

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)(11) 공개번호 10-2023-0086038
(43) 공개일자 2023년06월15일

(51) 국제특허분류(Int. Cl.)

H04N 19/46 (2014.01) H04N 19/176 (2014.01)
H04N 19/85 (2014.01) H04N 21/2347 (2016.01)
H04N 21/266 (2011.01)

(52) CPC특허분류

H04N 19/46 (2015.01)
H04N 19/176 (2015.01)

(21) 출원번호 10-2021-0174309

(22) 출원일자 2021년12월08일

심사청구일자 2021년12월08일

(71) 출원인

조선대학교산학협력단

광주광역시 동구 필문대로 309 (서석동)

(72) 발명자

신석주

광주광역시 남구 제석로 72 101-403

아흐마드 이자즈

광주광역시 동구 필문대로 253번길 21-12

(74) 대리인

김태영

전체 청구항 수 : 총 10 항

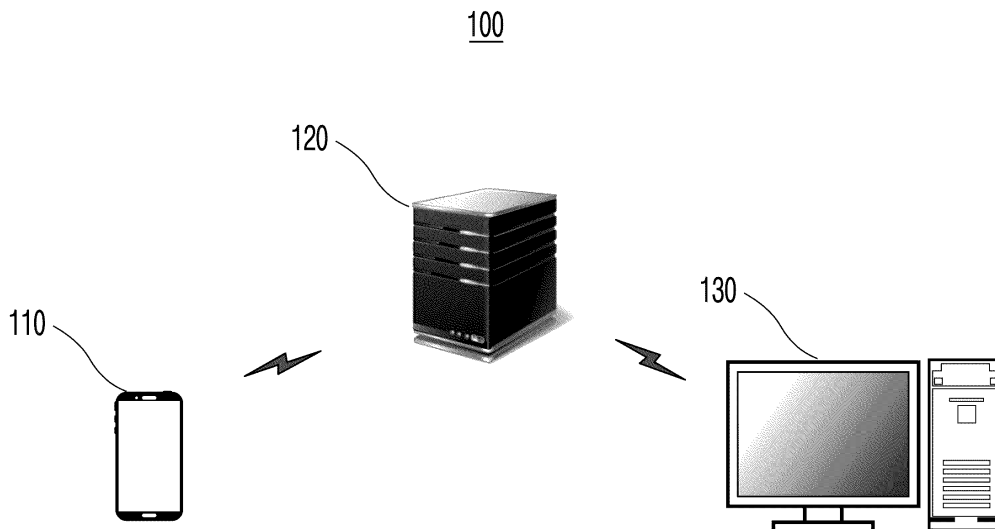
(54) 발명의 명칭 이미지 암호화/압축 장치 및 방법

(57) 요약

이미지 암호화/압축 장치 및 방법을 개시한다.

본 실시예의 일 측면에 의하면, 외부로 전송할 이미지를 암호화한 후 압축하여 전송하는 이미지 암호화/압축 장치에 있어서, 이미지 내 픽셀을 기 설정된 면적의 블록으로 구분하여, 각 블록마다 암호화를 수행하는 암호화부와 상기 암호화부에서 암호화된 이미지를 압축하는 압축부 및 상기 압축부에 의해 압축된 이미지를 외부로 전송하는 통신부를 포함하는 것을 특징으로 하는 이미지 암호화/압축 장치를 제공한다.

대표도 - 도1



(52) CPC특허분류

H04N 19/85 (2015.01)

H04N 21/2347 (2019.01)

H04N 21/26613 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1345342424
과제번호	2018R1D1A1B07048338
부처명	교육부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구
연구과제명	대규모 IoT 환경에서의 초저지연 매체 접속 제어 알고리즘 및 응용 기술 연구
기 여 율	1/1
과제수행기관명	조선대학교
연구기간	2021.03.01 ~ 2022.02.28

명세서

청구범위

청구항 1

외부로 전송할 이미지를 암호화한 후 압축하여 전송하는 이미지 암호화/압축 장치에 있어서,
 이미지 내 픽셀을 기 설정된 면적의 블록으로 구분하여, 각 블록마다 암호화를 수행하는 암호화부;
 상기 암호화부에서 암호화된 이미지를 압축하는 압축부; 및
 상기 압축부에 의해 압축된 이미지를 외부로 전송하는 통신부
 를 포함하는 것을 특징으로 하는 이미지 암호화/압축 장치.

청구항 2

제1항에 있어서,
 상기 암호화부는,
 구분된 각 블록을 무작위로 치환하는 것을 특징으로 하는 이미지 암호화/압축 장치.

