



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년06월28일
(11) 등록번호 10-1751971
(24) 등록일자 2017년06월22일

(51) 국제특허분류(Int. Cl.)
H04N 21/2347 (2016.01) H04N 21/4385 (2011.01)

H04N 21/4408 (2016.01)

(52) CPC특허분류
H04N 21/23473 (2013.01)
H04N 21/43856 (2013.01)

(21) 출원번호 10-2016-0005891

(22) 출원일자 2016년01월18일

심사청구일자 2016년01월18일

(56) 선행기술조사문헌

KR1020120006926 A*

채효철, R. S. 라마크리시나, “암호화된 영상에
서의 2차원 영상 필터링”, 한국정보과학회 학술
발표논문집, 34(1A), 117-118, 2007. 6.*

Nan Hu et al., “Secure image filtering”,
IEEE International Conference on Image
Processing, Atlanta, Ga, USA, Oct. 2006, pp.
1553-1556.*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암
동5가)

(72) 발명자

윤지원

서울특별시 용산구 한강대로43길 8, 102동 1401호
(한강로2가, 벽산메가트리움)

기영준

서울특별시 성동구 독서당로39길 37-1 (옥수동)

(74) 대리인

특허법인엠에이피에스

전체 청구항 수 : 총 14 항

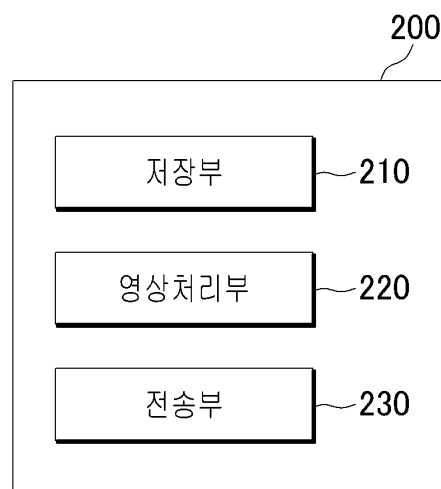
심사관 : 이성현

(54) 발명의 명칭 암호화 상태의 이미지에 대한 영상처리방법 및 영상처리장치

(57) 요약

본 발명의 일 실시예에 따르는, 암호화 상태의 이미지에 대한 영상처리방법은 (a) 클라이언트 단말로부터 HE (Homomorphic Encryption) 기법을 통해 암호화된 이미지를 수신하는 단계; (b) 상기 클라이언트 단말로부터의 요청에 따라, 상기 이미지에 대하여 암호화된 상태에서 FIR (Finite Impulse Response) 필터를 적용하여 영상처리를 수행하는 단계; 및 (c) 상기 영상처리가 수행된 이미지를 암호화된 상태로 상기 클라이언트 단말에 전송하는 단계를 포함한다.

대표도 - 도2



(52) CPC특허분류

H04N 21/4408 (2013.01)

명세서

청구범위

청구항 1

서버에 의해 수행되는 암호화 상태의 이미지에 대한 영상처리방법에 있어서,

- (a) 클라이언트 단말로부터 HE (Homomorphic Encryption) 기법을 통해 암호화된 이미지를 수신하는 단계;
 - (b) 상기 클라이언트 단말로부터의 요청에 따라, 상기 이미지에 대하여 암호화된 상태에서 FIR (Finite Impulse Response) 필터를 적용하여 영상처리를 수행하는 단계; 및
 - (c) 상기 영상처리가 수행된 이미지를 암호화된 상태로 상기 클라이언트 단말에 전송하는 단계를 포함하며,
- 상기 HE 기법은 Paillier Cryptosystem 기법이며,

상기 암호화된 이미지는, 상기 이미지의 각 픽셀값에 대한 평문을 암호화하기 위한 두 개의 공개키와 두 개의 비밀키가, 미리 설정된 기준에 따라 선택된 평문과 난수에 적용됨으로써 암호화된 것이며, 서로 동일한 평문을 갖는 픽셀값들이 존재한다 하더라도 각 픽셀값들에 대한 난수에 따라 서로 다른 암호문으로 암호화될 수 있는 것인, 암호화 상태의 이미지에 대한 영상처리방법.

청구항 2

삭제

청구항 3

제 1 항에 있어서,

상기 수신된 이미지는,

상기 이미지의 각 픽셀마다 암호화된 것인, 암호화 상태의 이미지에 대한 영상처리방법.

청구항 4

제 1 항에 있어서,

상기 (b) 단계는,

상기 이미지를 구성하는 전체 픽셀들을 부분 픽셀 집합으로 분할하고, 각 부분 픽셀 집합에 대하여 상기 FIR 필터를 적용하는 단계를 포함하는, 암호화 상태의 이미지에 대한 영상처리방법.

청구항 5

제 4 항에 있어서,

상기 (b) 단계는,

상기 부분 픽셀 집합을 이루는 픽셀들 중 가운데 픽셀에 대한 필터가중치를 양(+)으로 설정하고, 나머지 픽셀에 대한 필터 가중치를 음(-)으로 설정하여 FIR 필터를 수행하는 단계를 포함하는, 암호화 상태의 이미지에 대한 영상처리방법.

