트리구조를 이용한 이미지의 선택적 암호화에 관한 연구☆

A Study of Selective Encryption for Images using Tree Structures

한 명 묵* 김 금 실**
Myung-Mook Han Geum-Sil Kim

요 약

멀티미디어의 응용이 날로 빈번해지면서 유효한 데이터에 대한 저장과 전송의 기술에 아주 큰 수요가 나타났다. 많은 압축과 암호화를 결합한 방법들이 제기되어 왔지만 그들은 안전하지 못하거나 계산의 양이 너무 큰 단점이 있고 특히 모바일 기기에서의 무선통신에는 더욱더 부적합할 수밖에 없다. 본 논문에서는 새로운 해결책인 선택적 암호화를 제안한다. 본 논문에서는 quadtree와 zerotree에 기반 한 웨이블릿 압축 기법을 도입하여 압축된 데이터의 일부만을 암호화 하는 방법을 제안하였는데, 압축비율에 영향을 주지 않으면서 계산의 양을 줄임으로서 모바일 장치에서의 데이터 전송을 위하여 시간을 감소시키는 효과를 얻었다. 결론적으로 제안한 선택적 암호화 기법은 속도가 빠르고 안전하며 압축 성능을 감소시키지 않은 방법이라고 할 수 있다.

ABSTRACT

The increased popularity of multimedia applications places a great demand on efficient data storage and transmission techniques. Some methods have been proposed to combine compression and encryption together to reduce the overall processing time, but they are either insecure or intensive computationally. specially, they are unsuitable to wireless communication of mobile device. We propose a novel solution called partial encryption, We introduce quadtree and zerotree wavelet image compression in this paper, it reduces computation for date transmission in mobile device, and does not reduce the compression rate. In conclusion, the proposed partial encryption schemes are fast, secure, and do not reduce the compression performance of underlying compression algorithm.

☞ KeyWords : Quad tree, Zero tree, Selective encryption, Wavelet image compression

1. 서 론

월드 와이드 웹과 화상회의처럼 이미지와 비디오 어플리케이션의 사용은 최근 몇 년 동안 극적으로 증가했다. 통신영역이 넓고 용량이 제한될 때, 데이터는 압축되어 처리되는데 무선망을 사용할 때 대폭역의 제한 때문에 우리는 낮은 비트비율의 압축기법이 필요하고 또한 사용자의 정보를 보호해야 한다면 암호화 기법도 사용하게 된다. 예를 들면, 무선망에서 데이터를 전송하려고 할 때 아주 쉽게 침입자의 공격을 당할 수 있는데 관례적으로 적당한 압축 기법으로 생성된 이미지 데이터를 다시 독립적인 암호화 알고리즘으로 암호화한다. 복호화과정은 그 반대라고 볼 수 있다.

암호화나 복호화의 처리시간은 실시간 이미지와 비디오의 통신과 처리에서 해결해야 할 과제이다. 대부분의 경우에 압축 알고리즘과 압축을 푸는 알고리즘은 하드웨어가 가속되면 필요한 비트 전송률이 계속 부족할 수 있다. 거기에 암호화와 복호화 처리가 추가되면 실시간으로 안전하게 이미지를 전송하는데 더욱 큰 어려움이 있다. 암호화를 위한 하드웨어의 기능이 가속화 되는 만큼 더 유연하고 저렴한 소프트웨어를 구현해야 한다. 특히 “비디오폰”처럼 손에 휴대가 가능한

* 종신회원 : 경원대학교 IT대학 컴퓨터소프트웨어학과 부교수 mmhan@kyungwon.ac.kr
** 준 회 원 : 경원대학교 강사직 hakuna1103@hotmail.com
[2008/12/30 투고 - 2009/01/05 심사(2009/04/10 2차 - 2009/05/25 3차) - 2009/06/04 심사완료]
☆이 연구는 2009년도 경원대학교 지원에 의한 결과임.

장치의 하드웨어 생산 비용은 크기 및 장치의 전력 소모 등으로 비용을 증가 시킬 수 있다. 처리 시간 감소 및 전산 요구 사항뿐만 아니라 이러한 휴대용 기기에 대한 더 강력한 하드웨어 또한 중요하다[1].

과학자들은 압축과 암호화를 한 단계에서 실현하여 총 처리 시간을 감소시키는 제안을 제기해 왔는데 이런 방법들은 대부분 안전하지 못하거나 계산이 너무 복잡하다[2]. 본 문에서는 새로운 선택적 암호화 방법을 제안한다. 제안한 알고리즘은 이미지의 일부 데이터에 대해서만 암호화하여 이미지의 통신과 처리할 때 암호화와 복호화의 시간을 감소하면서 안전하다. 우리는 선택적 암호화 알고리즘은 암호화와 복호화에 소요되는 시간을 크게 감소시키면서 압축비율에 영향을 주지 않은 압축방법인 quadtree와 zerotree 웨이블릿 압축기법을 도입하여 이미지의 선택적 암호화를 실행하였다. 대부분의 압축 데이터가 암호화 되지 않아 여전히 보일 수 있지만 비밀키로 복호화를 하지 않으면 원래의 데이터를 복구할 수는 없다.