청구항 3

제1항에 있어서,
 상기 암호화부는,
 구분된 각 블록을 무작위로 회전시키거나 반전시키는 것을 특징으로 하는 이미지 암호화/압축 장치.

청구항 4

제1항에 있어서,
 상기 암호화부는,
 구분된 각 블록 내 픽셀들의 픽셀값을 반전시키는 것을 특징으로 하는 이미지 암호화/압축 장치.

청구항 5

제1항에 있어서,
 상기 암호화부는,
 비밀키를 생성하여, 생성된 비밀키를 이용하여 암호화를 수행하는 것을 특징으로 하는 이미지 암호화/압축
 장치.

청구항 6

이미지 암호화/압축 장치가 외부로 전송할 이미지를 암호화하여 압축하는 방법에 있어서,
 이미지 내 픽셀들을 기 설정된 면적의 블록으로 구분하는 구분과정;
 상기 구분과정에 의해 구분된 각 블록을 무작위로 치환하는 치환과정;
 상기 구분과정에 의해 구분된 각 블록을 무작위로 회전하거나 반전시키는 회전과정; 및
 상기 구분과정에 의해 구분된 각 블록 내 픽셀의 픽셀값을 반전시키는 반전과정
 을 포함하는 것을 특징으로 하는 이미지 암호화/압축 방법.

청구항 7

제6항에 있어서,
상기 치환과정, 회전과정 및 반전과정은,
생성된 비밀키를 이용하여 진행되는 것을 특징으로 하는 이미지 암호화/압축 방법.

청구항 8

제7항에 있어서,
상기 치환과정, 회전과정 및 반전과정은,
서로 다른 비밀키에 의해 진행되는 것을 특징으로 하는 이미지 암호화/압축 방법.

청구항 9

제6항에 있어서,
상기 반전과정을 거친 이미지를 압축하는 압축과정을 더 포함하는 것을 특징으로 하는 이미지 암호화/압축 방법.

청구항 10

제0항에 있어서,
상기 압축과정을 거친 이미지를 외부로 전송하는 전송과정을 더 포함하는 것을 특징으로 하는 이미지 암호화/압축 방법.

발명의 설명

기술 분야

[0001] 본 발명은 이미지를 외부로 전송함에 있어 보안을 위해 암호화한 후 압축하는 장치 및 방법에 관한 것이다.

배경 기술

[0002] 이 부분에 기술된 내용은 단순히 본 실시예에 대한 배경 정보를 제공할 뿐 종래기술을 구성하는 것은 아니다.

[0003] 정보의 안전하고 효율적인 전송 및 저장을 위해, 근래의 통신 시스템은 암호화(Encryption)와 압축(Compression) 모두를 요구하고 있다. 이에, 종래의 대부분의 경우에는 데이터가 먼저 압축된 다음 암호화가 진행되어 왔다.

[0004] 다만, 이미지의 경우에는 종래와 같이 압축이 진행된 후 암호화가 진행될 경우 문제가 발생해왔다. 이미지에 압축이 진행되는 경우 품질저하가 발생할 가능성이 존재한다. 압축이 우선하여 진행하며 이미지의 품질저하가 발생한 후 추가적으로 암호화가 진행될 경우, 품질저하된 이미지에 추가적인 암호화가 진행된다. 이에, 추후, (복호화 등을 거쳐) 복원된 이미지의 품질에 심각한 손상이 발생할 가능성이 존재한다.

[0005] 이러한 문제로 인해, 이미지와 같이 압축에 있어 품질 저하가 발생할 수 있는 데이터는 압축없이 암호화만을 진행하여 전송하는 방안이 제시되고 있다. 그러나 압축이 진행되지 않는 점에서, 전송 및 데이터 저장에 있어 제약이 발생하거나 불편을 야기한다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 일 실시예는, 품질 저하를 최소화하면서 안전하게 데이터를 저장하거나 전송할 수 있도록 하는 이미지 암호화/압축 장치 및 방법을 제공하는 데 일 목적이 있다.

과제의 해결 수단

[0007] 본 발명의 일 측면에 의하면, 외부로 전송할 이미지를 암호화한 후 압축하여 전송하는 이미지 암호화/압축 장치

에 있어서, 이미지 내 픽셀을 기 설정된 면적의 블록으로 구분하여, 각 블록마다 암호화를 수행하는 암호화부와 상기 암호화부에서 암호화된 이미지를 압축하는 압축부 및 상기 압축부에 의해 압축된 이미지를 외부로 전송하는 통신부를 포함하는 것을 특징으로 하는 이미지 암호화/압축 장치를 제공한다.

[0008] 본 발명의 일 측면에 의하면, 상기 암호화부는 구분된 각 블록을 무작위로 치환하는 것을 특징으로 한다.