청구항 6

제 4 항에 있어서,

상기 (b) 단계는,

상기 FIR 필터가 적용된 전체 픽셀들의 암호문들을 서로 곱하는 단계를 포함하는, 암호화 상태의 이미지에 대한

영상처리방법.

청구항 7

제 1 항에 있어서,

상기 클라이언트 단말로 전송된 암호화된 이미지는 상기 클라이언트 단말에서 복호화될 경우, 상기 FIR 필터에 의한 영상처리가 수행된 상태로 복호화되는 것인, 암호화 상태의 이미지에 대한 영상처리방법.

청구항 8

제 1 항에 있어서,

상기 수신된 이미지는,

상기 이미지를 구성하는 복수의 픽셀들의 각 행(row) 또는 열(column)을 기준으로 암호화된 것이며,

상기 (b) 단계는,

상기 암호화된 행 또는 열을 기준으로 상기 FIR 필터를 적용하는 단계를 포함하는, 암호화 상태의 이미지에 대한 영상처리방법.

청구항 9

암호화 상태의 이미지에 대한 영상처리장치에 있어서,

암호화 상태의 이미지에 대한 영상처리를 수행할 수 있는 프로그램을 저장한 메모리; 및

상기 프로그램을 실행하는 프로세서를 포함하며,

상기 프로세서는, 상기 프로그램이 실행될 경우,

클라이언트 단말로부터 HE (Homomorphic Encryption)기법을 통해 암호화된 이미지를 수신하고,

상기 클라이언트 단말로부터의 요청에 따라, 상기 이미지에 대하여 암호화된 상태에서 FIR 필터를 적용하여 영상처리를 수행하며,

상기 영상처리가 수행된 이미지를 암호화된 상태로 상기 클라이언트 단말에 전송하되,

상기 HE 기법은 Paillier Cryptosystem 기법이며,

상기 암호화된 이미지는, 상기 이미지의 각 픽셀값에 대한 평문을 암호화하기 위한 두 개의 공개키와 두 개의 비밀키가, 미리 설정된 기준에 따라 선택된 평문과 난수에 적용됨으로써 암호화된 것이며, 서로 동일한 평문을 갖는 픽셀값들이 존재한다 하더라도 각 픽셀값들에 대한 난수에 따라 서로 다른 암호문으로 암호화될 수 있는 것인, 암호화 상태의 이미지에 대한 영상처리장치.

청구항 10

삭제

청구항 11

제 9 항에 있어서,

상기 수신된 이미지는,

상기 이미지의 각 픽셀마다 암호화된 것인, 암호화 상태의 이미지에 대한 영상처리장치.

청구항 12

제 9 항에 있어서,

상기 프로세서는,

상기 이미지를 구성하는 전체 픽셀들을 부분 픽셀 집합으로 분할하고, 각 부분 픽셀 집합에 대하여 상기 FIR 필터를 적용하는, 암호화 상태의 이미지에 대한 영상처리장치.

청구항 13

제 12 항에 있어서,

상기 프로세서는,

상기 부분 픽셀 집합을 이루는 픽셀들 중 가운데 픽셀에 대한 필터가중치를 양(+)으로 설정하고, 나머지 픽셀에 대한 필터 가중치를 음(-)으로 설정하여 FIR 필터를 수행하는, 암호화 상태의 이미지에 대한 영상처리장치.

청구항 14

제 12 항에 있어서,

상기 프로세서는,

상기 FIR 필터가 적용된 전체 픽셀들의 암호문들을 서로 곱하는, 암호화 상태의 이미지에 대한 영상처리장치.

청구항 15

제 9 항에 있어서,

상기 클라이언트 단말로 전송된 암호화된 이미지는 상기 클라이언트 단말에서 복호화될 경우, 상기 FIR 필터에 의한 영상처리가 수행된 상태로 복호화되는 것인, 암호화 상태의 이미지에 대한 영상처리장치.

청구항 16

제 1 항 및 제 3 항 내지 제 8 항 중 어느 한 항에 따르는 암호화 상태의 이미지에 대한 영상처리방법을 수행하는 프로그램이 저장된 컴퓨터 판독가능 기록매체.

발명의 설명

기술 분야

[0001] 본 발명은 암호화 상태의 이미지에 대한 영상처리방법 및 영상처리장치에 관한 것으로서, 보다 상세하게는 클라우드 컴퓨팅 환경에서 사용자의 프라이버시를 보호하기 위한 암호화 상태의 이미지에 대한 영상처리방법 및 영상처리장치에 관한 것이다.

배경 기술

[0002] 환자의 의료 영상과 같은 멀티미디어 정보가 양이 많아지면서 클라우드 환경에 데이터를 저장하는 경향이 많아지고 있다. 이러한 환경에서 영상처리 작업을 수행할 때 두 가지 방법이 사용되고 있다.

