



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0006847
(43) 공개일자 2012년01월19일

(51) Int. Cl.

H04N 7/24 (2011.01)

(21) 출원번호 10-2010-0067536

(22) 출원일자 2010년07월13일

심사청구일자 없음

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가 1

(72) 발명자

정용화

대전광역시 유성구 은구비로 31, 505동 402호 (지족동, 열매마을아파트5단지)

이성주

서울특별시 마포구 월드컵북로22길 20 (성산동)

(뒷면에 계속)

(74) 대리인

특허법인충현

전체 청구항 수 : 총 11 항

(54) 정지 영상 압축 / 암호화 방법 및 압축 / 암호화 시스템

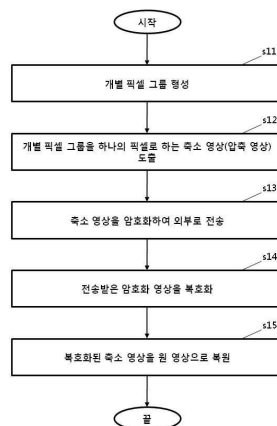
(57) 요약

본 발명은 무선 센서 네트워크(Wireless Sensor Network: WSN)처럼 저전력 소모(저에너지 소모)가 요구되고 아울러 정보 처리의 실시간성이 요구되는 환경에 최적화된 정지 영상 압축 / 암호화 방법에 관한 것이다.

본 명세서에서 개시하는 정지 영상 압축 / 암호화 방법은 $m \times n$ 크기(m 과 n 은 자연수)를 갖는 정지 영상(원 영상)의 한 픽셀과 상기 한 픽셀의 근접한 픽셀들로 각 개별 픽셀 그룹을 형성하는 단계; 상기 각 개별 픽셀 그룹을 하나의 픽셀로 하는 $j \times k$ 크기의 축소 영상을 도출하는 단계; 및 상기 축소 영상을 암호화하는 단계를 포함하여 본 방법 발명의 과제를 해결한다.

본 발명은 정지 영상의 압축에 소요되는 연산을 획기적으로 줄여, 압축에 요구되는 시간 및 에너지를 획기적으로 감소시킬 수 있고, 아울러 축소 영상(압축 영상)을 외부로 전송하는 경우 압축 영상에 대한 암호화를 통해 원 영상 전체에 대한 암호화 효과를 볼 수 있으므로 원 영상 전체에 대해 완전한 보안성을 확보할 수 있다.

대표도 - 도1a



(72) 발명자

이은지

경상북도 경산시 정평동 130 현대타운 106-602

정서현

서울특별시 동작구 동작대로29길 119, 102동 1506호 (사당동, 극동아파트)

반성범

광주광역시 동구 서석동 375번지 조선대학교 제어계측로봇공학과

이 발명을 지원한 국가연구개발사업

과제고유번호 20090086148

부처명 한국연구재단

연구관리전문기관

연구사업명 중견연구자지원사업

연구과제명 멀티미디어 데이터 압축 특성을 이용한 기밀성 및 무결성 보장 전용 하드웨어 개발

기여율

주관기관 고려대학교 산학협력단

연구기간 2009년 09월 01일 ~ 2010년 08월 31일

특허청구의 범위

청구항 1

(a) $m \times n$ 크기(m 과 n 은 자연수)를 갖는 정지 영상(원 영상)의 한 픽셀과 상기 한 픽셀의 근접한 픽셀들로 각 개별 픽셀 그룹을 형성하는 단계; 및

(b)상기 각 개별 픽셀 그룹을 하나의 픽셀로 하는 $j \times k$ 크기의 축소 영상을 도출하는 단계를 포함하는 정지 영상 압축 / 암호화 방법.

여기서, 상기 j 와 k 는 자연수이고 $[1 \leq j \leq m \text{ and } 1 \leq k \leq n]$ 또는 $[1 \leq j < m \text{ and } 1 \leq k \leq n]$ 또는 $[1 \leq j < m \text{ and } 1 \leq k < n]$ 이다.

청구항 2

제 1 항에 있어서,

(c)상기 도출된 축소 영상을 암호화하는 단계를 더 포함하는 것을 특징으로 하는 정지 영상 압축 / 암호화 방법.

청구항 3

제 2 항에 있어서, 상기 암호화는

AES(Advanced Encryption Standard) 암호화를 포함하는 것을 특징으로 하는 정지 영상 압축 / 암호화 방법.

청구항 4

제 1 항 내지 제 3 항 중 어느 한 항에 있어서, 상기 (b)단계는

(b1)상기 각 개별 픽셀 그룹의 픽셀값들의 평균값을 산출하는 단계; 및

(b2)상기 산출된 평균값을 상기 하나의 픽셀값으로 지정하는 단계를 포함하는 것을 특징으로 하는 정지 영상 압축 / 암호화 방법.