[0009] 본 발명의 일 측면에 의하면, 상기 암호화부는 구분된 각 블록을 무작위로 회전시키거나 반전시키는 것을 특징으로 한다.

[0010] 본 발명의 일 측면에 의하면, 상기 암호화부는 구분된 각 블록 내 픽셀들의 픽셀값을 반전시키는 것을 특징으로 한다.

[0011] 본 발명의 일 측면에 의하면, 상기 암호화부는 비밀키를 생성하여, 생성된 비밀키를 이용하여 암호화를 수행하는 것을 특징으로 한다.

[0012] 본 발명의 일 측면에 의하면, 이미지 암호화/압축 장치가 외부로 전송할 이미지를 암호화하여 압축하는 방법에 있어서, 이미지 내 픽셀들을 기 설정된 면적의 블록으로 구분하는 구분과정과 상기 구분과정에 의해 구분된 각 블록을 무작위로 치환하는 치환과정과 상기 구분과정에 의해 구분된 각 블록을 무작위로 회전하거나 반전시키는 회전과정 및 상기 구분과정에 의해 구분된 각 블록 내 픽셀의 픽셀값을 반전시키는 반전과정을 포함하는 것을 특징으로 하는 이미지 암호화/압축 방법을 제공한다.

[0013] 본 발명의 일 측면에 의하면, 상기 치환과정, 회전과정 및 반전과정은 생성된 비밀키를 이용하여 진행되는 것을 특징으로 한다.

[0014] 본 발명의 일 측면에 의하면, 상기 치환과정, 회전과정 및 반전과정은 서로 다른 비밀키에 의해 진행되는 것을 특징으로 한다.

[0015] 본 발명의 일 측면에 의하면, 상기 이미지 암호화/압축 방법은 상기 반전과정을 거친 이미지를 압축하는 압축과정을 더 포함하는 것을 특징으로 한다.

[0016] 본 발명의 일 측면에 의하면, 상기 이미지 암호화/압축 방법은 상기 압축과정을 거친 이미지를 외부로 전송하는 전송과정을 더 포함하는 것을 특징으로 한다.

발명의 효과

[0017] 이상에서 설명한 바와 같이, 본 발명의 일 측면에 따르면, 품질 저하를 최소화하면서 안전하게 데이터를 저장하거나 전송할 수 있도록 하는 장점이 있다.

도면의 간단한 설명

[0018] 도 1 본 발명의 일 실시예에 따른 데이터 전송 시스템의 구성을 도시한 도면이다.

도 2는 본 발명의 일 실시예에 따른 이미지 암호화/압축 장치의 구성을 도시한 도면이다.

도 3은 본 발명의 일 실시예에 따른 암호화부의 구성을 도시한 도면이다.

도 4는 원본 및 본 발명의 각 실시예에 따라 암호화 및 압축된 이미지를 도시한 도면이다.

도 5는 본 발명의 각 실시예에 따라 암호화 및 압축된 후 복호화된 이미지들의 색차 및 휘도에 관한 이미지 품질을 도시한 그래프이다.

도 6은 본 발명의 일 실시예에 따른 이미지 암호화/압축 장치가 이미지를 암호화한 후 압축하는 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시 예를 가질 수 있는 바, 특정 실시 예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0020] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어

