JPEG 영상의 저작권 보호를 위한 Digital Watermarking 알고리즘

박 은 숙[†]·우 종 원[††]·이 석 희[††]·허 윤 석[†††]·조 기 형[††††]

요 약

본 논문에서는 암호화된 디지털 워터마크를 JPEG 부호화 과정 중 양자화 계수에 합성하는 디지털 워터마킹 방법을 제안한다. 제안된 워터마킹 방법은 다음과 같다. 먼저 각 블록의 DCT 계수를 양자화 한 후 지그재그 스캔으로 양자화 계수를 1차원으로 배열하여 각 블록을 치환한다. 치환된 각 블록의 일정 영역의 양자화 계수에 암호화된 워터마크를 주파수의 우기성을 적용, 합성한다. 합성이 끝난 후 치환되기 전 순서로 다시 복원하여 부호화 과정을 거쳐 압축된 영상데이터를 얻는다. 본 논문에서 제안된 방식은 합성 전 블록 치환 알고리즘을 사용함으로써 보안을 최대한 유지하면서 많은 정보를 합성할 수 있다. 또한 양자화 계수의 일정 영역을 선택하여 암호화된 정보를 합성하기 때문에 용도에 따른 합성량을 조절 할 수가 있고, 영상 및 양자화 값과 상관없이 합성 데이터를 고정시킬 수 있는 장점이 있다. 본 논문에서는 실험을 통해서 그 결과를 검증하고 기존 연구와의 비교 및 그에 따른 성능을 분석하였다.

Digital Watermarking Algorithm for Copyright Protection of JPEG Image

Eun-suk Park[†] · Jong-won Woo[††] · Seok Hee Lee[††]
Yoon-seok Heo[†††] · Ki Hyung Cho[††††]

ABSTRACT

In this paper, we propose the method of embedding the encrypted digital watermark in quantization coefficient when we encode the image data in the process of JPEG. The proposed method is as following. After a DCT coefficient of each block is quantized, we arrange the quantization coefficient as one dimension with a zigzag scan and replace each block. By applying even-odd feature of frequency of the encrypted watermark to a quantization coefficient of some fixed domain of replaced each block and embedding it, we obtain the compressed image data by encoding after placing it in the order prior to replacement. The advantages of the proposed method here are as follows: We can embed many information keeping a secret as much as possible by using the algorithm of block replacement. we can control the amount of embedding of each use, as we embed the encrypted information by selecting some fixed domain of a quantization coefficient. we can fix the embedding data regardless of the image and the value of quantization. We verified the results by experiments and analyzed the efficiency of them in comparison with the former study.

※ 본 논문은 정보통신부의 정부지원금으로 수행한 "정보통신 우수시범학교 지원사업"의 연구결과 입니다.
† 정 회 원 : 청주과학대학 전산실
†† 정 회 원 : 충북대학교 대학원 정보통신공학과
††† 정 회 원 : 충청대학 메카트로닉스학부 교수
†††† 정 회 원 : 충북대학교 전기전자공학부 교수
논문접수 : 1999년 8월 26일, 심사완료 : 1999년 11월 23일