[0003] 첫 번째는 클라이언트 측에서 해당 데이터를 직접 다운로드 한 뒤에 각각을 복호화한 후 영상처리를 수행하는 것이다. 하지만, 이러한 경우 서버는 단지 데이터 저장 이외의 정보 처리 등의 작업을 하지 않는 대신 클라이언트가 무리한 연산처리를 하게 되어 사용자 입장에서는 오랜 시간의 연산처리 과정을 기다려야 하는 문제가 있다.

[0004] 두 번째 방법은 첫 번째 방법을 해결하기 위한 것으로서, 클라이언트의 요청시 서버에서 직접 암호를 복호화한 뒤에 서버가 직접 이미지를 처리한 후에 클라이언트에 암호화된 데이터나 암호화되지 않은 그대로의 데이터를 전송하는 방법이다. 그러나 이러한 방법은 서버가 암호화된 이미지를 확인할 수 있게 되어, 서버 관리자 또는 해킹 등에 의해 클라이언트의 개인정보가 유출되거나 노출될 수 있다는 문제점이 존재한다.

[0005] 한편, 이러한 정보의 유출을 막기 위한 데이터베이스 보호 기술들은 크게 접근 제어를 사용하는 방법과 암호를 사용한 방법으로 나누어진다. 데이터 베이스의 접근 제어를 활용한 방법은 데이터 베이스에 접근하려는 사용자가 정당한 사용자인 것을 인증하는 방식으로 구현된다.

[0006] 암호를 사용한 방법에는 대표적으로 Order Preserving Encryption(OPE), Homomorphic Encryption(HE), Attribute Based Encryption (ABE) 가 있다. OPE는 데이터가 암호화된 상태에서도 평문에서의 순서를 유지하는 기술로, 암호화된 상태에서 데이터 검색을 가능하게 해주는 특징이 있다. HE는 데이터를 암호화된 채로 덧셈과 곱셈과 같은 연산이 가능하게 해주는 기술로, 서버는 평문에 대한 정보를 모른 채 암호문을 활용해 연산을 할 수 있다는 특징을 갖는다. ABE는 특정 속성을 갖는 데이터만 검색할 수 있게 해주는 기술로, 나이와 성별과 같

은 데이터의 특성에 대해서 검색을 할 수 있다는 특징이 있다.

선행기술문헌

비특허문헌

- [0007] (비특허문헌 0001) Paillier, Pascal. "Public-key cryptosystems based on composite degree residuosity classes." Advances in cryptology—EUROCRYPT'99. Springer Berlin Heidelberg, 1999.

발명의 내용

해결하려는 과제

- [0008] 본 발명은 서버에 저장된 암호화된 데이터를 복호화하지 않은 채 FIR 필터를 통해 바로 영상처리를 수행하여 클라이언트 측으로 제공함으로써, 사용자의 프라이버시를 보호하면서 손쉽고 빠른 영상처리가 이루어질 수 있도록 하는 방법 및 장치를 제공하는 데에 목적이 있다.

과제의 해결 수단

- [0009] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 일 실시예에 따르는, 서버에 의해 수행되는 암호화 상태의 이미지에 대한 영상처리방법은 (a) 클라이언트 단말로부터 HE (Homomorphic Encryption) 기법을 통해 암호화된 이미지를 수신하는 단계; (b) 상기 클라이언트 단말로부터의 요청에 따라, 상기 이미지에 대하여 암호화된 상태에서 FIR (Finite Impulse Response) 필터를 적용하여 영상처리를 수행하는 단계; 및 (c) 상기 영상처리가 수행된 이미지를 암호화된 상태로 상기 클라이언트 단말에 전송하는 단계를 포함한다.
- [0010] 또한, 본 발명의 다른 실시예에 따르는, 암호화 상태의 이미지에 대한 영상처리장치는, 암호화 상태의 이미지에 대한 영상처리를 수행할 수 있는 프로그램을 저장한 메모리; 및 상기 프로그램을 실행하는 프로세서를 포함하며, 상기 프로세서는, 상기 프로그램이 실행될 경우, 클라이언트 단말로부터 HE (Homomorphic Encryption) 기법을 통해 암호화된 이미지를 수신하고, 상기 클라이언트 단말로부터의 요청에 따라, 상기 이미지에 대하여 암호화된 상태에서 FIR 필터를 적용하여 영상처리를 수행하며, 상기 영상처리가 수행된 이미지를 암호화된 상태로 상기 클라이언트 단말에 전송한다.

발명의 효과

- [0011] 본 발명은 클라우드 서버에서 영상처리가 암호화된 채로 진행되어져 사용자가 안전하게 이미지를 클라우드 서버에 저장하고 편집할 수 있도록 할 수 있다. 사용자가 온라인 상으로 이미지를 편집하더라도 이미지의 원본, 편집 과정의 데이터가 모두 서버에 저장되기는 하나, 서버는 이미지에 대한 어떠한 정보도 얻어낼 수 없게 되므로, 서버 관리자나 해킹에 의한 노출 우려가 있더라도 데이터 소유자의 프라이버시를 보호할 수 있다. 이를 통해 본 발명의 일 실시예는 클라우드 서비스 환경에서의 영상 처리 과정에 보안성을 부여할 수 있다.