Quadtree 압축 기법을 사용하여 전형적인 이미지에 대해 암호화한 부분은 압축한 데이터의 3%~6%이고 zerotree에 기반 한 웨이블릿 압축 기술에서는 512×512의 이미지에 대해 선택적 암호화하는 경우 암호화 된 부분은 압축한 데이터의 2%~3%정도밖에 되지 않는다. 사실상 암호화 되는 부분이 이렇게 작으면 직접 공개키 암호화 알고리즘을 사용할 수 있어 비밀 키 암호화 알고리즘을 사용하여 드는 비용을 덜 수 있다[3].

2장에서는 선택적 암호 체계의 기반지식과 기타 선행연구에 대해 기술하고, 3장에서는 제안한 선택적 암호화 알고리즘에 대해 서술한다. 4장에서는 실험결과를 5장에서는 결론 및 향후 연구계획으로 끝을 맺는다.

2. 관련연구

2.1 이미지의 선택적 암호화

이미지의 선택적 암호화는 이미지의 일부 데이터에 대해서만 암호화 하는데 압축 기술에 따라서 선택된 데이터는 DCT기반 압축 기술에서는 DCT계수가 될 것이고, 웨이블릿 기반 압축 기술에서는 웨이블릿 계수와 분해된 quadtree 구조이거나 중요한 픽셀의 비트들이 될 것이다.

- DCT계수의 선택적 암호화

JPEG 압축의 DCT계수는 선택적 암호화에 선택될 수 있다. 하나의 방법은 각 DCT블록의 선도적 DCT계수들의 비트스트림을 암호화 하는 것이다. Cheng과 Li에 따르면 JPEG 압축 이미지에서 암호화 된 부분은 원본 데이터의 50%가 넘는 것으로 조사되었고, 개체의 전체적인 윤곽은 여전히 보인다[4]. 적절한 구조는 JPEG 압축 이미지의 한 블록의 저주파에서 DC계수를 제외한 모든 DCT계수를 암호화 하거나 DC계수와 AC계수를 함께 암호화 하는 것이다.

- 웨이블릿 압축 이미지의 선택적 암호화

선택적 암호화 방법은 기타 이미지의 압축 기술에도 추천한다. Zerotree에 기반한 웨이블릿 압축 알고리즘은 중요도에 따라 정보에 대해 등급을 나누어 코딩한다. 이는 선택적 암호화에 아주 잘 맞는다. 하나의 압축된 비트스트림에는 고유의 의존도가 존재하는데 아주 적은 양의 중요한 데이터를 암호화 하면 나머지 암호화 되지 않은 데이터가 소용없게 된다.

- 스페셜 도메인의 선택적 암호화

선택적 암호화는 스페셜 도메인에도 적용할 수 있다. 간단한 접근은 압축되기 전이나 압축하지 않은 이미지의 비트 판(bitplane)을 암호화 하는 것

이다. 높은 중요도를 가진 비트 판은 낮은 중요도의 비트 판보다 더 많은 가시 정보를 포함하고 있기 때문에, 선택적 암호화 체계는 자연스럽게 높은 중요도를 가진 비트 판에서 최소의 중요도를 가진 비트 판으로 하향으로 진행한다.

2.2 Quadtree 이미지 압축 기법

Quadtree 이미지 압축 알고리즘의 많은 변형된 형태들이 존재하는데[5][6], 여기서 오직 기본적인 개념만 설명한다. 비록 더 강력한 압축 알고리즘들이 존재하지만, 계산이 아주 복잡하다는 단점이 있다. Quadtree 압축은 계산의 복잡도가 낮고, JPEG 알고리즘보다 낮은 비트 비율에서 더 잘 수행할 수 있다. 특히 많은 계산 파워를 갖고 있지 않은 휴대용 기기에 적합하다.

Quadtree는 모든 노드가 0 또는 4개의 자식노드를 가지는 뿌리트리인데, 자식노드를 가지고 있는 노드를 내부노드(internal nodes)라고 하고, 반면에 자식노드를 가지고 있지 않는 노드를 잎노드(leaf nodes)라고 한다. 트리의 각 노드는 노드에서 뿌리 노드까지 제일 짧은 경로에서 가지의 수를 레벨이라고 정의한다. 노드의 레벨 중 최고치를 트리의 높이라고 한다. 따라서 레벨이 낮은 노드일수록 뿌리노드에 가깝다.

여기서 하나의 비어있지 않은 quadtree는 4k+1개의 노드들을 가지고 있고, k는 음수가 아닌 정수이고, k개의 내부노드와 3k+1개의 잎노드를 가지고 있다[7].

