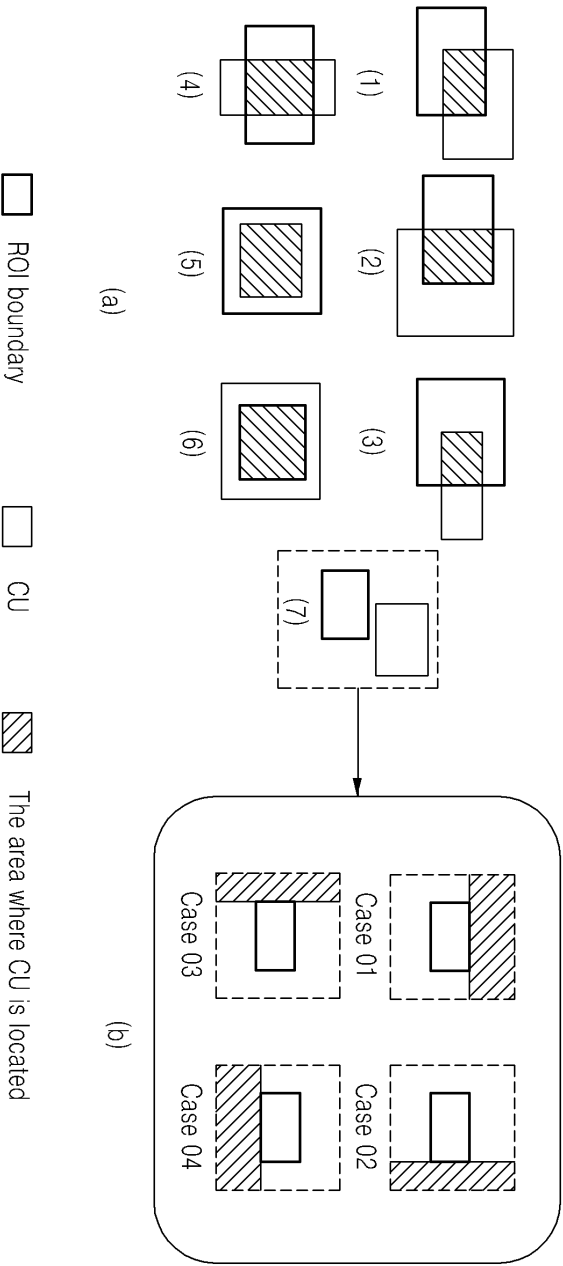
도면3



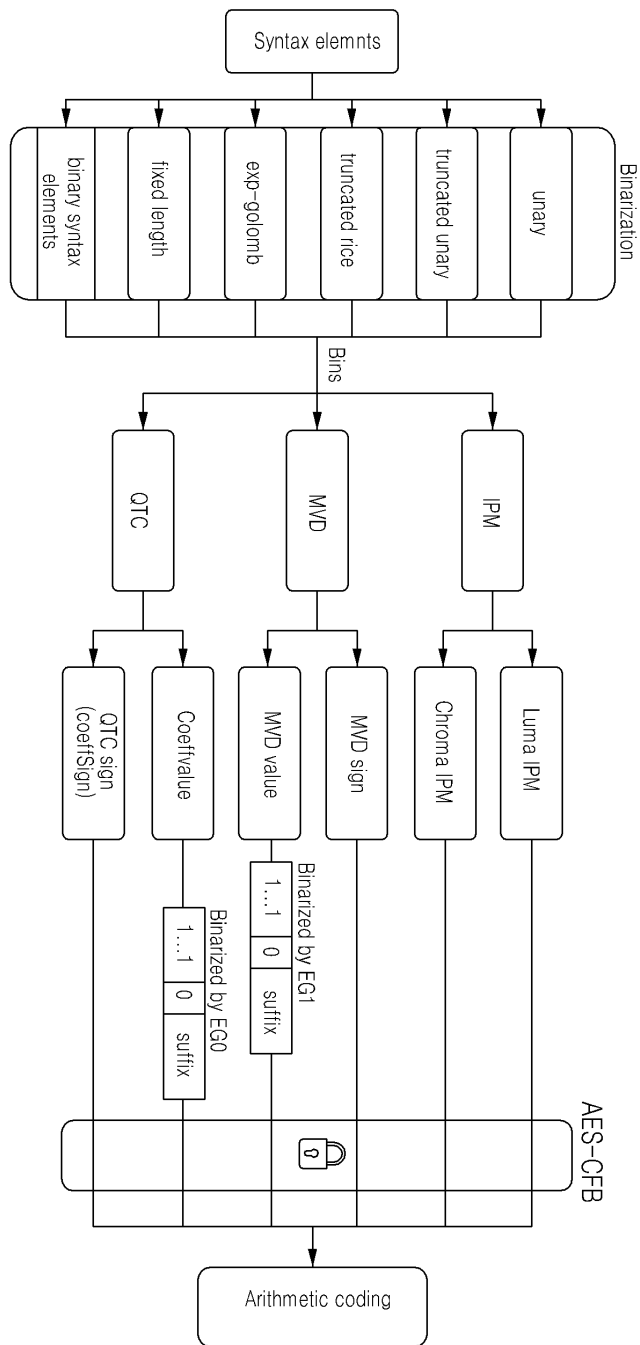
도면4



도면5