도면의 간단한 설명

- [0012] 도 1은 본 발명의 일 실시예에 따르는 암호화 상태의 이미지에 대한 영상처리 시스템에 관한 구조도이다.
- 도 2는 본 발명의 일 실시예에 따르는 암호화 상태의 이미지에 대한 영상처리장치의 구조도이다.
- 도 3a 내지 도 3c는 본 발명의 일 실시예에 따르는 암호화 상태에서 FIR 필터를 통해 영상처리하는 과정을 나타내는 예시도이다.
- 도 4a는 영상처리 전의 사진이며, 도 4b는 본 발명의 일 실시예에 따라 영상처리된 사진이다.
- 도 5는 본 발명의 일 실시예에 따르는 암호화 상태의 이미지에 대한 영상처리방법에 관한 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0013] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며

여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0014] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0015] 본 명세서에 있어서 '부(部)'란, 하드웨어에 의해 실현되는 유닛(unit), 소프트웨어에 의해 실현되는 유닛, 양방을 이용하여 실현되는 유닛을 포함한다. 또한, 1 개의 유닛이 2 개 이상의 하드웨어를 이용하여 실현되어도 되고, 2 개 이상의 유닛이 1 개의 하드웨어에 의해 실현되어도 된다. 한편, '~부'는 소프트웨어 또는 하드웨어에 한정되는 의미는 아니며, '~부'는 어드레싱 할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 '~부'는 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다. 구성요소들과 '~부'들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 '~부'들로 결합되거나 추가적인 구성요소들과 '~부'들로 더 분리될 수 있다. 뿐만 아니라, 구성요소들 및 '~부'들은 디바이스 또는 보안 멀티미디어카드 내의 하나 또는 그 이상의 CPU들을 재생시키도록 구현될 수도 있다.

[0016] 이하에서 언급되는 "클라이언트 단말"은 네트워크를 통해 서버나 타 단말에 접속할 수 있는 컴퓨터나 휴대용 단말기로 구현될 수 있다. 여기서, 컴퓨터는 예를 들어, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(desktop), 랩톱(laptop) 등을 포함하고, 휴대용 단말기는 예를 들어, 휴대성과 이동성이 보장되는 무선 통신 장치로서, PCS(Personal Communication System), GSM(Global System for Mobile communications), PDC(Personal Digital Cellular), PHS(Personal Handyphone System), PDA(Personal Digital Assistant), IMT(International Mobile Telecommunication)-2000, CDMA(Code Division Multiple Access)-2000, W-CDMA(W-Code Division Multiple Access), Wibro(Wireless Broadband Internet) 단말 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다. 또한, "네트워크"는 근거리 통신망(Local Area Network; LAN), 광역 통신망(Wide Area Network; WAN) 또는 부가가치 통신망(Value Added Network; VAN) 등과 같은 유선 네트워크나 이동 통신망(mobile radio communication network) 또는 위성 통신망 등과 같은 모든 종류의 무선 네트워크로 구현될 수 있다.

[0017] 먼저, 도 1을 참조하면, 본 발명의 일 실시예에 따르는 시스템은 클라이언트 단말(100)과 서버(200)를 포함하여 구성된다. 클라이언트 단말(100)은 상술한 바와 같이 사용자 측의 PC나 스마트폰, 태블릿 PC 등과 같은 단말이다. 서버(200)는 클라우드 환경의 서버가 될 수 있으며, 의료영상분석, 추가정보 처리 및 IOT 시스템 등의 목적으로 활용되는 서버가 될 수 있다.

[0018] 여기서 클라이언트 단말(100)은 임의의 이미지에 대한 암호화 처리를 수행한다. 사용자에 의해 클라이언트 단말(100)에서 특정한 방식에 의한 암호화 처리가 수행될 수 있다. 그리고, 클라이언트 단말(100)에서 서버(200)로 암호화된 이미지가 전송되어 저장될 수 있다. 서버(200)는 다수의 클라이언트 단말(100)로부터 복수의 이미지를 저장해두는 데이터베이스 역할을 수행할 수 있다. 이와 동시에, 클라이언트 단말(100)로부터 영상처리 요청을 수신하였을 경우, 서버(200)에 저장된 상태에서 영상처리를 수행할 수 있다. 여기서 중요한 것은 암호화된 상태 그대로 영상처리를 수행한다는 것이다. 그에 따라, 서버(200)의 관리자 입장에서는 서버(200) 내에 무엇이 저장되어 있는지 확인하기 어려우며, 어떠한 영상처리가 진행된 것인지 역시 확인하기 어렵다. 즉, 클라이언트의 프라이버시 보호가 철저히 이루어질 수 있다. 암호화된 채로 영상처리된 이미지는 클라이언트 단말(100)로 전송된 후, 클라이언트 단말(100) 측에서 복호화될 경우, 영상처리가 이루어진 후의 이미지로 제공될 수 있다.