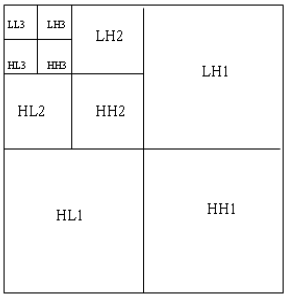
무손실 압축에서, 알고리즘은 트리의 한 노드에서 시작한다. 만약 전체 이미지가 동질(homoge-neous)이면 뿌리 노드는 하나의 잎을 만들고 전체 이미지를 서술하는 회색 레벨은 잎에 첨부된다. 만약 그렇지 않으면 이미지는 4개의 분면(quadrants)으로 나누어지고 4개에 대응하는 자식 노드를 트리의 뿌리에 추가한다. 그리고 알고리즘은 새로운 서브트리의 루트로서 네 자식노드의 각각을 이용해서 각 분면을 검사한다.

Quadtree 압축은 하향식이나 상향식 두 가지 중 하나의 방식으로 구현될 수 있는데, 실제로 보다 더 효율적인 상향식 구현방법을 더 선호한다.

2.3 Zerotree 웨이블릿 이미지 압축 기법

웨이블릿 전송(wavelet transform)은 많은 이미지 압축 알고리즘에 성공적으로 적용하였다[8]. 그림 1에서 보여주듯이 피라미드 분해라고 불리어지는 계수 밴드(coefficient bands)의 계층을 만든다. 밴드 라벨의 수는 그 밴드의 피라미드 레벨이다. 가장 높은 피라미드 레벨에서 LL 밴드는 뿌리 레벨이라고 부른다.

Zerotree를 이용한 영상 압축 방법은 웨이블릿 변환된 영상의 계수 값이 동일한 방향을 갖는 대역 사이에서 상관관계를 갖는다는 점을 이용한다. 즉, zerotree에 기반한 압축 알고리즘은 중요하지 않은 계수를 같이 zerotree에 그룹화하고 매우 효율적으로 이 계수들의 중요도를 표시한다.



(그림 1) 웨이블릿 계수 밴드의 계층구조

중요도를 측정하는 것은 다음과 같은 3개의 리스트를 통하여 구하여진다.

1) LIS(List of Insignificant Sets)
2) LIP(List of Insignificant Pixels)
3) LSP(List of Significant Pixels)

논문에서 다른 유사한 알고리즘에 기초가 되기 때문에 계층 트리에서 집합 분할 알고리즘 SPIHT(Set Partitioning in Hierarchy Trees)에 중점을 둔다. SPIHT알고리즘에서 루트 레벨에서 계수

들의 각2×2블록은 계수들의 세 개의 트리와 대응한다.

- $O(i,j)$는 (i,j)에서 계수의 자식의 좌표 집합
- $D(i,j)$는 (i,j)에서 계수의 모든 자손의 좌표 집합
- H는 루트 레벨에 있는 모든 계수들의 좌표 집합
- $L(i,j)=D(i,j)-O(i,j)$.

Zerotree를 이용한 영상의 압축 방법은 웨이블릿 변환된 영상의 계수 값이 동일한 방향을 갖는 대역 사이에서 상관 계를 갖는 다는 점을 이용한다.

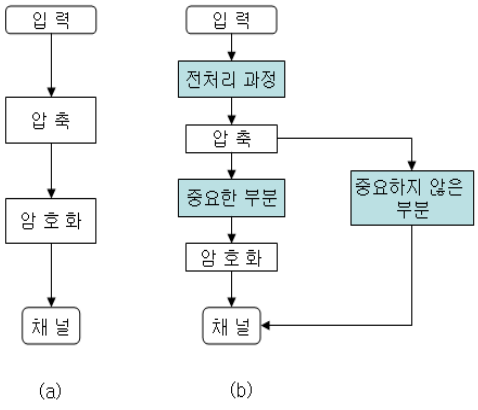
3. 압축 이미지의 선택적 암호화 알고리즘

이 장에서는 이미지의 암호화 부분을 면밀히 검토하기로 한다. 압축 알고리즘을 맹목적으로 선택적 암호 알고리즘에 적용할 수 없으며 각 제안된 알고리즘의 구조는 신중하게 평가되어야 한다. 우리는 알고리즘에서 선택적 암호화에 적합한 방법을 두 개 찾았다. Quadtree 압축 알고리즘은 계산이 간단하고 저주파인 JPEG에 뛰어나다. Wavelet 압축 알고리즘은 zerotree에 기반으로 하고 좋은 압축율을 가지고 있다[9]. 두 가지 유형의 알고리즘 모두 저주파 응용과 선택적 암호화 체계에 적합하게 제안되었다. 또한 계산이 복잡하지 않으며 각 체계가 안전하다고 분석된다. 압축된 이미지의 전체 크기와 중요한 부분의 크기는 직접 암호화와 복호화에 필요한 시간의 양에 비례한다.

3.1 데이터 분해에 기반한 선택적 암호화

대부분의 멀티미디어 데이터 압축 알고리즘은 입력을 다른 논리적 부분의 수로 나눈다. 예를 들면, 영역 기반 이미지와 비디오 압축은 영역을 나타내는 매개변수뿐 만아니라 영역의 모양과 위치를 산출한다. JPEG(Joint Picture Experts Group)과 MEPG(Moving Picture Experts Group)과 같은 주어진 변형 코딩 알고리즘(transform coding algorithm)은 다른 주파수들의 요소들을 나타내는 선택된 기초 함수에 대응하는 계수들을 생성한다[10].