들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

- [0021] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.
- [0022] 본 출원에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서 "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0023] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해서 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.
- [0024] 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0025] 또한, 본 발명의 각 실시예에 포함된 각 구성, 과정, 공정 또는 방법 등은 기술적으로 상호 간 모순되지 않는 범위 내에서 공유될 수 있다.
- [0026] 도 1 본 발명의 일 실시예에 따른 데이터 전송 시스템의 구성을 도시한 도면이다.
- [0027] 도 1을 참조하면, 본 발명의 일 실시예에 따른 데이터 전송 시스템(100)은 이미지 암호화/압축 장치(110, 이하에서 "암호화 장치"라 약칭함) 및 관리서버(120)를 포함한다.
- [0028] 데이터 전송 시스템(100)은 장소와 관계없이 암호화 장치(110)가 저장하고자 하는 데이터를 관리서버(120)로 전송(업로드)하여 저장하며, 관리서버(120)에 저장된 데이터를 자신 또는 자신과 관련있는 제3 단말(130)이 수신(다운로드)하여 확인할 수 있도록 하는 시스템이다.
- [0029] 이때, 암호화 장치(110)가 관리서버(120)로 데이터를 전송하는 과정 및 암호화 장치(110)나 제3 단말(130)이 관리서버로부터 데이터를 수신하는 과정 등에서 데이터가 외부로 노출되기 때문에, 데이터에 암호화가 진행되어야 한다. 또한, 발명의 배경이 되는 기술에서 언급한 바와 같이, 별도의 압축 없이 데이터 전체가 송·수신될 경우, 데이터의 크기에 따라 전송 또는 저장에 제약이 발생할 수 있다.
- [0030] 이에, 암호화 장치(110)는 데이터의 손상을 최소화하며 데이터를 외부로 전송할 수 있도록 한다. 암호화 장치(110)는 데이터에 암호화를 우선적으로 수행한 후 압축을 수행함으로써, 압축 과정에서 발생하는 (필연적인) 손상만이 발생하도록 한다. 이에 따라, 암호화 장치(110)는 데이터의 전송 과정에서의 보안을 확보하는 동시에, 자신 또는 제3 단말(130)이 추후 저장된 데이터를 수신하였을 때도 최대한 원본과 대응되는 데이터를 확인할 수 있도록 한다.
- [0031] 도 2는 본 발명의 일 실시예에 따른 이미지 암호화/압축 장치의 구성을 도시한 도면이다.
- [0032] 도 2를 참조하면, 본 발명의 일 실시예에 따른 암호화 장치(110)는 통신부(210), 암호화부(220), 압축부(230) 및 메모리부(240)를 포함한다.
- [0033] 통신부(210)는 암호화된 후 압축된 데이터를 관리서버(120)로 전송한다. 통신부(210)는 무선통신, 예를 들어, 3G, 4G, 5G, 3GPP(3rd Generation Partnership Project), LTE(Long Term Evolution), WIMAX(World Interoperability for Microwave Access), 와이파이(Wi-Fi), 블루투스 통신, 적외선 통신, 초음파 통신 또는 가시광 통신(VLC: Visible Light Communication) 등이 포함되나 이에 한정되지는 않는다.
- [0034] 암호화부(220)는 전송할 데이터를 암호화한다. 암호화부(220)는 관리서버(120)로 전송할 데이터에 대해 우선적으로 암호화를 진행한다. 암호화부(220)는 다양한 데이터의 유형 중 주로 이미지에 대해 우수한 암호화 효율을 갖는다. 암호화부(220)는 상대적으로 단시간 내에 우수한 암호화율을 갖는 동시에 데이터의 손실을 방지할 수 있는 방식으로 데이터를 암호화한다.

[0035] 암호화부(220)는 도 3에 도시된 바와 같은 구성을 가지며 데이터의 암호화를 진행한다.

[0036] 도 3은 본 발명의 일 실시예에 따른 암호화부의 구성을 도시한 도면이다.

[0037] 도 3을 참조하면, 본 발명의 일 실시예에 따른 암호화부(220)는 제1 암호화 수행부(310), 제2 암호화 수행부(320), 제3 암호화 수행부(330) 및 비밀키 생성부(340)를 포함한다.

[0038] 제1 암호화 수행부(310)는 이미지 내 픽셀을 기 설정된 면적의 블록으로 구분하여, 제1 비밀키를 이용해 각 블록을 무작위로 치환한다.

[0039] 제1 암호화 수행부(310)는 이미지 내 각 픽셀들을 기 설정된 면적의 서로 겹치지 않는 블록으로 구분한다. 예를 들어, $W \times H$ 픽셀을 갖는 이미지를 암호화하여야 할 경우, 제1 암호화 수행부(310)는 $B_M \times B_N$ 개의 픽셀을 갖는 면적의 블록으로 이미지를 구분한다. 이에 따라, 암호화될 이미지는 아래와 같이 n 개의 블록으로 구분될 수 있다.

$$n = \frac{W \times H}{B_M \times B_N}$$

[0040]

[0041] 제1 암호화 수행부(310)는 암호화될 이미지를 n 개의 블록으로 구분한 후, 제1 비밀키를 이용하여 각 블록을 무작위로 치환한다. 제1 암호화 수행부(310)는 비밀키 생성부(340)에 의해 생성된 제1 비밀키를 이용하여 각 블록을 무작위로 치환한다. 제1 암호화 수행부(310)의 암호화로 인한 경우의 수는 $n!$ 에 해당한다.

[0042] 제2 암호화 수행부(320)는 블록으로 구분된 각 이미지들에 대해 각 블록을 무작위로 회전하고 반전시킨다. 제2 암호화 수행부(320)는 비밀키 생성부(340)에 의해 생성된 제2 비밀키를 이용하여, 제1 암호화 수행부(310)에 의해 각 블록들을 무작위로 회전시키거나 반전시킨다. 이에 따라, 제2 암호화 수행부(320)의 암호화로 인한 경우의 수는 8^n 에 해당한다.