[0019] 이하, 도 2 내지 도 4a 및 도 4b를 참고하여, 본 발명의 일 실시예에 따르는 암호화 상태의 이미지에 대한 영상처리장치의 구성에 대하여 구체적으로 설명한다.

[0020] 아래의 영상처리장치는 도 1의 서버(200)에 대응하는 구성이다. 영상처리장치는 암호화 상태의 이미지에 대한 영상처리방법을 수행하기 위한 프로그램(또는 애플리케이션)이 저장된 메모리와 위 프로그램을 실행하는 프로세서를 포함하여 구성될 수 있다. 여기서 프로세서는 메모리에 저장된 프로그램의 실행에 따라 다양한 기능을 수행할 수 있는데, 각 기능에 따라 프로세서에 포함되는 하위 모듈들을 저장부(210), 영상처리부(220), 전송부(230)로 나타낼 수 있다.

[0021] 저장부(210)는 클라이언트 단말(100)로부터 전송된 이미지를 저장한다. 클라이언트 단말(100)로부터 전송된 이미지는 암호화된 이미지일 수 있다. 바람직하게는, HE (Homomorphic Encryption) 기법을 통해 암호화된 이미지일 수 있으며, 더 바람직하게는, Paillier Cryptosystem 기법을 통해 암호화된 이미지일 수 있다.

[0022] Paillier Cryptosystem 기법의 암호화 방식에 대하여 단순화하여 설명하면 아래와 같다.

[0023] 먼저, 길이가 같은 두 개의 큰 소수 p ($p > 1$)와 q ($q > 1$)가 결정된다. 이때, p 와 q 에 의해 n , λ , g , μ 는 수학식 1과 같이 정의된다.

수학식 1

$$n = pq, \lambda = (p-1)(q-1), g = n+1, \mu = \lambda^{-1} \bmod n$$

[0024]

[0025] 이어서, 이미지의 각 픽셀값에 대한 평문을 암호화하기 위한 키(key)들 중 공개키를 (n , g)로 설정하고, 비밀키를 (λ , μ)로 설정한다.

[0026] 암호화는 다음과 같이 진행되는데, 먼저, 평문(m)과 난수(r)는 $m \in Z_n$, $r \in Z_{n^2}$ 와 같이 규정 하에서 선택된다. 그리고 선택된 평문과 난수에 기초하여 수학식 2와 같이 암호문(c)을 계산한다.

수학식 2

$$c = g^m r^n \bmod n^2$$

[0027]

[0028] 이 경우, 암호문을 평문으로 변환하는 복호화는 수학식 3과 같이 진행될 수 있다.

수학식 3

$$m = \left\lfloor \frac{(c^\lambda \bmod n^2) - 1}{n} \right\rfloor \mu \bmod n$$

[0029]

[0030] 이상의 과정을 통해 암호화 과정이 이루어지게 되며, 암호화는 이미지의 각 픽셀마다 이루어진다.

[0031] 영상처리부(220)는 클라이언트 단말(100)로부터의 요청에 따라, 이미지에 대하여 암호화된 상태에서 FIR (Finite Impulse Response) 필터를 적용하여 영상처리를 수행한다.

[0032] 구체적으로, 영상처리부(220)는 이미지를 구성하는 전체 픽셀들을 복수의 부분 픽셀 집합으로 분할하고, 각 부분 픽셀 집합에 대하여 FIR 필터를 적용한다. 이때, 부분 픽셀 집합을 이루는 픽셀들 중 가운데 픽셀에 대한 필터가중치를 양(+)으로 설정하고, 나머지 픽셀에 대한 필터 가중치를 음(-)으로 설정하여 FIR 필터를 수행할 수 있다.

[0033] 여기서 FIR 필터는 이산 데이터에 대하여 수학식 4와 같은 수식으로 정의될 수 있다.

수학식 4

$$y[n] = b_0 x[n] + b_1 x[n-1] + \dots + b_N x[n-N]$$

$$= \sum_{i=0}^N b_i x[n-i]$$

[0034]

[0035]

위 수학식 4에서 b_i ($i=0, \dots, N$)는 i 번째 데이터 $x[n-i]$ 에 대한 계수이며, 필터 별로 상이하게 설정되는 값이다. 이러한 수학식 4를 이미지와 같은 2차원 데이터에 적용할 경우, FIR 필터는 수학식 5와 같이 정리될 수 있다.

수학식 5

$$y[m,n] = \sum_{i=-N}^N \sum_{j=-N}^N b_{i,j} x[m-i, n-j]$$

[0036]

[0037]

일 예로, 이미지 내의 임의의 3 x 3 크기의 부분 픽셀 집합에 대한 Sharpening Filter는 수학식 6과 같이 정의될 수 있다.