청구항 5

제 4 항에 있어서,

상기 축소 영상을 상기 원 영상으로의 복원하는 경우, 상기 복원은 바이큐빅 보간법에 의한 보간을 통해 이루어지는 것을 특징으로 하는 정지 영상 압축 / 암호화 방법.

청구항 6

제 4 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 판독 가능한 기록 매체.

청구항 7

일정 크기($m \times n$, m 과 n 은 자연수)를 갖는 정지 영상(원 영상)의 한 픽셀과 상기 한 픽셀의 근접한 픽셀들로 각 개별 픽셀 그룹을 형성하는 픽셀 그룹 형성부; 및

상기 각 개별 픽셀 그룹을 하나의 픽셀로 하는 $j \times k$ 크기의 축소 영상을 도출하는 축소 영상 도출부를 포함하는 정지 영상 압축 / 암호화 시스템.

여기서, 상기 j 와 k 는 자연수이고 $[1 \leq j \leq m \text{ and } 1 \leq k \leq n]$ 또는 $[1 \leq j < m \text{ and } 1 \leq k \leq n]$ 또는 $[1 \leq j < m \text{ and } 1 \leq k < n]$ 이다.

청구항 8

제 7 항에 있어서,

상기 도출된 축소 영상을 암호화하는 암호화부를 더 포함하는 것을 특징으로 하는 정지 영상 압축 / 암호화 시스템.

템.

청구항 9

제 8 항에 있어서, 상기 암호화는

AES(Advanced Encryption Standard) 암호화를 포함하는 것을 특징으로 하는 정지 영상 압축 / 암호화 시스템.

청구항 10

제 7 항 내지 제 9 항 중 어느 한 항에 있어서, 상기 축소 영상 도출부는

상기 각 개별 픽셀 그룹의 픽셀값들의 평균값을 산출하는 평균값 산출부; 및

상기 산출된 평균값을 상기 하나의 픽셀값으로 지정하는 픽셀값 지정부를 포함하는 것을 특징으로 하는 정지 영상 압축 / 암호화 시스템.

청구항 11

제 10 항에 있어서,

상기 축소 영상을 상기 원 영상으로의 복원하는 복원부를 더 포함하고, 상기 복원은 바이큐빅 보간법에 의한 보간을 통해 이루어지는 것을 특징으로 하는 정지 영상 압축 / 암호화 시스템.

명세서

기술분야

[0001] 본 발명은 정지 영상 압축 / 암호화 방법 및 압축 / 암호화 시스템에 관한 것으로, 보다 상세하게는 무선 센서 네트워크(Wireless Sensor Network: WSN)처럼 저전력 소모(저에너지 소모)가 요구되고 아울러 정보 처리의 실시간성이 요구되는 환경에 최적화된 정지 영상 압축 / 암호화 방법 및 압축 / 암호화 시스템에 관한 것이다.

배경기술

[0002] 인터넷은 모든 시스템의 네트워크화를 가능하게 하고 있으며, 요즘은 특히 유비쿼터스(ubiquitous) 시대의 도래로 언제 어디서나 네트워킹이 가능하도록 무선 네트워크로 통신 환경이 진화하고 있다. 이중에서 특히 WSN은 그 적용 영역이 무한한 관계로 최근 많은 각광을 받고 있다.

[0003] WSN은 사물에 대한 인식정보 또는 주변의 환경정보를 감지할 수 있는 센서가 탑재된 센서 노드를 통해 무선 센서 네트워크를 구성하고, 다양한 센서들을 통해 입력되는 정보를 '실시간으로' 네트워크를 통해 외부와 연결하여 정보를 처리하고 관리하는 네트워크 시스템을 의미한다. WSN은 궁극적으로 모든 사물에 컴퓨팅 및 통신 기능을 부여함으로써, 언제나(anytime), 어디서나(anywhere) 네트워크, 디바이스 또는 서비스에 관계없이 통신 가능한 환경의 구현을 목적으로 한다.

[0004] 한편 WSN을 형성하는 센서 노드(node)들의 대부분은 배터리에 의해 동작되는 특성으로 인하여, WSN에서는 정보의 처리량이나 지연 등과 같은 정보 전송 품질을 높이는 것보다 전력 소모(power consumption)를 최대한으로 줄이는 즉, 에너지 효율을 높이는 것이 더욱 중요하게 다뤄지고 있다.