[0043] 이때, 제2 암호화 수행부(320)는 제1 암호화 수행부(310)에 의해 구분된 블록들을 더 작은 크기의 단위블록으로 추가적으로 구분할 수 있다. 예를 들어, 제1 암호화 수행부(310)에 의해 구분된 블록의 크기가 8×8 이라고 가정할 경우, 제2 암호화 수행부(320)는 각 블록들을 4×4 또는 2×2 크기의 단위블록으로 추가로 구분할 수 있다. 제2 암호화 수행부(320)는 각 블록을 추가로 단위블록으로 구분한 후, 각 단위블록에 대해 회전하고 반전시킨다. 각 블록마다 m 개의 단위 블록으로 구분된 경우, 제2 암호화 수행부(320)의 암호화로 인한 경우의 수는 $8^{n \times m}$ 개로 증가하게 된다.

[0044] 제3 암호화 수행부(330)는 각 블록 내 모든 픽셀들에 대해 픽셀값을 반전시킨다. 제3 암호화 수행부(330)는 제1 암호화 수행부(310)에 의해 구분된 블록들 또는 제2 암호화 수행부(320)에 의해 구분된 단위 블록들 내의 각 픽셀들에 대해 픽셀값을 반전시킨다. 제3 암호화 수행부(330)는 비밀키 생성부(340)에 의해 생성된 제3 비밀키를 이용하여, 블록 또는 단위 블록들 내 픽셀들에 대해 픽셀값을 반전시킨다. 예를 들어, 제3 암호화 수행부(330)는 제3 비밀키를 이용하여 다음과 같이 픽셀값을 반전시킨다. 제3 비밀키를 이용하여 생성되는 임의의 이진 정수값에 따라, 아래와 같이 픽셀값을 그대로 두거나 반전시킨다. 기존 픽셀값을 $p(i)$ 로, 암호화된 픽셀값을 $p'(i)$ 로, 제3 비밀키에 의해 생성된 정수값을 K_3 라 정의하면,

$$p'(i) = \begin{cases} p(i), & K_3 = 0 \\ 255 - p(i), & K_3 = 1 \end{cases}$$

[0045]

[0046] 블록 또는 단위블록 내 모든 픽셀들은 제3 비밀키에 의해 생성되는 임의의 (이진) 정수값에 따라 픽셀값을 유지하거나 반전된 픽셀값을 갖는다. 제3 암호화 수행부(330)의 암호화로 인한 경우의 수는 2^n 에 해당하며, 제3 암

호화 수행부(330)가 각 단위블록에 대해 암호화를 수행할 경우, 경우의 수는 2^{n*nm} 개까지 증가할 수 있다.