1. 서 론

최근 네트웍 기술이 발달하면서 인터넷이 보급되어 단순히 문자나 음성 정보의 교환만 하는 것이 아니라 정보 전달 효과가 뛰어난 영상정보가 포함된 멀티미디어 정보의 교환이 활발해 지고 있다. 특히, 디지털 영상을 제작하는 각종 도구들이 발달하면서 영상 데이터의 생성, 편집, 저장 등이 쉬워지고 영상을 왜곡 없이 전송하기 위해 장애에 강한 디지털 데이터로의 변경이 확산되고 있다. 영상의 공급과 수요가 급속하게 증가하고 있는 이러한 상황에서 디지털 원 영상과 복사한 영상을 구분할 수가 없으며, 눈에 보이지 않는 데이터를 영상에 첨가하여 얻어진 변형된 영상과 원 영상을 시각적으로 구분 할 수 없다는 문제가 발생되었다. 이러한 문제점은 디지털 영상의 소유권 및 저작권보호와 인증에 대한 분쟁으로 이어지고 있으며 현재까지 이러한 분쟁을 해결하기 위해 학술적으로 여러 가지 연구가 진행되어 왔다. 그 중에서도 네트웍상의 모든 이용자들이 자유로이 영상을 이용 할 수 있고 전송이 가능하면서 영상의 소유권 보장과 불법적인 내용 조작을 동시에 막을 수 있는 디지털 워터마킹 방법이 가장 활발히 연구되고 있다[1]. 디지털 워터마크는 영상의 각 화소 값을 수정하여 특정한 데이터를 삽입하는 기술로서 일반적으로 삽입된 내용이 보이지 않는 마크를 말한다[2]. 이러한 디지털 워터마크는 정지영상, 동영상, 음성 등 모든 멀티미디어 데이터에 적용 할 수 있다.

본 논문에서는 정지영상의 저장 및 전송을 위한 효율적인 압축 방법으로 국제표준인 DCT(Discrete Cosine Transform)를 기본으로 하는 JPEG(Joint Photographic Expert Group)을 이용하여 압축된 영상에 워터마크를 삽입하는 방법을 제안한다. 원 영상을 JPEG 과정에서 블록별로 DCT계수를 양자화 한 후 양자화 계수를 지그재그 스캔하여 1차원으로 배열한다. 배열된 각 블록을 주사선 치환 알고리즘을 적용하여 치환하고 주파수의 우기성[3]을 이용하여 암호화된 디지털 워터마크를 합성한 후 치환하기 전 원위치로 다시 치환한다. 워터마크가 합성된 양자화 계수는 부호화 과정을 통해 압축되어 JPEG 영상을 얻는다. 본 논문에서 제시하는 워터마킹 삽입방법을 적용할 경우 블록을 치환함으로써 보안성을 강화 할 수 있고 영상의 큰 열화 없이 대량의 정보를 합성 할 수 있다. 또한 영상에 관계없이 합성데이터의 크기를 고정시킬 수 있고 영상에 따라 합성 데이터의 크기도 다르게 할 수 있으므로 용도에 따른 합성 량의 제한이 가능하다. 본 논문의 구성은 2장에서는 디지털 워터마킹과 JPEG 알고리즘에 대하여 기술하며, 3장에서는 기존의 워터마킹 삽입 및 추출 알고리즘을 분석하여 새로운 알고리즘을 제안하고, 4장에서는 제안한 알고리즘에 대한 실험 및 평가 결과를 제시한 후 5장에서 결론을 맺는다.

2. 디지털 워터마킹과 JPEG 알고리즘

워터마크는 모든 멀티미디어 데이터에 적용 할 수 있지만 본 장에서는 정지영상에 대한 워터마킹 기술에 대하여 설명하고, 제한된 전송 대역폭이나 저장 매체의 효율적인 공간 활용을 위해서 정지영상을 압축하는 기법인 JPEG 알고리즘에 대하여 살펴보고자 한다.

2.1 디지털 워터마킹

어떤 개인이 특정한 작품을 만들어 자신의 창작물임을 주장하기 위해 보이지 않는 투명한 형태의 정보를 표시해두는 기존의 워터마킹 기법을 컴퓨터에 적용한 것이 바로 디지털 워터마크이며, 이것을 멀티미디어 데이터에 특정한 코드 값을 삽입하는 방식이 디지털 워터마킹이다. 디지털 워터마킹은 디지털 영상 데이터의 끝에 따로 첨가되는 것이 아니라 영상 데이터와 혼합되어지므로 데이터 크기가 변동되거나 전혀 새로운 영상으로 만들어지는 것이 아니며, 보이는 워터마크와 보이지 않는 워터마크로 나눌 수 있지만 저작권 보호를 위해서 일반적으로 보이지 않는 마크를 말한다[2, 4]. 디지털 워터마킹의 원리를 살펴보면 원 영상 I가 있고, 영상에 삽입할 정보 w가 있을 때 원 영상 I를 인자로 하는 함수 값 $f(I, w)$을 원 영상 I에 삽입하는 작업이며, 이러한 작업을 통해 워터마크가 입혀진 영상 $I' = I + f(I, w)$을 얻을 수 있다[5].