수학식 6

$$y[m,n] = \sum_{i=-1}^1 \sum_{j=-1}^1 b_{i,j} x[m-i, n-j]$$

$$= -x[m-1, n-1] - x[m-1, n] - x[m-1, n+1]$$

$$- x[m, n-1] + 9x[m, n] - x[m, n+1]$$

$$- x[m+1, n-1] - x[m+1, n] - x[m+1, n+1]$$

[0038]

[0039]

즉, 수학식 6에 따르면, Sharpening Filter에 있어서, 부분 픽셀 집합 내의 가운데 픽셀에 대해서는 가장 높은 가중치인 9가 적용되며, 가운데 픽셀을 제외한 나머지 가장자리를 구성하는 픽셀들에 대해서는 -1이라는 가중치가 적용된다.

[0040]

도 3a 내지 도 3c를 예로 들어 설명하면, 먼저, 이미지는 도 3a와 같이 여러 가지의 픽셀들로 구성되는 데 그 중 일부 픽셀(즉, 부분 픽셀 집합)은 도 3a에 도시된 바와 같은 픽셀값으로 구성될 수 있다. 여기서 픽셀값이란 픽셀의 R, G, B에 관한 값을 의미할 수 있다. 이어서, 클라이언트 단말(100)에서 Paillier Cryptosystem 기법을 통해 이미지가 암호화될 경우, 도 3b와 같이 각 픽셀값마다 암호화될 수 있다. 여기서 주의할 점은 각 픽셀 별로 동일한 평문을 갖는다고 하더라도 암호화될 때 난수에 의해 서로 다른 암호문으로 구성될 수 있다는 점이다. 또한, 암호화된 데이터는 일반적으로 암호화 전의 데이터보다 더 큰 크기를 가진다. 이어서, 도 3b의 암호화된 이미지는 서버(200)로 전송되어 저장되었다고 가정한다. 서버(200)에서 클라이언트 단말(100)의 요청에 따라 FIR 필터를 통한 영상처리를 수행하는 경우, 이미지를 구성하는 픽셀들을 3x3과 같은 소정의 크기의 부분 픽셀 집합들로 분할 하여 FIR 필터에 맞게 수정한 후, 도 3c와 같이 각 부분 픽셀 집합 별로 FIR 필터를 적용한다. 도 3c는 Sharpening Filter에 대하여 연산한 결과를 나타낸 것이다. 이때, $n-1$ 은 모듈러 공간의 특성상 -1과 동일한 값을 갖는다.

[0041]

이후, 영상처리부(220)가 Paillier Cryptosystem의 특성을 이용해 각 부분 픽셀 집합 별로 모든 픽셀들의 암호문을 서로 곱하게 되면, 곱해진 데이터는 평문들의 합에 대한 암호화 상태를 나타내게 된다. 이를 일반화 할 경우 수학식 7과 같이 정의할 수 있다.

수학식 7

$$E[m,n] = \prod_{i=-N}^N \prod_{j=-N}^N E[m-i, n-j]^{b_{i,j}}$$

$$= E\left(\sum_{i=-N}^N \sum_{j=-N}^N b_{i,j} x[m-i, n-j]\right)$$

[0042]

[0043]

전송부(230)는 영상처리부(220)에 의해 영상처리된 이미지를 클라이언트 단말(100)로 전송한다. 클라이언트 단말(100)에서는 암호화된 이미지를 비밀키를 통하여 복호화하게 되며, 복호화에 따라 각 픽셀들의 평문들이 합해진 상태의 이미지가 제공되므로, 즉, 영상처리가 수행된 상태의 이미지가 제공되므로, 사용자는 클라이언트 단말(100)에서의 오랜 연산과정을 거칠 필요없이 영상처리된 이미지를 수신할 수 있다.

[0044]

도 4a 및 도 4b를 참조하면, 도 4a는 암호화되기 전의 원본 이미지를 나타내는 것이며, 도 4b는 서버(200) 내에서 암호화 상태로 FIR 필터(예를 들어, Sharpening Filter)를 통한 영상처리가 수행된 후 클라이언트 단말(100)에서 복호화된 이미지를 나타내는 것이다. 도 4a와 도 4b를 비교해보면, FIR 필터에 의해 확실히 더욱 선명해진 결과가 도출된 것을 확인할 수 있다.

[0045]

한편, 추가 실시예로서, 암호화된 이미지는 하나의 행(row) 또는 열(column)에 속한 모든 픽셀마다 암호화된 이미지일 수 있다. 상술한 암호화 과정에서는 하나의 픽셀마다 하나의 암호문을 생성해야 하므로, 암호화된 이미지 파일은 많은 용량을 차지하게 된다. 그러나, 하나의 픽셀 단위가 아닌, 각 행 또는 열에 배치된 복수의 픽셀 단위로 암호화될 경우, 암호문의 개수를 대폭 줄일 수 있게 되므로 암호화된 이미지의 용량을 줄일 수 있으며, 추후에 이루어질 FIR (Finite Impulse Response) 필터 처리도 신속히 이루어질 수 있다.