- [0047] 비밀키 생성부(340)는 각 암호화 수행부(310 내지 330)가 암호화를 수행하는데 사용할 비밀키를 생성하여 제공한다.
- [0048] 암호화부(220)의 전술한 동작에 따라, 하나의 이미지에 대해 암호화를 진행함에 있어 발생할 수 있는 최소 경우의 수는 $n! * 8^n * 2^n$ 이 되며, 최대 경우의 수는 $n! * 8^{n*nm} * 2^{n*nm}$ 이 된다. 이에 따라, 암호화부(220)는 간단한 조작으로 단시간 내에 우수한 암호화율을 확보할 수 있다.
- [0049] 다시 도 2를 참조하면, 압축부(230)는 암호화부(220)에 의해 암호화된 데이터를 압축한다. 데이터의 크기를 줄임으로서, 암호화 장치(110)가 관리서버(120)로 데이터를 전송하거나, 관리서버(120)가 데이터를 저장함에 있어 보다 원활히 진행할 수 있도록 한다.
- [0050] 메모리부(240)는 암호화부(220)에서 생성된 제1 내지 제3 비밀키를 저장한다. 추후, 메모리부(240)는 생성된 비밀키들을 저장함으로서, 관리서버(120)에서 저장된 데이터를 자신 또는 자신과 관련있는 제3 단말(130)이 수신하여 복호화할 수 있도록 한다.
- [0051] 도 4는 원본 및 본 발명의 각 실시예에 따라 암호화 및 압축된 이미지를 도시한 도면이다.
- [0052] 도 4a는 원본 이미지를, 도 4b는 블록(8*8)을 이용해 암호화를 진행한 이미지와 그를 복호화한 이미지를, 도 4c는 단위 블록(4*4)까지 이용해 암호화를 진행한 이미지와 그를 복호화한 이미지를, 도 4d는 단위 블록(2*2)까지 이용해 암호화를 진행한 이미지와 그를 복호화한 이미지를 각각 도시한다. 암호화 및 복호화에 있어서, 색상 서브 샘플링이 없는 휘도 양자화 테이블이 이용되었으며, JPEG 품질계수는 100으로 설정된 상태에서 진행되었다. 도 4를 참조하면, 블록을 이용하여 암호화를 진행한 경우에도 충분한 암호화율을 보이고 있음이 확인되었으며, 서브 블록을 추가로 이용하였을 경우, 암호화 효율이 보다 우수해짐을 확인할 수 있었다. 또한, 암호화를 우선적으로 진행한 후 압축이 진행되었을 경우, 복호화된 이미지 내에서 데이터 손실이 거의 발생하지 않은 것도 함께 확인할 수 있었다.
- [0053] 도 5는 본 발명의 각 실시예에 따라 암호화 및 압축된 후 복호화된 이미지들의 색차 및 휘도에 관한 이미지 품질을 도시한 그래프이다.
- [0054] 도 5a는 복호화된 이미지들의 색차 양자화 테이블을 이용하였을 경우의 이미지 품질을 도시한 그래프이며, 도 5b는 복호화된 이미지들의 휘도 양자화 테이블을 이용하였을 경우의 이미지 품질을 도시한 그래프이다. x축은 비트 전송률을 의미하며, y축은 복호화된 이미지의 품질을 의미한다. PSNR이 작을수록 이미지 품질이 우수해지며, 압축성능이 향상됨을 의미한다. 본 발명의 모든 실시예에서의 이미지 품질을 보더라도 낮은 비트 전송률에서 복호화된 이미지들의 품질이 우수한 것을 확인할 수 있다.
- [0055] 상대적으로 블록만을 이용한 실시예에서 이미지 품질이 우수함을 확인할 수 있었다. 이는 암호화율에 있어서는 단위블록을 이용한 실시예가 보다 우월함을 의미할 수 있다.
- [0056] 도 6은 본 발명의 일 실시예에 따른 이미지 암호화/압축 장치가 이미지를 암호화한 후 압축하는 방법을 도시한 순서도이다.
- [0057] 제1 암호화 수행부(310)는 이미지 내 픽셀들을 기 설정된 면적의 블록으로 구분한다(S610).
- [0058] 제1 암호화 수행부(310)는 제1 비밀키를 이용하여 구분된 각 블록을 무작위로 치환한다(S620).
- [0059] 제2 암호화 수행부(320)는 제2 비밀키를 이용하여 구분된 각 블록을 무작위로 회전하거나 반전한다(S630).
- [0060] 제3 암호화 수행부(330)는 제3 비밀키를 이용하여 각 블록 내 픽셀의 픽셀값을 반전시킨다(S640)
- [0061] 압축부(340) 및 통신부(310)는 암호화된 이미지를 압축하여 전송한다(S650).
- [0062] 도 6에서는 각 과정을 순차적으로 실행하는 것으로 기재하고 있으나, 이는 본 발명의 일 실시예의 기술 사상을 예시적으로 설명한 것에 불과한 것이다. 다시 말해, 본 발명의 일 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 일 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 각 도면에 기재된 순서를 변경하여 실행하거나 각 과정 중 하나 이상의 과정을 병렬적으로 실행하는 것으로 다양하게 수정 및 변형하여 적용 가능할 것이므로, 도 6은 시계열적인 순서로 한정되는 것은 아니다.
- [0063] 한편, 도 6에 도시된 과정들은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것

이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 즉, 컴퓨터가 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등) 및 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등)와 같은 저장매체를 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0064]

이상의 설명은 본 실시예의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 실시예들은 본 실시예의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 실시예의 기술 사상의 범위가 한정되는 것은 아니다. 본 실시예의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 실시예의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0065]