워터마킹하는 방법으로는 영상을 변환하기 전의 공간영역에 삽입하는 방법[6, 7], 변환과정인 주파수영역에 삽입하는 방법[8], 압축공간에 삽입하는 방법 등 크게 3가지로 나눌 수 있다. 공간 영역에서의 워터마킹 방법은 인간의 시각시스템에 의존하여 영상 내에서 밝기의 변화가 적은 부분에 워터마크를 삽입하는 방법이다. 하지만 이 방법은 각종 영상 처리에 의해 워터 마크가 쉽게 제거 될 수 있으며 삽입 할 수 있는 워터마크의 정보가 적고 각종 공격에 약하다는 단점이 있다.

주파수 영역에서의 워터마킹은 DCT, DFT, Wavelet 변환을 하여 얻은 주파수 성분의 계수에 워터마크를 삽입함으로써 영상 내에서 시각적으로 덜 민감한 고주파 성분에 워터마크를 삽입하는 방법이 있다[9]. 그러나 영상압축 기법은 일단 시각에 덜 민감한 고주파 성분을 많이 압축하기 때문에 압축손실에 의해 워터마크가 쉽게 제거 될 수 있다. 주파수 영역에서의 또 다른 방법은 시각 특성상 저주파 성분에서 변화에 민감한 성질을 이용하여 저주파 부분에 워터마크를 삽입하는 방법이다[8]. 이러한 저주파수 영역에서의 워터마크 삽입 방법은 영상 압축 알고리즘의 경우 저 주파수보다는 고 주파수 성분을 갖는 영상 요소를 제거함으로써 압축된 영상을 얻게 되므로 원 영상에 가까운 영상을 얻을 수 있으며 워터마크를 제거하면 영상자체에 열화가 일어나 워터마크의 조작 여부가 금방 시각적으로 확인된다.

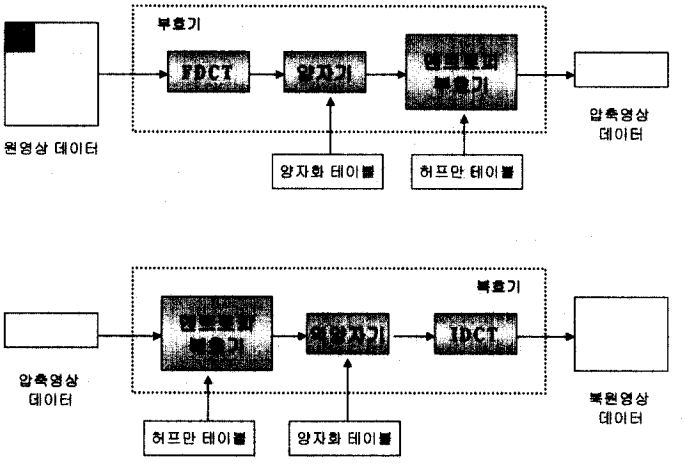
디지털 워터마크를 저작권 보호를 위한 기법으로 적용하기 위해서는 기본적으로 갖추어야 할 특성이 있다[8, 10]. 첫째 영상에 디지털 워터마크가 포함되었는지를 시각적으로 알아보기가 어려워야 한다. 둘째 각종 영상 처리에 대해 워터마크가 손실되지 않고 유지되어야 한다. 셋째 영상에 워터마크 삽입 알고리즘이 알려져 있다고 해도 특정 값을 알지 못하면 워터마크 추출 및 삭제가 불가능해야 한다. 넷째 원 영상의 화질을 최소한으로 유지하면서 가능한 한 많은 워터마크를 합성 할 수 있어야만 한다.