[0005] 아울러 최근 WSN의 데이터 전송과정에서 보안(security)에 대한 이슈도 증가하고 있는데, 이것을 위하여 기존의 암호화 기술을 적용하게 된다면 자원 제약적인 센서 노드의 부하가 커진다. 따라서 정지 영상(still image)과 같은 고용량 정보(데이터)를 암호화하여 전송함에 있어서 WSN과 같이 자원 제약적인 네트워크 환경에서는 컴퓨팅 파워(computing power)를 효율적으로 활용할 필요가 있다.

[0006] 이러한 필요에 부응하여 노드-노드 간 또는 노드-서버 간 정보의 송수신 측면에서 고려해 보면, 고용량 정보를 효율적으로 압축하여 에너지 효율을 높이는 방안이 있으며, 암호화 측면에서도 정보에 대한 전체 암호화 대신 일부만을 선택적으로 부분 암호화하여 에너지 효율을 높이는 방안이 있다.

[0007] 고용량 정보의 대표적인 예로 정지 영상(still image)을 들 수 있는데, 정지 영상 자체를 압축/복원하는 방안으로는 JPEG 등 기 공지된 여러 방안들이 있으나, 이들 기존 방안은 압축/복원을 위해 DCT(Discrete Cosine Transform) 등 매우 복잡한 수학적 과정을 거쳐야 하므로 이를 위한 전력 소모가 많고, 따라서 WSN에서의 중요

한 화두인 에너지 효율의 향상(전력 소모의 감소)과 WSN에서의 또 하나의 중요한 팩터인 정보 처리의 실시간성을 고려해볼 때 기존의 동영상 압축 방안을 WSN에 그대로 적용하기에는 문제가 있다.

[0008] 아울러 상기한 부분 암호화를 이용할 경우, WSN 환경에서 에너지 효율성을 높일 수 있는 효과는 어느 정도 있는 반면에 암호분석 등을 통하여 부분 암호를 공격할 수 있는 문제도 있다.

[0009] 따라서 WSN 환경에서 정지 영상과 관련된 제반 처리시에 에너지 효율성을 증가시키면서 동시에 보안성을 훼손시키지 않는 방안이 필요하다.

발명의 내용

해결하려는 과제

[0010] 본 발명은 상기와 같은 문제를 해결하기 위해 창안된 것으로, 본 발명이 해결하려는 과제는 WSN에서처럼 고용량 정지 영상의 에너지 효율적(energy-effective) 송수신이 요구되는 환경에서 이의 전제가 되는 고용량 정지 영상의 효과적인 압축 방안을 제안하는 것이다. 아울러 정지 영상의 외부 전송 실행시에 보안성을 확보하는 방안도 제안하는 것이다.

과제의 해결 수단

[0011] 상기와 같은 과제의 해결을 위하여, 본 명세서에서 개시하는 정지 영상 압축 / 암호화 방법은

[0012] $m \times n$ 크기(m 과 n 은 자연수)를 갖는 정지 영상(원 영상)의 한 픽셀과 상기 한 픽셀의 근접한 픽셀들로 각 개별 픽셀 그룹을 형성하는 단계; 및 상기 각 개별 픽셀 그룹을 하나의 픽셀로 하는 $j \times k$ 크기의 축소 영상을 도출하는 단계를 포함하여 본 방법 발명의 과제를 해결한다.

[0013] 본 명세서에서 개시하는 정지 영상 압축 / 암호화 방법은 상기 도출된 축소 영상을 암호화하는 단계를 더 포함하여서도 본 방법 발명의 과제를 해결한다.

[0014] 상기와 같은 과제의 해결을 위하여, 본 명세서에서 개시하는 정지 영상 압축 / 암호화 시스템은

[0015] $m \times n$ 크기(m 과 n 은 자연수)를 갖는 정지 영상(원 영상)의 한 픽셀과 상기 한 픽셀의 근접한 픽셀들로 각 개별 픽셀 그룹을 형성하는 픽셀 그룹 형성부; 및 상기 각 개별 픽셀 그룹을 하나의 픽셀로 하는 $j \times k$ 크기의 축소 영상을 도출하는 축소 영상 도출부를 포함하여 본 시스템 발명의 과제를 해결한다.

[0016] 본 명세서에서 개시하는 정지 영상 압축 / 암호화 시스템은 상기 도출된 축소 영상을 암호화하는 암호화부를 더 포함하여서도 본 시스템 발명의 과제를 해결한다.

[0017] 이때, 상기 j 와 k 는 자연수이고 $[1 \leq j \leq m \text{ and } 1 \leq k \leq n]$ 또는 $[1 \leq j < m \text{ and } 1 \leq k \leq n]$ 또는 $[1 \leq j < m \text{ and } 1 \leq k < n]$ 이다.