[0046]

구체적으로, 각 픽셀값마다 zero padding을 수행하여 각 픽셀값들을 네 자리 숫자로 변환한 후, 하나의 행 내에 속한 모든 픽셀값들을 연결하는 cascading을 수행할 경우, 하나의 행에 속한 복수의 픽셀값에 대한 하나의 정수값이 생성된다. 이어서, FIR 필터를 적용할 경우, 각 정수값을 단위로 하여 필터가 적용됨으로써, 암호화된 이미지 전체에 대한 필터 작업이 수행될 수 있다.

[0047]

예를 들어, 4x4 픽셀 구조의 이미지가 있으며, 가장 상단 행에 속한 각 픽셀값들은 좌측에서부터 순차적으로 41, 23, 44, 21로 구성된다고 가정한다. 이때, 각 픽셀마다 zero padding을 수행하면, 각 픽셀값들은 0041, 0023, 0044, 0021로 변환된다. 그리고 변환된 숫자들을 연결하는 cascading을 수행하면 가장 상단 행에 대한 픽셀값은 0041002300440021과 같이 하나의 정수값으로 취급될 수 있다. 이와 같이 각 행마다 암호문을 생성할 수 있다. 그리고, FIR 필터 적용을 통해, 0041002300440021에 10000이라는 정수를 곱할 경우, 각 픽셀값이 좌측으로 하나씩 시프트된 형태의 암호문(00410023004400210000)이 생성된다. 이때, 본래의 값인 0041002300440021과 00410023004400210000을 더할 경우, 좌우 방향으로 서로 이웃한 픽셀이 더해지는 효과가 나타날 수 있다.

[0048]

이하, 도 5를 참조하여, 본 발명의 일 실시예에 따르는 암호화 상태의 이미지에 대한 영상처리방법에 대하여 구체적으로 설명하도록 한다.

[0049]

이하의 영상처리방법은 상술한 영상처리장치에 의해 수행되는 것으로서, 이하에서 생략된 내용이라고 하더라도 상술한 내용으로 같음될 수 있다.

[0050]

먼저, 영상처리장치는 클라이언트 단말(100)로부터 암호화된 이미지를 수신하고 저장한다(S510). 이때, 이미지는 Paillier Cryptosystem 기법을 통해 암호화된 것일 수 있다.

[0051]

이어서, 영상처리장치는 클라이언트 단말(100)의 요청에 따라, 암호화 상태에서 이미지에 대하여 FIR 필터를 통한 영상처리를 수행한다(S520). 구체적으로, FIR 필터에 맞게 이미지 내 전체 픽셀들을 여러 개의 부분 픽셀 집합으로 분할하고, 각 부분 픽셀 집합에 대하여 암호화된 상태 그대로 FIR 필터를 적용한다. 예를 들어, 가운데 암호화된 픽셀값은 높은 양(+)의 가중치로 연산되고 가장자리의 암호화된 픽셀값은 음(-)의 가중치로 연산될 수 있다. 그리고 연산된 암호화된 픽셀값들은 서로 곱해짐으로써 영상처리 과정이 완료될 수 있다.

[0052]

영상처리장치는 영상처리된 이미지를 암호화된 상태 그대로 클라이언트 단말(100)에 전송한다(S530). 서로 곱셈 처리된 암호문들은 복호화를 통해 서로 합해진 평문들로 변환되며, 서로 합해진 평문에 대응하는 이미지는 FIR

필터를 통해 영상처리된 상태의 이미지를 나타내게 된다.

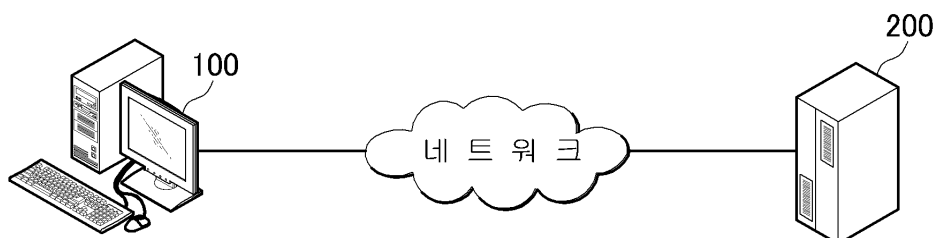
- [0053] 이와 같이, 본 발명의 일 실시예는 클라우드 서버에서 영상처리가 암호화된 채로 진행되어져 사용자가 안전하게 이미지를 클라우드 서버에 저장하고 편집할 수 있도록 할 수 있다. 사용자가 온라인 상으로 이미지를 편집하더라도 이미지의 원본, 편집 과정의 데이터가 모두 서버에 저장되기는 하나, 서버는 이미지에 대한 어떠한 정보도 얻어낼 수 없게 되므로, 서버 관리자나 해킹에 의한 노출 우려가 있더라도 데이터 소유자의 프라이버시를 보호할 수 있다. 이를 통해 본 발명의 일 실시예는 클라우드 서비스 환경에서의 영상 처리 과정에 보안성을 부여할 수 있다.
- [0054] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다.
- [0055] 본 발명의 방법 및 시스템은 특정 실시예와 관련하여 설명되었지만, 그것들의 구성 요소 또는 동작의 일부 또는 전부는 범용 하드웨어 아키텍처를 갖는 컴퓨터 시스템을 사용하여 구현될 수 있다.
- [0056] 진술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.
- [0057] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