2.2 JPEG 알고리즘

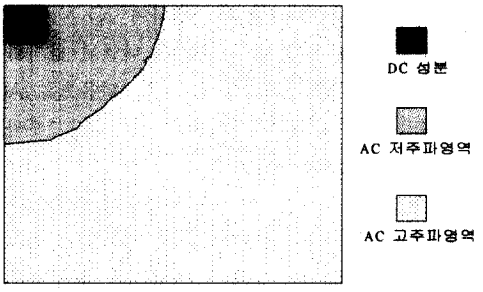
JPEG은 칼라 또는 명암을 갖는 정지영상 압축을 위한 표준으로써 유 손실 압축 방법과 무 손실 압축 방법을 결합한 하이브리드(hybrid) 압축 방법이며 가장 간단한 DCT기반의 순차식 모드를 기본 JPEG이라 하고, 부가적인 DCT기반의 점진식 및 계층식 과정들과 무 손실 모드를 확장 JPEG이라 한다. (그림 1)의 JPEG 과정을 살펴보면 입력영상은 부호기에서 FDCT(Forward DCT), 양자화, 엔트로피 부호화가 실행되어 압축데이터가 출력된다. 복호기에서는 압축데이터에 대해서 엔트로피 복호화, 역양자화, IDCT(Inverse DCT)를 행하고 복호 영상이 출력된다. DCT계수는 양자화에 의한 연산의 반올림 오차에 의해 복원 화상에 왜곡이 존재하는 비가역 압축 방식이지만 시각적으로 지장이 없는 왜곡의 범위 내에서 충분한 압축의 효과를 얻을 수 있다.

2.2.1 DCT

DCT는 공간 영역의 신호를 블록 단위로 주파수 영역의 정보로 변환하는 방법으로 공간영역에서 널리 퍼져있는 에너지를 몇 개의 계수들로 집중시킴으로써 에너지 집중 효과를 크게 하는 변환 기법이다. 부호기에서는 입력 영상을 N×N 화소 블록으로 분할하여 블록별로 식(1)의 계산식에 따라 2차원 DCT 과정을 거쳐 N×N 화소의 DCT계수로 변환된다. FDCT에 의해 변환된 DCT 계수의 주파수 성분의 분포는 (그림 2)와 같다.



(그림 1) DCT 기반 JPEG 부호기 및 복호기 블록도



(그림 2) DCT 특성

$$\text{FDCT}: F(u,v)=\frac{4C(u)C(v)}{n^2}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1}f(j,k)\cos\left(\frac{(2j+1)u\pi}{2n}\right)\cos\left(\frac{(sk+1)v\pi}{2n}\right) \quad (1)$$

$$\text{IDCT}: f(j,k)=\sum_{u=0}^{n-1}\sum_{v=0}^{n-1}C(u)C(v)F(u,v)\cos\left(\frac{(2j+1)u\pi}{2n}\right)\cos\left(\frac{(sk+1)v\pi}{2n}\right) \quad (2)$$

$$C(u),C(v)=\begin{cases}1/\sqrt{2} & u,v=0\\ 1 & otherwise\end{cases}$$

(그림 2)에서 보인 것처럼 FDCT는 N×N의 영상 세그먼트를 N×N→H개의 공간주파수 성분으로 분리하는 역할을 한다, 즉, 입력 세그먼트가 가지고 있는 공간주파수를 주파수 크기별로 분리해 주는 역할을 한다. 또한 주파수 분리와 함께 DC성분 근처에 몇 개의 AC계수들로 에너지 집중현상을 일으키는데, 이것이 변환부호화를 압축에 이용하는 이유이다. 그러므로 왼쪽 위가 DC성분(직류성분)이며, 이 외에는 AC성분(교류성분)이라 부르며 수평방향에서 오른쪽으로 갈수록, 수직방향에서 아래로 내려갈수록 공간 주파수가 높게 된다.