발명의 효과

[0018] 본 발명은 정지 영상의 압축에 소요되는 연산을 획기적으로 줄여, 압축에 요구되는 시간 및 에너지를 획기적으로 감소시킬 수 있고, 아울러 축소 영상(압축 영상)을 외부로 전송하는 경우 압축 영상에 대한 암호화를 통해 원 영상 전체에 대한 암호화 효과를 볼 수 있으므로 원 영상 전체에 대해 완전한 보안성을 확보할 수 있다.

도면의 간단한 설명

[0019] 도 1a 내지 도 1b는 본 방법 발명의 바람직한 일 흐름을 제시한 도면이다.

도 2a 내지 도 2b는 본 시스템 발명의 바람직한 일 구성을 제시한 도면이다.

도 3a는 본 발명의 동작 설명을 위해 제시한 원 영상 및 압축 영상의 일례이다.

도 3b는 개별 픽셀 그룹 설정의 일례를 제시한 도면이다.

도 3c는 바이큐빅 보간법을 설명하기 위한 일례를 제시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0020] 본 발명을 실시하기 위한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하려는 과제의 해결

방안의 개요를 우선 제시한다.

- [0021] 본 발명은 특히 WSN과 같이 에너지 소모를 최소로 요하고 아울러 정보의 실시간 처리가 요구되는 환경에서 고용량 정지 영상의 효율적인 압축을 통해 고용량 정지 영상의 에너지 효율적인 송수신을 꾀하는 것이다. 이를 위해 본 발명은 에너지 효율적인 송수신 및 실시간 처리의 전제가 되는 고용량 정지 영상의 효율적인 압축 방안을 제안하는데, 기존의 압축 방안에서 적용되었던 복잡한 연산 과정(대표적인 예로 DCT)을 배제하고 매우 간단한 연산 과정만을 통해 정지 영상(이하 '원 영상'과 혼용한다)보다 작은 영상(축소 영상)을 구현하여 정지 영상의 압축을 꾀한다. 압축은 정보량을 감소시키는 것을 의미하는데, 본 발명에서는 영상 정보량의 감소를 영상의 '크기'를 줄이는 개념으로 실현하는 것이다.
- [0022] 아울러 본 발명은 이러한 압축을 통하여 획득한 축소 영상을 암호화하여, 원 영상을 외부로 전송시에 원 영상 전체에 대한 암호화 효과를 볼 수 있도록 한다.
- [0023] 이하, 본 발명을 실시하기 위한 구체적인 내용을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.
- [0024] 도 1a 및 도 1b는 본 방법 발명의 바람직한 일 흐름을 제시한 도면이고, 도 2a 및 도 2b는 본 시스템 발명의 바람직한 일 구성을 제시한 도면이다. 도 3a는 본 발명의 동작 설명을 위해 제시한 원 영상 및 축소 영상(압축 영상)의 일례이다.
- [0025] 픽셀 그룹 형성부(21)는 $m \times n$ 크기(m 과 n 은 자연수)를 갖는 정지 영상(원 영상)의 한 픽셀(A)과 한 픽셀(A)의 근접한 픽셀들로 각 개별 픽셀 그룹(j, k)을 형성한다(s11). 여기서, j 와 k 는 자연수이고 $[1 \leq j \leq m \text{ and } 1 \leq k \leq n]$ 또는 $[1 \leq j < m \text{ and } 1 \leq k \leq n]$ 또는 $[1 \leq j < m \text{ and } 1 \leq k < n]$ 이다. 이때 각 개별 픽셀 그룹(j, k)의 형성은 매우 다양하게 이루어질 수 있는데, 예를 들어 한 픽셀(A)과 한 픽셀(A)의 좌우 하나씩의 픽셀의 세 개의 픽셀을 하나의 픽셀 그룹으로 형성하던지 한 픽셀(A)과 한 픽셀(A)의 상하 각각 하나의 픽셀의 세 개의 픽셀을 하나의 픽셀 그룹으로 형성하던지 등이다. 픽셀 그룹은 이처럼 WSN이 구축된 환경, WSN의 복잡도, 노드의 개수, 영상 정보의 송신 빈도 등 어느 하나의 고정된 기준에 의해서가 아닌 제반 기준(환경)에 따라 결정된다.