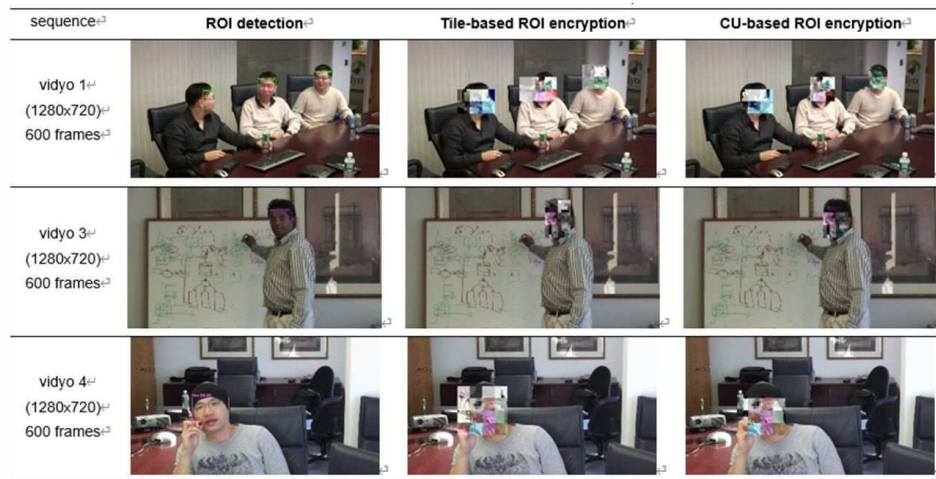
도면6



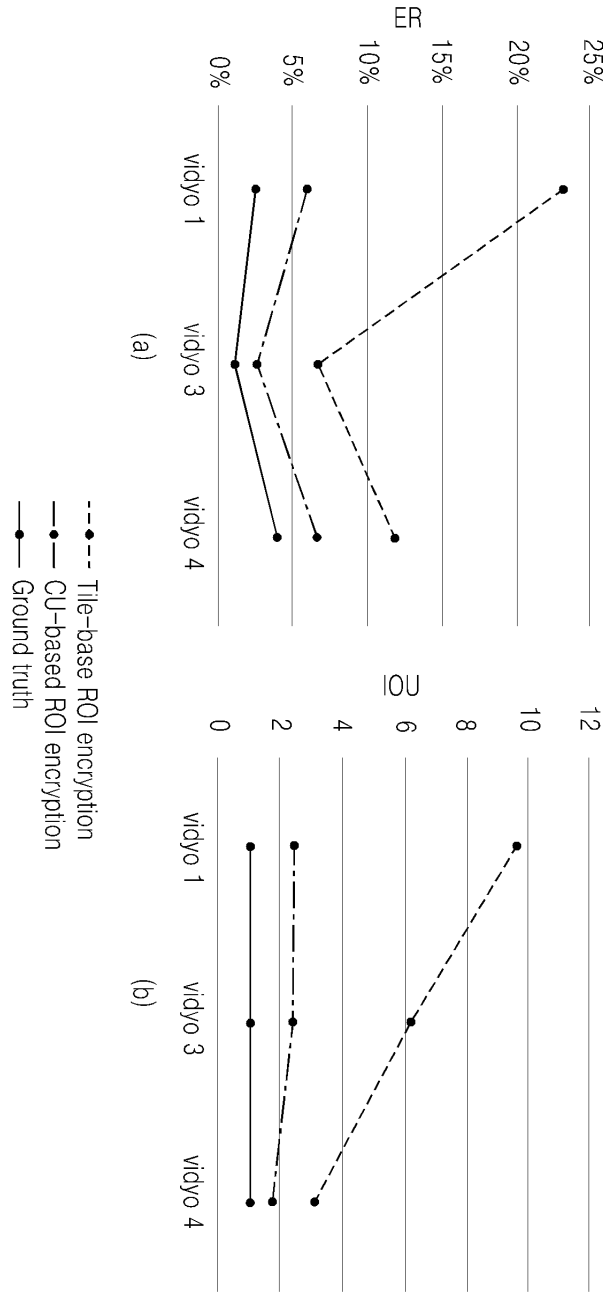
도면7



도면8



도면9



도면10