2.2.2 양자화와 엔트로피 부호화

FDCT에서 얻어진 계수들은 양자화 테이블에서 주어진 스텝 크기로 나눈 후, 다음 식 (3)과 같이 가장 가까운 정수를 취하여 양자화 된다. 이 과정의 목적은 실제적으로 압축 효과를 얻기 위한 것인데, 일반적으로 JPEG에서의 압축율 조정이 여기서 이루어진다. 양자화 결과 DC 와 AC 성분의 저주파 영역은 0이 아닌 작은 값으로, 고주파 영역으로 갈수록 더 작은 값을 갖거나 0이 되기 쉬운데 이것은 실제로 필요한 정보가 대부분 저주파 영역으로 집중되어 있기 때문이다. 이렇게 양자화 된 AC 계수들은 지그재그 스캔으로 1차원 배열로 바뀐 후 엔트로피 부호화 과정을 거치게 된다.

$$\text{양 자 화}: Fq(u,v)=round\left\{\frac{F(u,v)}{Q(u,v)}\right\} \quad (3)$$

$$\text{역양자화}: F^*=Fq(u,v)Q(u,v) \quad (4)$$

3. 워터마킹 삽입 알고리즘

영상에 워터마크를 삽입하는 알고리즘에 대해 지금까지 여러 가지 기법이 제안되었다. 그 중에서도 영상 압축 기법을 이용한 주파수 영역에서의 워터마크 삽입 알고리즘에 대한 연구가 가장 활발히 진행되고 있다. 본 장에서는 우선 기존의 주파수 영역에서의 워터마크 삽입 알고리즘 중 JPEG 과정에서 워터마크를 합성하는 알고리즘에 대하여 기술한다. 그리고 이와 비교하여 본 논문에서 제안하는 워터마킹 삽입 알고리즘과 그 특징을 설명한다.

3.1 기존의 워터마크 삽입 및 추출 알고리즘

기존의 JPEG 과정에서 워터마킹 방법은 원 영상을 DCT하여 얻은 계수를 양자화식에 의해 양자화 할 때 지그재그 순서로 0이 아닌 양자화 계수에 대하여 반올림 과정을 약간 수정하여 워터마크를 합성시킨다[11]. 즉, 합성하고자 하는 워터마크 계열 중 1bit를 취한 후, 그것이 0이면 양자화 계수에 가장 가까운 홀수에, 1이면 가장 가까운 짝수에 근사화시켜 워터마크가 합성된 양자화 계수가 얻어 진다. 합성된 양자화 계수는 엔트로피 부호화를 거쳐 압축된 영상을 얻어 전송되어 진다. 전송된 영상을 복원하는 과정에서 양자화 계수가 0 이외의 짝수이면 워터마크가 1이고, 홀수이면 워터마크가 0인 값을 추출하여 전체 워터마크계열을 복원할 수 있다. 이러한 합성 과정의 예를 <표 1>에 나타내었다.

복원하는 영상의 왜곡을 최소화하기 위해 합성시킬 양자화 계수의 위치를 선택하고, 합성하는 기밀 데이터의 양에 따라 여러 가지 합성 방법이 고려되어 질 수 있다. Matsui 연구 그룹의 KTNM 방식[12]은 0이 아닌 모든 양자화 계수에 합성하는 방법을 사용하고 있다. 이를 개선한 JPEG 기밀 데이터 합성법[11][13]으로 첫 번째 KTNM방식에 문턱치의 개념을 도입하여 양자화 계수가 임의로 설정한 고정된 문턱치보다 클 때만 워터마크를 합성하고, 그 외의 양자화 계수에 대

해서는 합성하지 않는 방법이 있고, 두 번째 압축하고자 하는 화상의 크기와 DCT를 위한 블록 크기가 주어지면 합성되는 워터마크의 길이를 고정하는 방식으로 1블럭에 1bit씩 선택하여 합성하는 방법이 있다. 두 번째 방법에서 합성하고자 하는 위치는 0이 아닌 양자화 계수 중에서 선정한다.