- [0026] 도 3b에는 일례로 한 픽셀(A)과 한 픽셀(A)에 인접한(adjacent) 8개의 픽셀로 이루어진 9개의 픽셀(붙게 음영 처리된 부분)을 개별 픽셀 그룹(j, k)으로, 한 픽셀(B)과 한 픽셀(B)에 인접한 8개의 픽셀(푸르게 음영 처리된 부분)로 이루어진 9개의 픽셀을 또 다른 개별 픽셀 그룹($j+1, k$)으로 형성한 예를 보이고 있다.
- [0027] 축소 영상 도출부(22)는 개별 픽셀 그룹(j, k)을 하나의 픽셀로 하는 축소 영상을 원 영상으로부터 도출하여(s12), 원 영상을 압축한 영상을 생성한다. 즉, 축소 영상 도출부(22)는 원 영상의 '크기'의 축소를 통해 원 영상의 정보량을 압축하는 것이다.
- [0028] 구체적으로 본 발명에서 축소 영상의 도출(s12)은 개별 픽셀 그룹(j, k)의 픽셀값들의 평균값을 이용하며, 기존의 압축 방식에서의 DCT와 같은 복잡한 연산을 통해 압축(축소)을 행하는 것이 아니다.
- [0029] 먼저 평균값 산출부(221)에 의해 각 개별 픽셀 그룹의 픽셀값들의 평균값이 산출된다(s121). 도 3b에 제시된 개별 픽셀 그룹의 예를 참조하여 산출되는 개별 픽셀 그룹(j, k)의 평균값($M_{j,k}$)과 개별 픽셀 그룹($j+1, k$)의 평균값($M_{j+1,k}$)은 다음과 같다.
- [0030]
$$M_{j,k} = [P_{(a-1,b-1)} + P_{(a,b-1)} + P_{(a+1,b-1)} + P_{(a-1,b)} + P_{(a,b)} + P_{(a+1,b)} + P_{(a-1,b+1)} + P_{(a,b+1)} + P_{(a+1,b+1)}]/9.$$
- [0031]
$$M_{j+1,k} = [P_{(a+2,b-1)} + P_{(a+3,b-1)} + P_{(a+4,b-1)} + P_{(a+2,b)} + P_{(a+3,b)} + P_{(a+4,b)} + P_{(a+2,b+1)} + P_{(a+3,b+1)} + P_{(a+4,b+1)}]/9.$$
- [0032] 여기서 $P_{(a,b)}$ 는 한 픽셀(A)의 픽셀값을 의미하고, $P_{(a+3,b)}$ 는 한 픽셀(B)의 픽셀값을 의미하며, 상기 식에서 첫 번째 항부터 차례로 해당 픽셀의 픽셀값을 의미한다. 그리고 a 와 b 는 각각 한 픽셀(A)의 2차원 평면상의 가로축의 좌표값 및 세로축의 좌표값으로 $1 \leq a \leq m, 1 \leq b \leq n$ 을 만족하는 자연수이다.
- [0033] 픽셀값 지정부(222)는 산출된 평균값($M_{j,k}$)을 상기 하나의 픽셀의 픽셀값으로 지정하여(s122) 축소 영상(압축 영상)을 도출한다. 따라서 도출되는 축소 영상(압축 영상)의 크기는 $j \times k$ 가 된다. 위의 픽셀 그룹 설정예에 의하면, 만일 원 영상의 크기가 $m \times n = 360 \times 240$ 이라 하면, 축소 영상의 크기는 $j \times k = 120 \times 80$ 이 된다. 크기의 비는