이러한 알고리즘들의 일부는 원본 데이터에서 꼭 필요한 정보를 가지고 있는 중요한 부분(important parts)을 가지고 있는 반면, 중요한 부분 외에 남은 부분은 없어도 되는 정보를 가지고 있다. 간단하게, 중요한 정보를 하나의 중요한 정보 부분에, 그리고 중요하지 않은 부분은 중요하지 않은 부분그룹에 분리해 둔다. 만약 이 부분이 원본 데이터를 재구성하고, 접근하고, 인식하는데 사용될 수 있으면 우리는 중요한 정보를 제공한다고 말한다. 중요하지 않은 부분으로만 정보를 얻어내기는 어렵기 때문에 논문에서는 중요한 부분만을 선택하여 암호화 하는 선택적 암호화 알고리즘을 제안한다.



(그림 2) 이미지 통신의 전통적인 방법(a)과 제안된 방법(b)의 비교

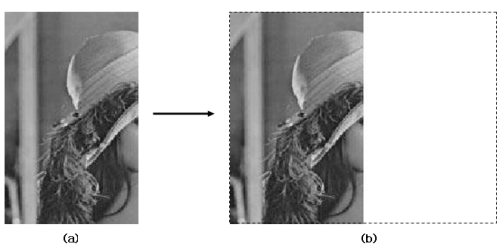
암호화 알고리즘은 중요한 부분의 암호화를 위해 사용된다. 그림 2에서는 제안된 접근 방법과 전통적인 방법의 차이를 보여준다. 전통적인 방법에서는 압축된 모든 출력 데이터를 모두 암호화한다. 중요한 부분과 관련된 사이즈는 작기 때문에 암호화와 복호화 하는 시간을 감소시키는 효과를 볼 수 있다. 실시간으로 안전한 비디오 통신

과 처리를 하려면 데이터 감소 없이는 불가능 하다. 어떤 경우에는, 선택적 암호화를 하면서 중요하지 않은 부분을 동시에 시간을 무시할 수 있도록 병렬로 전송될 수도 있다.

3.2 이미지에 대한 전처리

Quadtree 압축법이나 zerotree 압축법은 입력 이미지에 대해 256×256 또는 512×512처럼 길이와 너비가 같은 정방형의 형태를 요구로 하고 있다. 하지만 실제로 그렇지 않은 이미지가 많다. 그리하여 하나의 이미지가 입력되면, 우선 전처리과정을 거쳐 길이와 너비가 같은 정방형의 형태로 바꾸어준다.

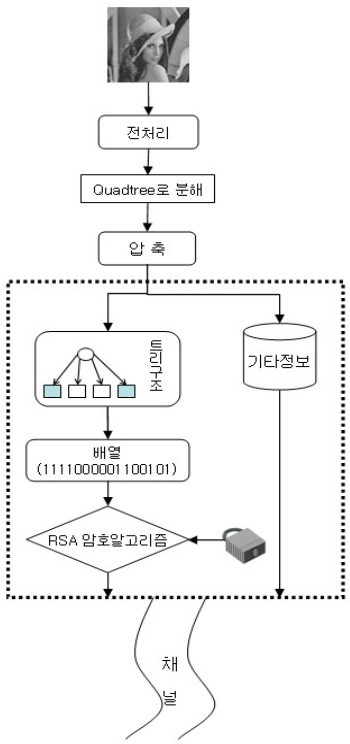
우리는 다른 연구에서 흔히 사용되는 'lena' 이미지를 이용하여 512×256의 이미지를 만들어 예로 설명한다. 그림 3에서처럼 이미지 (a)를 입력하면 길이가 긴 밑변에 맞춰 (b)처럼 512×512의 이미지로 여백을 채워준다. 여백에는 실질적인 값을 가지지 않고 한 블록을 1비트로 표현하며, 각 블록은 이진 수 0으로 채워진다.



(그림 3) 이미지의 전처리과정

3.3 Quadtree 압축을 이용한 알고리즘

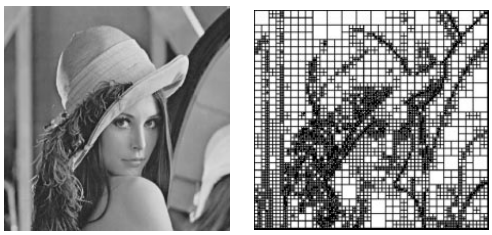
앞서 소개했듯이 논문에서 두 가지 선택적 암호 알고리즘을 제안하였다. 다음 그림 4는 quadtree 압축기법을 이용한 선택적 암호화 알고리즘의 개요를 표현한 것이다.



(그림 4) Quadtree 압축을 이용한 알고리즘

Quadtree 압축 알고리즘에서 두개의 논리적 부분이 제안되었는데 각각의 블록을 quadtree와 매개변수로 설명했다. Quadtree 분해는 원본 이미지에서 객체의 윤곽을 제공하는데 그림 5에서 볼 수 있다. 반면 우리는 원래의 이미지에 대해 많이 학습이 되어 있지 않은 각 블록의 명암도만을 가지는데, 각 블록의 위치와 크기로는 알 수 없다. 우리는 오직 quadtree 구조만 암호화하는 선택적 암호화 방식을 제안했다. Quadtree에서 각 잎 노드에 대응하는 명암도에서 잎의 값은 블록의 명암도를 참조한다. 여기서 분명한건 제안한 방법을 사용하여 그 압축 성능은 저하되지 않았다.