〈표 1〉 Watermark 합성 예

DCT 계수	양자화 계수	Watermark	합성양자화 계수
F_{00} = 260	Fq_{00} = 16	1	Fq'_{00} = 16
F_{01} = 49	Fq_{01} = 4	0	Fq'_{01} = 5
F_{10} = -79	Fq_{10} = -7	1	Fq'_{10} = -6
F_{20} = 36	Fq_{20} = 3	1	Fq'_{20} = 2
F_{11} = -16	Fq_{11} = -1	0	Fq'_{11} = -1

3.2 제안하는 워터마크 합성법

3.2.1 삽입 및 추출 알고리즘의 제안

제안하는 알고리즘은 다음과 같다. 우선 (그림 3)에서 나타나는 것과 같이 M×M 화소로 구성된 입력영상을 N×N 화소블록으로 분할하면 M /N → K의 K ×K수만큼 블록이 만들어진다. 각 블록별로 FDCT한 후 얻어진 계수를 양자화 테이블을 사용하여 양자화한다. 양자화하여 얻어진 N×N 화소인 양자화 계수로 구성된 각 블록을 지그재그 스캔하여 N×N→H개의 크기만큼의 1차원 배열로 나열한다. 나열된 양자화 계수의 구성은 첫 번째 위치에 DC성분, 다음으로 AC저주파성분들 그리고 대부분 0으로 구성된 AC고주파 성분들이 순서대로 위치하게 된다. 이렇게 1차원 배열된 블록은 K×K→V개의 수만큼 형성되어, V행 H열로 구성된 2차원 테이블이 만들어진다. 테이블의 각 행을 아래와 같은 Knuth의 random shuffling algorithm[14]을 이용하여 V개의 요소로 나누어지는 블록 K_0, K_1,..., K_{V-1}의 위치를 치환한다.

순서 1. 변수 j를 V으로 초기화한다.

순서 2. 난수 r을 생성한다.(0.0≤r≤1.0)

순서 3. int(r,j)를 계산하여 f로 한다.(0≤f≤j-1)

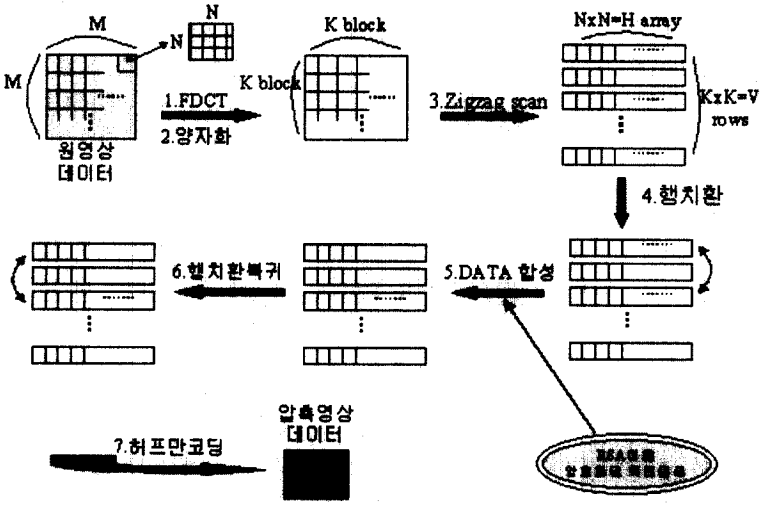
단, int는 소수점 이하를 잘라 정수화하는 함수이다.

순서 4. K_f 와 K_j를 교환한다.

순서 5. j>1 일 때까지 j ← j-1로 한다.

순서 2로 이 random shuffling algorithm으로 치환된 출력되기 직전의 암호 정보를 다시 다음의 무작위 주소를 생성하는데 사용한다.