9:1이 된다.

- [0034] 개별 픽셀 그룹(j, k)의 픽셀값으로 산출된 평균값($M_{j,k}$)을 상기 하나의 픽셀의 픽셀값으로 지정하는 이유는 압축을 위한 연산량의 감소를 피할 수 있고, 아울러 원 영상의 정보 손실을 상대적으로 줄일 수 있기 때문이다. 즉, 기존의 압축 방안은 DCT와 같은 복잡한 연산을 필요로 하고 아울러 손실 압축(lossy compression)에 근거하기 때문에 정보의 무결성(완전성)을 보장하기 어렵다. 그러나 평균값($M_{j,k}$)을 축소 영상의 픽셀값으로 지정하는 경우에는 상대적으로 압축에 요구되는 연산량을 획기적으로 감소시킬 수 있고(요구되는 연산이 더하기, 나누기 만이다), 통상적으로 어떤 정보의 평균값은 개별 정보(원 정보, raw data)의 속성을 가장 많이 함유하고 있으므로 정보의 완전성을 상대적으로 더 기할 수 있다.
- [0035] 한편 본 발명은 WSN에 적용되는 것을 지향하므로 필연적으로 정지 영상의 외부로의 전송이 수반된다. 따라서 영상의 전송 과정 중의 보안성 확보도 중요한 이슈가 된다. 센서 노드에서 특정 이벤트의 검출 시 정지 영상을 전송하여야 하는 경우, 그 영상의 내용은 기밀을 유지해야 경우가 대부분이고 아울러 실시간 암호화 및 실시간 전송 처리가 요구되는데, 통상적으로 영상에 대한 암호화 자체의 계산량이 너무 과중하기 때문에 WSN 환경에서는 실시간 암호화 및 실시간 전송 처리가 에너지 효율 측면에서 문제가 될 수 있다.
- [0036] 이러한 문제를 해결하기 위해 별도의 암호화 전용 하드웨어를 사용하거나 전송 대상 영상 정보를 부분적으로 암호화하여야 하는데, 전용 하드웨어를 사용하는 경우에는 하드웨어를 구동시키기 위한 부하(load)가 가중되는 문제가 있고 부분적 암호화의 경우에는, 암호화를 '부분적'으로만 하기 때문에 정당 권원 없는 자등이 암호화되지 아니한 정보로부터 전체 정보를 쉽게 유추해낼 수 있는 가능성이 있으므로 완전한 보안성(기밀성) 확보가 어렵다.
- [0037] 그러나 본 발명은 WSN이 구축된 환경에 맞게 원 영상을 충분히 축소하고, 외부로 전송시에 암호화부(23)에 의해 축소 영상을 암호화하여 전송하기(s13) 때문에 원 영상 정보'전체'에 대한 암호화 효과를 볼 수 있다. 환경에 맞게 축소된 영상에 대하여 암호화 및 전송이 이루어지므로 실시간 암호화 및 전송 처리가 가능하다. 이때 암호화는 여러 방식이 있을 수 있으나(예를 들어 watermarking 기법 등), WSN처럼 에너지 효율이 높아야 할 필요가 있는 네트워크 환경에서는 정보의 암호화를 위한 연산량이 가장 작다고 알려진 AES(Advanced Encryption Standard)에 의해 이루어짐이 바람직하다.
- [0038] AES는 암호화 대상 정보를 블록 단위로 암호화하는 방식으로 대칭키 암호화 표준(symmetric key encryption standard)이며 AES-128, AES-192, AES-256의 세 개의 블록 암호들로 이루어진다. 각 암호 블록은 128 비트의 블록 크기를 가지며, 각각 128, 192 및 256 비트의 키 크기(key size)를 갖는다.
- [0039] 본 시스템 발명은 암호화되어 전송된 축소 영상을 수신하는 노드 또는 서버가 원 영상을 확인할 수 있게 하기 위해 복호화부(24)에 의해 복호화된(s14) 축소 영상을 원 영상으로 복원하는(s15) 복원부(25)를 더 포함한다. 복원은 소정의 보간법을 통해 이루어진다.
- [0040] 보간법은 여러 가지 기법이 알려져 있다. 일반적으로 많이 사용되는 보간법은 바이큐빅 보간법(bicubic interpolation)이다. 이 보간법은 보간 대상 픽셀에 인접한 16개의 픽셀을 참조함으로써 보간 작업이 이루어진다. 또한, 주변 픽셀의 참조 방법은 3차 컨볼루션(convolution) 함수를 이용함으로써 픽셀간의 거리에 따라 비선형적인 가중치를 적용하여 기존에 보간 기법으로 많이 사용되었던 양선형 보간법(bilinear interpolation) 보다 뭉그러짐 현상이 적어 화질을 부드럽게 해주는 장점이 있다. 도 4는 주변 4*4 픽셀(A부터 P까지)을 참조하여 보간을 수행하는 바이큐빅 보간법의 예를 보여주고 있다. 이때, x, y는 픽셀의 위치 좌표이며, 0부터 1 사이의 정규화된 값을 가지며, 주변 픽셀과 3차 컨볼루션 함수를 이용하여 보간 대상 픽셀의 값이 구해진다.
- [0041] 본 방법발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.
- [0042] 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 유무선 네트워크를 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.
- [0043] 이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수

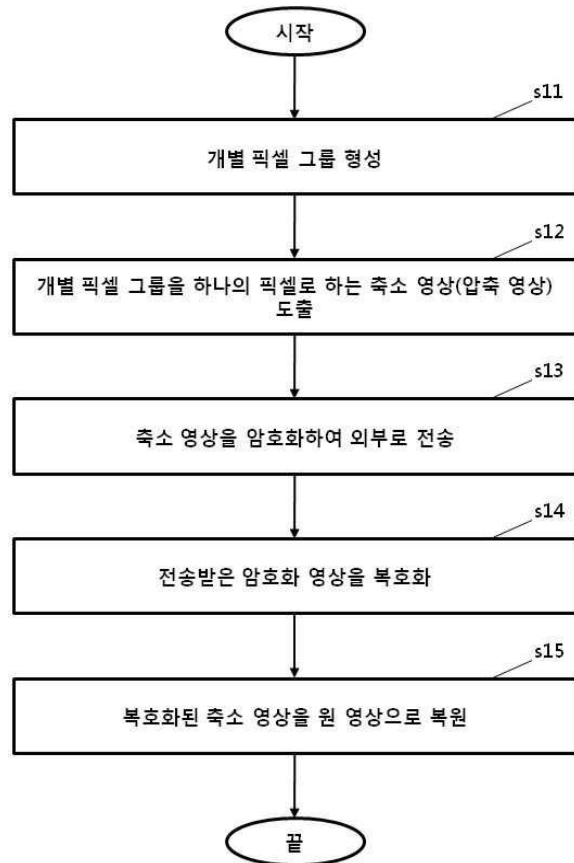
있음을 이해할 수 있을 것이다.