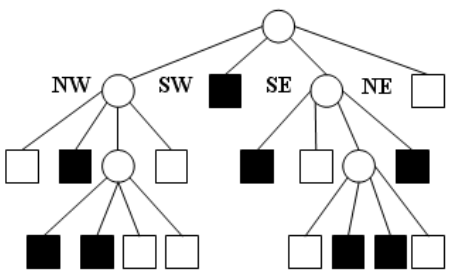
제안한 quadtree 암호화 방식은 무손실 압축을 채택한다. 블록이 클 때는 명암도를 정확하게 나타내는 것이 중요하다. 아주 적은 비트수로 할당된 비트를 표현할 수 있으며 이것 역시 암호화 부분에 포함된다.



(a)원본 이미지 (b)Quadtree로 분해

(그림 5) 이미지를 quadtree로 분해

잎의 값은 일정한 순서로 전송되어야 하는데 두 개의 배열로 소개한다. 그림 6는 quadtree의 하나의 배열을 보여주며 아래와 같이 설명 할 수 있다. 우리는 그 배열에서 각 노드의 네 개의 가지에 해당하는 NW, SW, SE, NE을 탐색한다고 가정한다. 여기서 우리는 블랙 잎 노드는 값이 1, 화이트 잎 노드는 0값을 갖는다고 가정한다.



(그림 6) 이진 이미지의 quadtree의 예

잎의 값 배열 I은 깊이-우선 탐색의 순서에 따라 유도된다. 잎 값은 0 111 000 110 011 010으로 인코딩 된다. 잎에 배열 I에서 잎의 값은 높은 레벨에서 한 단계 낮은 레벨로 디코딩되며 디코딩된 후에는 배열이 자연스럽게 상향식 quadtree 구조를 가지게 된다. 이와 반대로 너비-우선 순서로 트리를 탐색하면 잎의 값은 낮은 레벨에서 높은 레벨로 연결된다. 각 레벨에서 블록들은 잎의 가치에 상응하는 래스터 스캔을 한다. 블록의 각 행은 왼쪽에서 오른쪽으로, 행들은 위에서 아래로의 순서이다. 잎의 값은 해당 블록들의 순서에 따라 배열된다. 만약 quadtree 역시 알려져 있으면 이 레벨에서 잎의 가치와 연결된 각 레벨에서는 별도의 특별한 인코딩이 필요하지 않는다. 따라서 최종 출력한 인코딩된 값은 1 010 001 100 111 001이다[11].

잎의 배열 II는 최선 탐색(Best-First Search)에 의해 유도된다. 최선 탐색은 깊이-우선 탐색과 너비-우선 탐색의 장점을 결합시켰다. 이는 깊이-우선 탐색과 유사하지만 현재의 모든 잎들로부터 가장 좋은 노드를 얻는다는 점이 다르다. 따라서 최종 출력한 인코딩된 값은 1 100 110 110 010 010 이다.

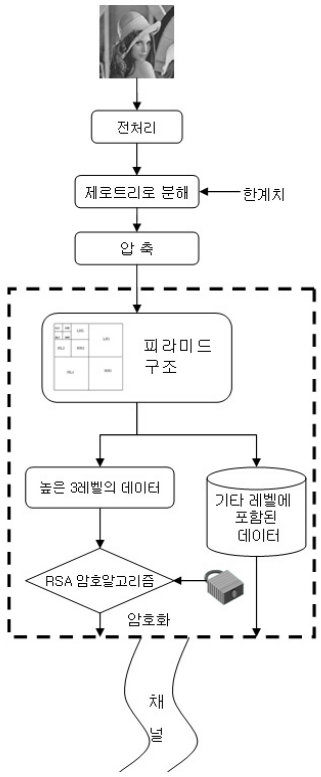
잎의 배열 I는 특정한 속성을 보유하고 있어 암호해독에 취약하다. 이 속성들은 잎의 배열 II에 존재하지 않으므로 트리 열거법으로부터 안전하여 암호해독이 더욱더 어렵게 만든다. 이것은 선택적 암호화 체계를 디자인 할 때 중요하지 않은 부분을 고려하여 제시한 것을 보여준다.

형제 노드의 값이 아주 근사한 잎의 배열 I에서 필요 없는 속성이 있으므로 잎의 배열 I는 우리의 손실 압축의 선택적 암호화 체계에는 적합하지 않다. 하지만 잎의 배열 II는 무 손실 압축이든 손실 압축이든 모두 안전하다[9].

3.4 Zerotree 웨이블릿 압축을 이용한 알고리즘

그림 7에서 zerotree 압축방법을 이용한 선택적 암호알고리즘의 전체 개요도이다. 이는 quadtree 압축방법을 이용한 알고리즘과 유사하지만 압축에 있어 서로 다른 구조로 이미지를 분해하기 때문에 중요한 부분의 선택에 있어서 다른 부분이 있다.