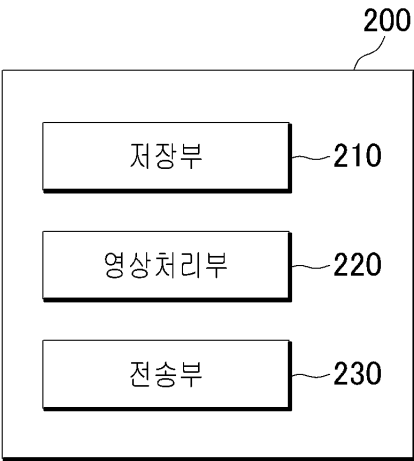
- [0058] 100: 클라이언트 단말 200: 서버
- 210: 저장부 220: 영상처리부
- 230: 전송부

도면

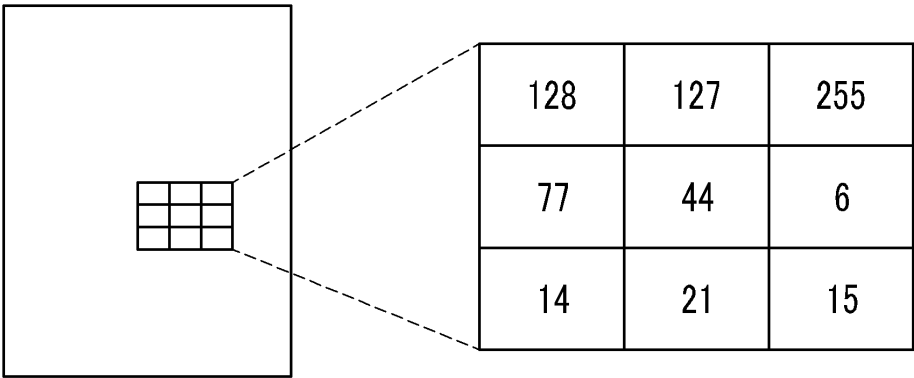
도면1



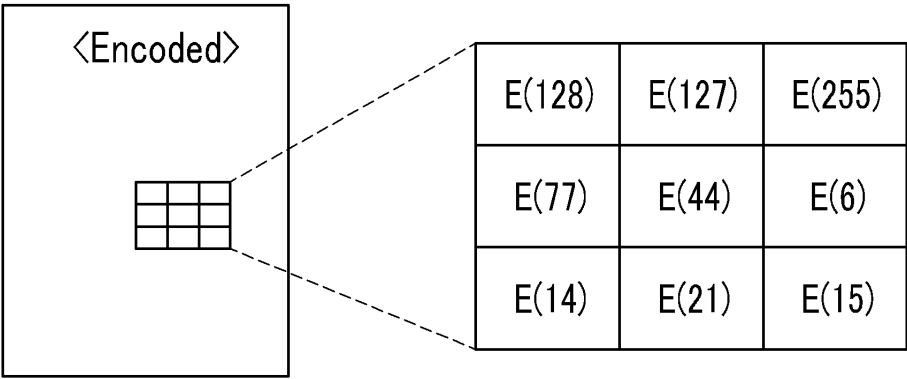
도면2



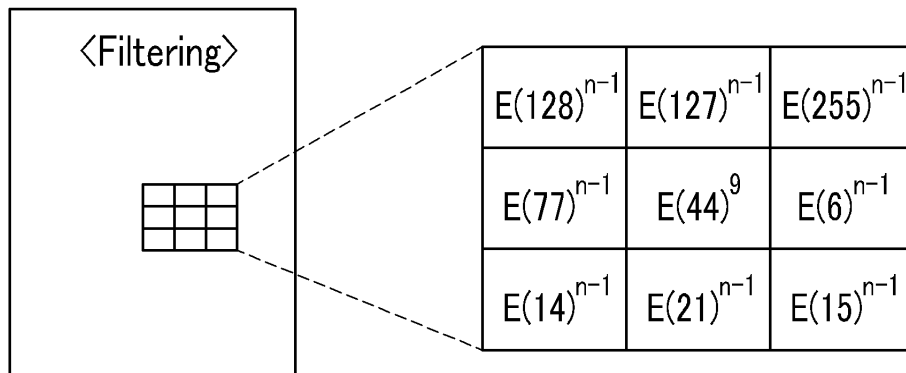
도면3a



도면3b



도면3c



도면4a



도면4b



도면5