[0044]

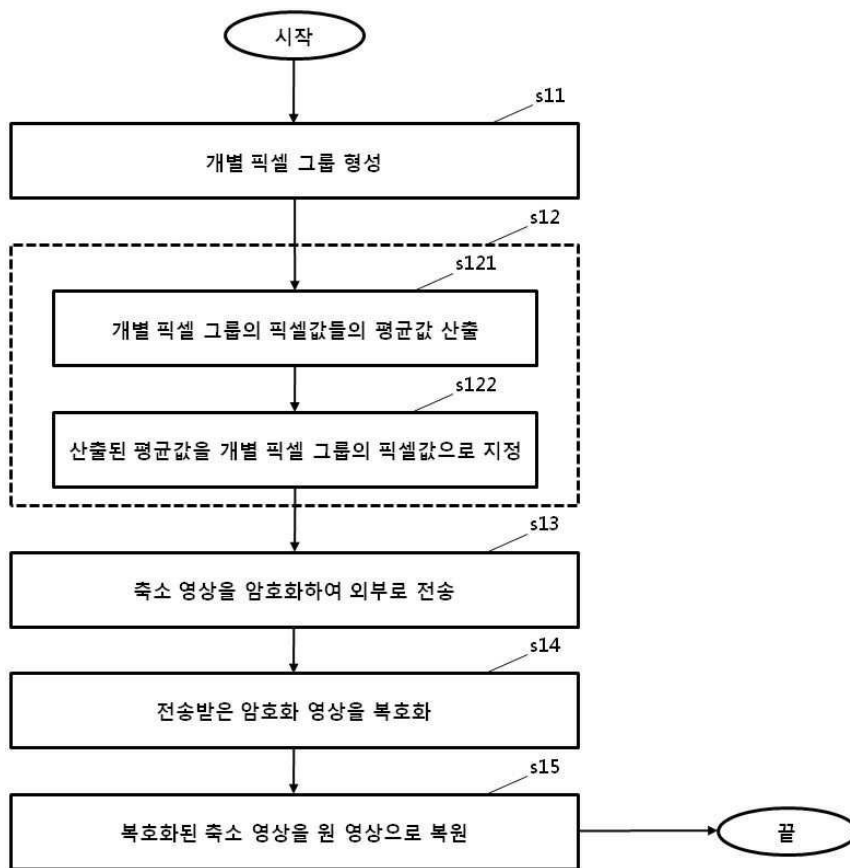
그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