Zerotree에 기반한 압축 알고리즘은 일반적으로 중요한 계수를 추가한 zerotree 구조를 전송한다. 예를 들면, SPIHT 압축 알고리즘은 전송한 중요한 계수의 집합은 트리구조의 계수와 서로 대응한다. 이것은 quadtree 압축알고리즘과 아주 유사하다[5].

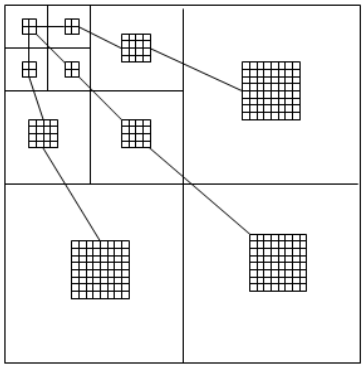


(그림 7) Zerotree 웨이블릿 압축을 이용한 알고리즘

이 방법에서 우리는 동질성을 대체하여 중요성으로 하나의 집합이 계속 분할해야할지를 결정한다. 우리는 SPIHT 압축 알고리즘의 이론에 중점을 두면서 다른 zerotree를 기반으로 한 알고리즘도 역시 사용될 수 있다. SPIHT 알고리즘은 집합의 중요성으로 트리의 구조를 결정하고, 또한 알고리즘의 실행은 zerotree의 구조에 강하게 의지한다. 적은 양의 중요한 정보의 인코딩 데이터가 정확하지 않아도, 이 알고리즘은 정확한 이미지의 디코딩이 이루어지지 않는다[9].

본 논문에서 제안한 선택적 암호화 알고리즘은 피라미드에서 제일 높은 레벨의 중요한 의미가 있는 정보의 픽셀과 집합, 그리고 초기화시의 계수에만 암호화를 한다. 형식적으로, 그리고 (i,j)가 피라미드의 제일 높은 세 레벨에 속해 있는 경우에 대해서만, 우리는 중요한 정보 $S_n(i,j)$, $S_n(D(i,j))$과$S_n(L(i,j))$에 대해서만 암호화 한다. 만약 뿌리 레벨이 8×8의 차원을 갖고 있다면, 중요한 정보는 오직 $0 \le i,j < 16$일 경우에만 암호화 된다. 그리고 압축비율은 영향을 받지 않는다.

일반적으로, 이미지가 0.80 b/pixel 로 압축된 경우 6에서 10개의 정렬 패스가 실행된다. 중요한 부분의 상한선을 5200bit로 한다. 실험을 통해 실제로 중요한 부분의 사이즈는 이것보다 훨씬 작게 나온다.



(그림 8) 웨이블릿 계수의 트리구조

그림 8에서 볼 수 있듯이 웨이블릿 계수의 트리구조의 특성 때문에 피라미드의 두 높은 레벨의 중요한 정보가 없이는, LIS, LIP, LSP 리스트가 알 수 없도록 이니셜이 바뀌게 된다. 정확하게 이미지를 디코딩하려면 최소 160bit의 중요한 정보를 알아야 한다. 따라서 철저한 탐색방법은 최소 2^{160}번의 가능성을 테스트해야 한다[9].

위의 이론에 근거하여 피라미드 구조의 높은 두 레벨만 암호화 하여도 공격자가 쉽게 원본 이미지를 얻어내지 못하지만, 계층구조의 특성에 따라 한 레벨을 추가암호화 하면 더욱더 공격을 어렵게 하므로, 세 개의 레벨을 암호화 한 것과 2레벨을 암호화 한 것을 각각 비교하였다. 세 레벨을 암호화 한 경우 중요한 부분이 조금 추가되었지

만 실험결과에서 사이즈가 비교적 큰 '성'의 이미지는 972bit에 불과하므로 공개 키 암호화 알고리즘을 사용하기에 충분하다[12].

이것은 SPIHT 알고리즘에 우리의 선택적 암호화 방법을 추가한 것이다. 각 중요한 비트가 전송되는 데는 운행시간의 추가를 발생시키지 않았다.

4. 실험 및 분석

실험에서 우리는 다른 연구에서 보편적으로 사용되었던 'lena'이미지를 실험대상 이미지로 정하였다. 여기서 quadtree 압축을 이용한 알고리즘과 zerotree 웨이블릿 압축을 이용한 알고리즘 두 가지 방법으로 나누어 실험을 하였고, 선택된 데이터는 RSA 공개 키 암호 알고리즘으로 암호화 하여 전송하는 방법을 채택하였다.

4.1 압축비율에 대한 테스트 결과

비교의 편의를 위해 quadtree 압축 방법을 이용한 선택적 암호화를 '알고리즘 A' zerotree 웨이블릿 압축 방법을 이용한 선택적 암호화를 '알고리즘 B' 라고 한다.

실험에서우리는 'lena'이미지를 비롯한 몇 개의 이미지를 이용하여 기존의 다른 알고리즘과 비교를 하였다.