100: 데이터 전송 시스템

110: 이미지 암호화/압축 장치

120: 관리서버

130: 제3 단말

210: 통신부

220: 암호화부

230: 압축부

240: 메모리부

310: 제1 암호화 수행부

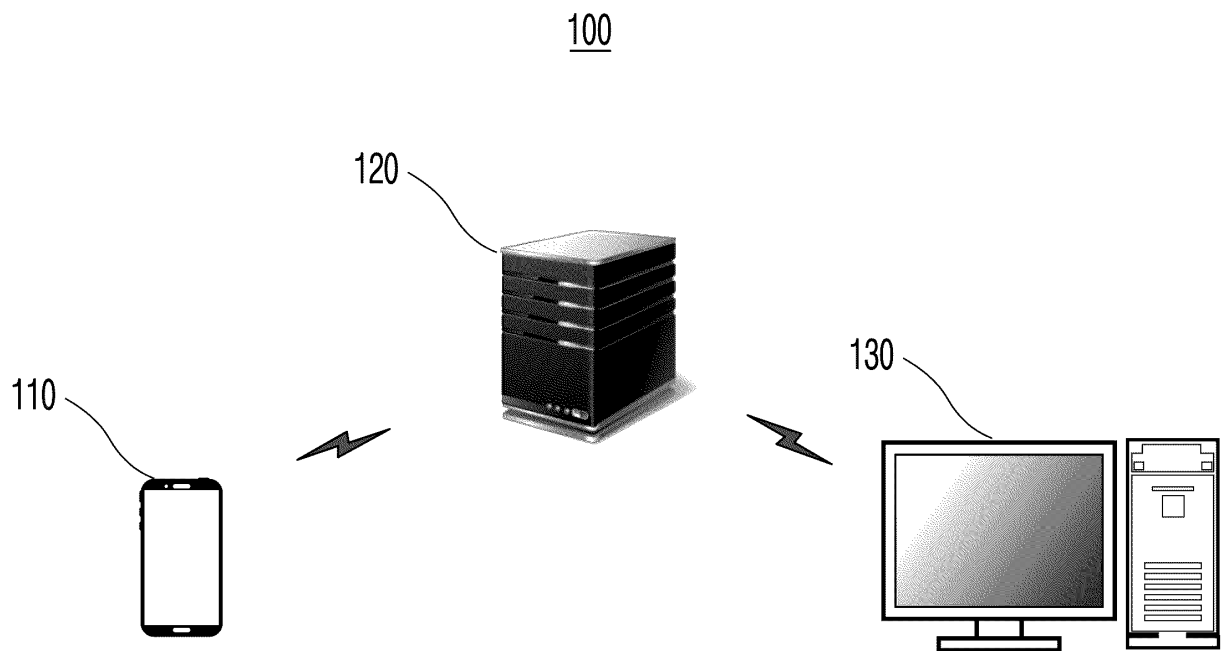
320: 제2 암호화 수행부

330: 제3 암호화 수행부

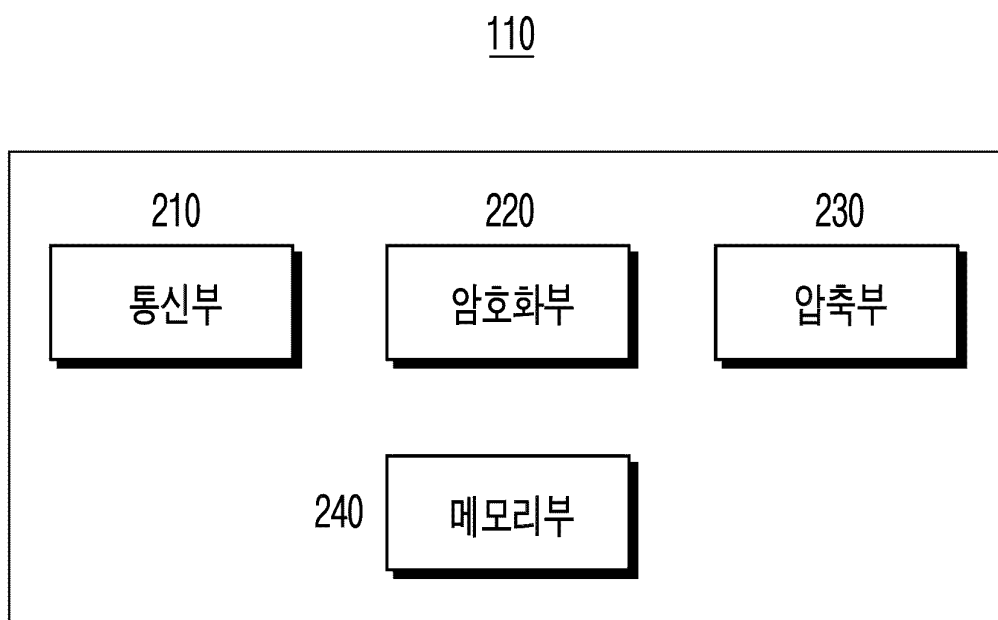
340: 비밀키 생성부

도면

도면1

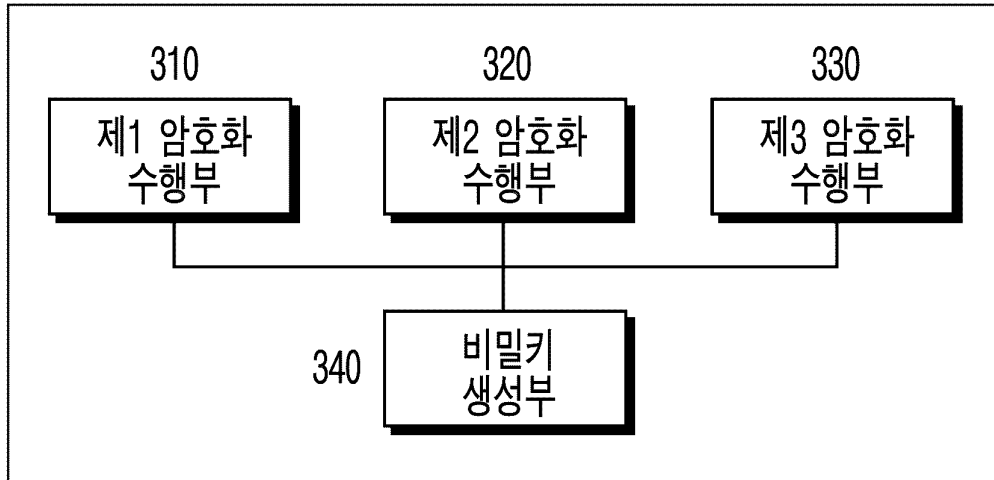