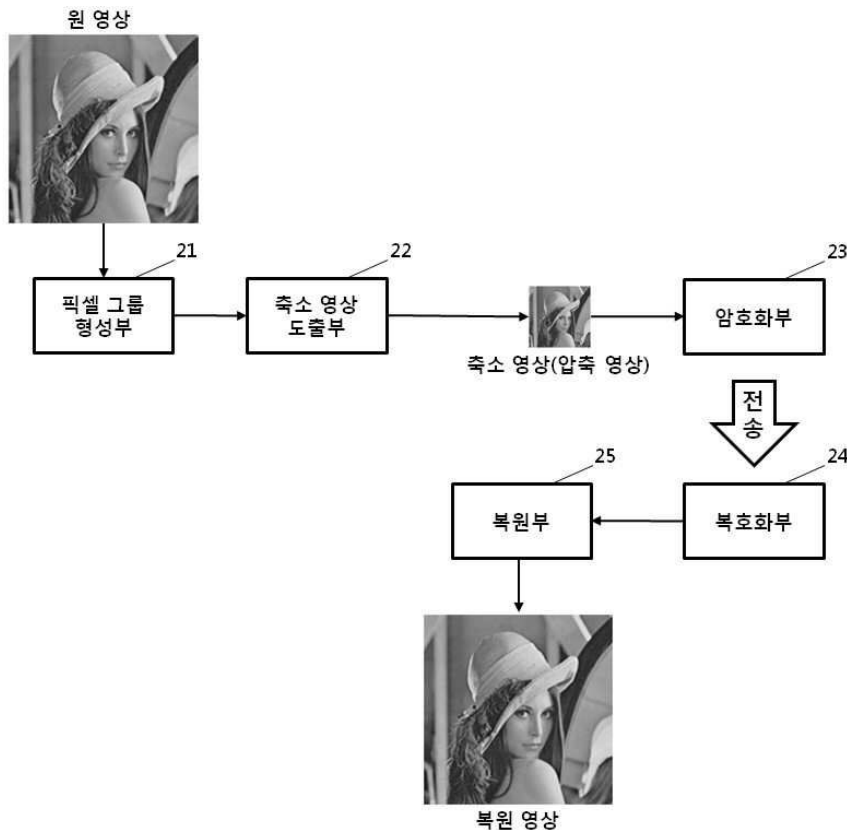
도면1a



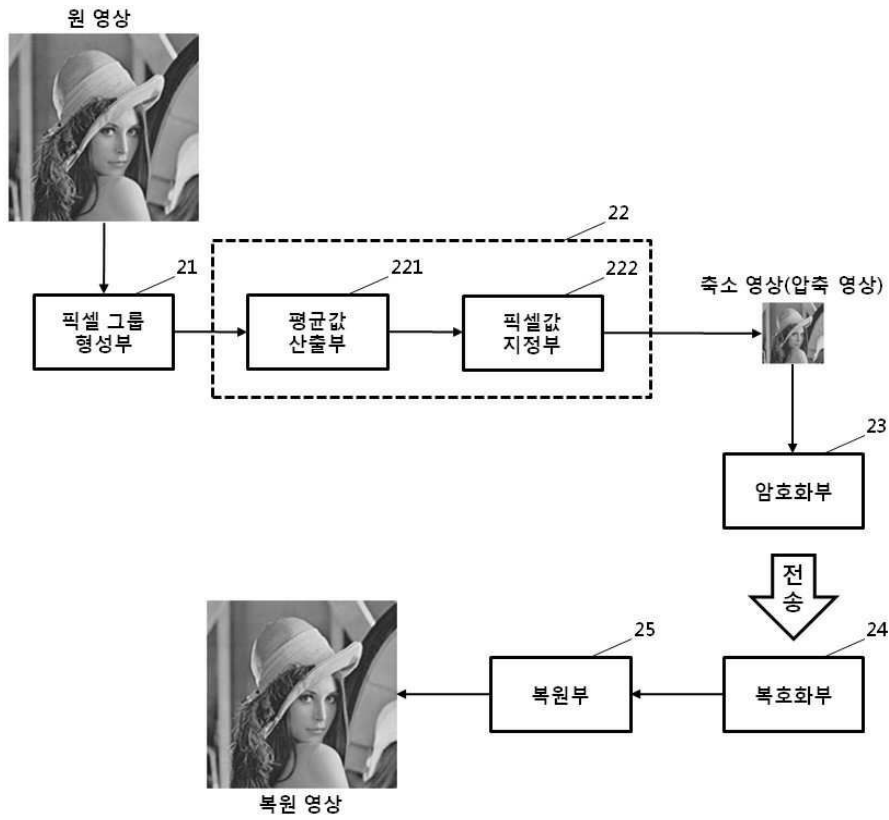
도면1b



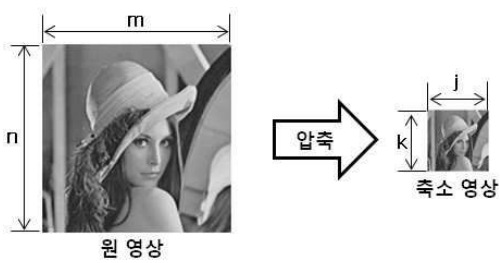
도면2a



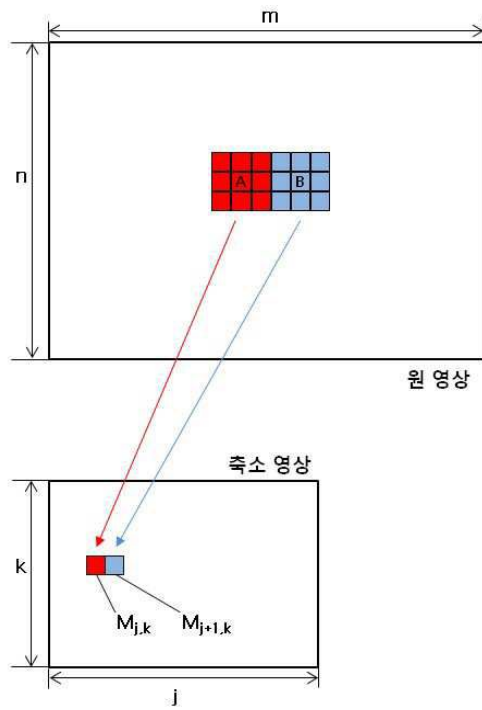
도면2b



도면3a



도면3b



도면3c