(표 1) 압축비율의 비교

이미지	차원	전체 사이즈 (bytes)	압축비율(%)				
			기존 알고리즘	알고리즘 A		알고리즘 B	
				잎의 배열 I	잎의 배열 II	level=2	level=3
lena	512×512	30,154	19.7%	14.4%	14.4%	0.8%	0.8%
강아지	512×512	74,587	17.8%	13.9%	13.9%	0.8%	0.8%
성	512×512	667,994	15.6%	13.0%	13.0%	0.7%	0.7%
키	256×256	19.3	16.7%	12.8%	12.8%	0.8%	0.8%
자물쇠	256×256	48.3	18.3%	11.7%	11.7%	0.6%	0.6%
책상	256×256	74.0	16.5%	12.3%	12.3%	0.7%	0.7%

표 1에서 볼 수 있듯이 두 가지 압축 알고리즘 모두 기존의 압축 알고리즘보다 낮은 압축 비율을 나타내고 있다.

4.2 선택적 암호화에서 중요한 부분의 비율에 대한 테스트 결과

위와 마찬가지로 'lena' 이미지를 비롯한 몇 개의 이미지를 이용하여 기존의 다른 알고리즘과 비교를 하였다. 이용하여 기존의 다른 알고리즘과 비교를 하였다.

(표 2) 전체 이미지에서 중요한 부분의 비율에 대한 비교

이미지	차원	전체 사이즈 (bytes)	중요한 부분의 비율(%)				
			기존 알고리즘	알고리즘 A		알고리즘 B	
				잎의 배열 I	잎의 배열 II	level=2	level=3
lena	512×512	30,154	7.3%	5.2%	4.5%	2.6%	2.8%
강아지	512×512	74,587	8.5%	6.5%	5.1%	3.2%	3.5%
성	512×512	667,994	7.8%	5.8%	4.8%	2.1%	2.6%
키	256×256	19.3	9.2%	5.3%	4.2%	2.5%	3.1%
자물쇠	256×256	48.3	9.5%	5.5%	4.6%	2.8%	3.3%
책상	256×256	74.0	8.9%	4.8%	3.6%	2.2%	2.5%

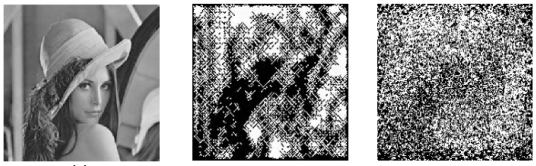
RSA 암호 알고리즘은 대표적인 공개키 암호 알고리즘으로서 대칭키 암호알고리즘에 비해 안전하다는 가장 큰 장점이 있지만 암호화 할 데이터의 양이 큰 경우 알고리즘의 특성상 상대적으로 많은 시간이 많이 필요하므로 주로 대칭키의 비밀키를 암호화 하거나 인증에 많이 사용되어 왔다.

본 논문에서 압축비율이 좋은 압축기법을 사용하였고, 또한 표 2에서 볼 수 있듯이 중요한 부분은 오직 원본 데이터의 2%~6%밖에 되지 않기 때문에 충분히 공개키 알고리즘에 직접 적용할 수 있다. 'lena'의 경우 전체 이미지 데이터에서 실제로 암호화 되는 중요한 부분은 알고리즘A에서는 1563bit이고, 알고리즘B에서 3개의 레벨을 암호화 할 경우 50bit밖에 되지 않는다.

4.3 이미지의 안전성에 대한 테스트 결과

이미지 암호화의 안전성을 실험하기 위하여 'lena' 이미지를 이용하여 원본 이미지를 두 가지 방법으로 암호화 한 후의 결과를 비교한다.

다음은 'lena' 이미지를 알고리즘A로 실험한 결과이다. 여기서 (a)는 원본이미지이고, (b)는 k=1000일때, (c)는 k=1500일때의 암호화한 이미지이다.



(그림 9) 알고리즘 A를 이용한 선택적 암호화 결과

다음은 'lena' 이미지를 알고리즘B를 이용한 선택적 암호화 알고리즘의 실험결과와 기존의 연구결과와 비교한 것이다. (b)는 Lian이 제안한 방법[13]의 실험결과 이고, (c)는 논문에서 제안한 알고리즘B로 암호화한 이미지이다.

(그림 10) 알고리즘 B를 이용한 선택적 암호화 결과

두 가지 알고리즘을 테스트한 결과 모두 기존의 알고리즘보다 낮은 압축비율과 적은 중요한 부분의 비율을 얻을 수 있었으며 이미지의 안전성 또한 잃지 않았다는 결과를 얻을 수 있었다.

5. 결 론

본 논문에서는 이미지를 위한 선택적 암호화 방법을 제안하였다. 특히 낮은 계산의 복잡도, 빠른 전송속도가 요구되는 모바일 디바이스에 적합한 방법이다. 논문에서 quadtree 압축기법과 zerotree 웨이블릿 압축기법을 사용한 두 가지 선택적 암호화 알고리즘을 제안하였는데 트리구조의 특성을 이용하여 압축과 암호화를 한 단계에서 실현하였다.