도면2



도면3

220



도면4a



도면4b

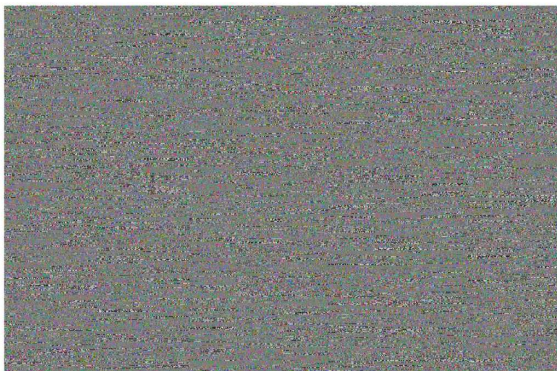


(a)



(b)

도면4c

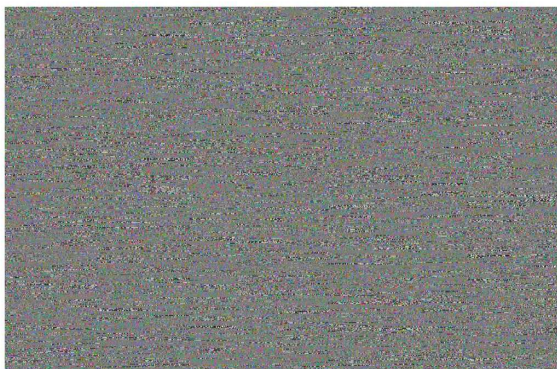


(a)



(b)

도면4d

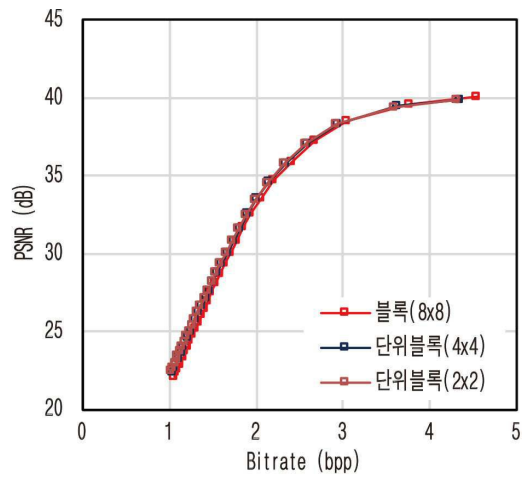


(a)

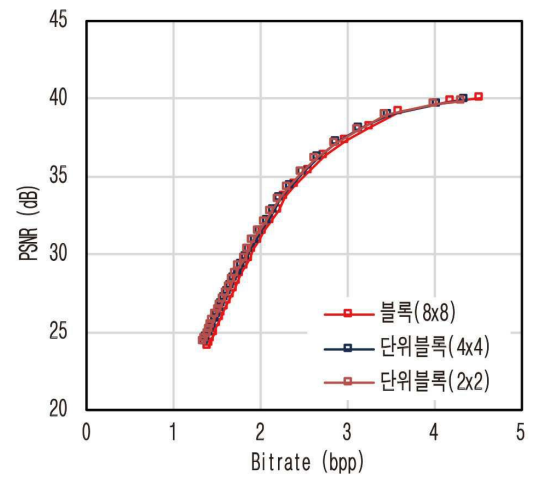


(b)

도면5



(a)



(b)

도면6