Quadtree 압축기법을 사용한 알고리즘에서는 quadtree의 트리구조만 추출하여 최선탐색으로 배열을 생성하여 암호화 하였고, zerotree 웨이블릿 압축기법을 사용한 알고리즘에서는 피라미드구조의 상위 세 레벨만 암호화함으로써 실질적으로 암호화한 중요한 부분은 전체 압축한 데이터의 각각 3~6%와 2~3%이다. 또한 두 알고리즘에서 사용한 압축방법은 모두 아주 낮은 압축비율을 자랑하는데 quadtree 압축방법은 11~14%이고, zerotree 웨이블릿 압축방법은 0.8%정도이다. 두 알고리즘 모두 이미지의 전송과 암호화 복호화의 시간을 현저하게 감소시켰다. 이미지의 전송에 있어서 전송시간의 감소는 아주 의미가 있는 것이다. 여기서 선택적 암호화가 가능한 것은 사용한 압축 알고리즘이 계산의 복잡도가 낮기 때문에 실행이 가능한 것이다.

결론적으로, 본 논문에서 제안한 알고리즘은 이미지가 모바일 디바이스에서의 전송에서 시간을 단축하고 또한 안전성을 보장하였으며 계산의 복잡도를 줄이는 아주 유효한 방법이라고 할 수 있다.

실험데이터에서 사이즈가 상대적으로 큰 '성'의 경우 알고리즘 B로 암호화 한 경우, 중요한 부분의 사이즈가 972bit이다. 알고리즘 B에서는 중요한 부분의 상한선을 5200bit로 두고 있는데, 만약 이미지의 데이터가 몇 배 더 커질 경우 알고리즘 B의 사용에 문제가 될 수 있다. 향후 더욱더 안전하고 신속하며, 사이즈의 제한을 두지 않는 암호 알고리즘을 개발하겠다.

참 고 문 헌

[1] Y. Matias and A. Sharmir, "A video scrambling technique bsed on space filling curves," in Proc. CRYPTO, pp. 398-417, 1998.

[2] N. Bourbakis and C. Alexopoulos, 'Picture data encryption using scan patterns,' Pattern Recognit., vol. 25. no. 6, pp. 567-581, 1992.

[3] X. Li, Knipe, and H. Cheng, 'Image compression and encryption using tree structu- res,' Pattern Recognit. Lett., vol. 18, no. 11-13, pp. 1253-1259, Nov. 1997.

[4] H. Cheng and X. Li, 'On the application of image decomposition to image compression and encryption,' Commun. Multimedia Security II, pp. 116-127, 1996.

[5] Howard Cheng, and Xiaobo Li, 'Partial encryption of compressed images and videos,' IEEE Trans. Signal Processing, vol. 48, no, 8. 2000.

[6] G. J. Sullivan and R. L. Baker, "Efficient quadtree coding of images and video," IEEE Trans. Image Processing, vol. 3, pp. 327-331, May 1994.

[7] A. Said and W. A. Pearlman, 'A new, fast, and efficient image codec based on set partitioning in hierarchical trees,' IEEE Trans. Circuits Syst. Video Technol, vol. 6, pp. 243-350, June. 1996.

[8] P. Strobach, 'Quadtree-structured recursive plane decomposition coding of images,' IEEE Trans. Signal Processing, vol. 39, pp. 1380-1397, June 1991.

[9] C. D. Creusere, "A new method of robust image compression based on the embedded zerotree wavelet algorithm," IEEE Trans. Image Processing, vol. 6, pp. 1436-1442, Oct. 1997.

[10] W. B. Pennebaker and J. L. Mitchell, 「JPEG Still Image Data Compression Standard」. New York: Van Nostrand Reinhold, 1993.

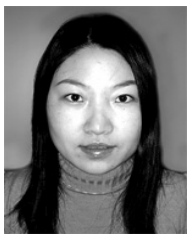
[11] H. Cheng, 'Partial encryption for image and video communication,' M.S.thesis, Univ. Alberta, Edmonton, Alta., Canada, 1998.

[12] William Stallings, 「Network Security Essentials」, Prentice Hall, 2007.

[13] S. Lian and J. Sun, "Pereceptual Cryptography on SPIHT Compressed Images or Videos" IEEE Trans. ICME,

◐ 저 자 소 개 ◑

한 명 묵
1980년 연세대학교 요업공학과 졸업(학사)
1987년 뉴욕공과대학교 대학원 전산학과 졸업(석사)
1997년 오사카시립대학교 대학원 정보공학과 졸업(박사)
1998~현재 경원대학교 IT대학 컴퓨터소프트웨어학과 부교수
관심분야 : 정보보호, Data Mining.
E-mail : mmhan@kyungwon.ac.kr



김 금 실
2003년 경원대학교 전자계산학과 졸업(학사)
2008년 경원대학교 대학원 전자계산학과 졸업(석사)
2009.3~현재 경원대학교 강사직
관심분야 : 콘텐츠 암호화, 모바일 보안.
E-mail : hakuna1103@hotmail.com