각 행을 치환후 주파수의 우기성을 이용하여 RSA 암호 알고리즘을 적용한 이진코드로 구성된 암호화된



(그림 3) 제안된 워터마크 합성 알고리즘

워터마크를 선택된 일정 영역의 양자화 계수에 합성한다. 즉, 양자화 된 계수 중 선택된 값을 2로 나누어 나머지가 0인 경우 합성할 워터마크 1bit가 0인지를 체크하여 0이면 그대로 두고 0이 아니면 양자화계수의 값을 1 증가한다. 그리고 2로 나눈 나머지가 1이면 합성할 워터마크 1bit가 0인지를 체크하여 0이면 양자화 계수의 값을 1 증가하고 0이 아니면 그대로 둔다. 합성 알고리즘은 아래와 같다.

```
if (주파수의 우기성 = 0)
    {
     if (합성bit(s)=0)
        그대로 둔다
     else
        주파수 계수++ }
elseif(주파수의 우기성 = 1)
    {
     if(합성bit(s)=0)
       주파수 계수++
     else
       그대로 둔다 }
```

치환된 전체블록에 워터마크를 위와 같이 합성한 후, 블록을 치환하기 전 원 위치로 복귀시킨다. 합성된 양자화 계수를 전체 블록에 대해 허프만 테이블을 이용하여 엔트로피 부호기로 부호화 하여 압축 데이터를 얻는다.

3.2.2 제안된 삽입 알고리즘의 특징

본 논문에서 제안하는 알고리즘은 크게 두 가지 관점에서 기존의 알고리즘과는 다른 특성을 지닌다. 우선 DCT 결과의 양자화 계수에 워터마크를 삽입하는 측면에서 보안이 강화되었다. 기존의 경우 저작권 보호를 위한 디지털 워터마크는 단순히 합성 알고리즘에만 의존하였으나, 본 논문에서는 합성하기 이전에 Random Shuffling Algorithm을 이용하여 양자화계수 테이블을 치환한 후 워터마크를 합성하였기에 저작권을 주장하고자 할 경우 난수 발생기의 키 값을 알고 있어야만 숨겨진 디지털 워터마크를 추출할 수 있다. 영상 정보는 그 정보량의 방대성 때문에 단순하게 기존의 암호 방식을 이용하면 정보보호에 문제점이 발생하게 된다. 왜냐하면 암호방식은 충분한 암호강도를 유지하게 위해 비교적 많은 계산 량을 필요로 하기 때문이다. 이러한 문제점을 효과적으로 해결하기 위해 보다 빠르고 암호 구현이 간단하면서 충분한 암호강도를 갖는, 영상 정보에 맞는 암호방식에 대해 많은 연구가 진행되어 왔으며 그 중에서도 고속성을 유지하면서 암호강도 면에서의 문제점을 해결한 것이 위에서 언급한 RSA이다. 이와 같이 합성할 각 블록을 치환 알고리즘을 적용하여 치환함으로써 1차적인 보안을 유지할 수 있고, RSA 암호 알고리즘을 이용하여 암호화된 디지털 워터마크를 사용함에 따라 2차적 보안을 유지함으로써 보안을 한층 더 강화할 수 있다. 그러므로 합성 알고리즘이 공개되어도 보다 안정적으로 영상의 저작권 및 소유권을 보호할 수 있으며 JPEG 과정에서 합성하여 압축함으로써 저작권 및 소유권 정보가 합성된 영상데이터를 네트웍 상에서 전송이 가능하다.

또한 기존의 방법에서 양자화계수가 0이 아닌 값에만 합성을 한 반면 제안하는 방법에서는 양자화계수가 0이더라도 이미지의 열화가 크지 않은 범위 내에서 합성이 가능하도록 하였다. 이때 합성할 양자화 계수의 일정영역을 선택함으로 화상 및 양자화 값에 따라 합성 데이터의 크기가 가변적이 되는 기존 알고리즘과 비교하여 필요한 양의 데이터를 고정적으로 합성할 수가 있으며, 용도에 따른 합성량의 제한이 가능하다. 다음의 <표 2>는 제안된 알고리즘을 통하여 합성하는 경우의 예이다.

〈표 2〉 제안된 방식의 Watermark 합성 예

DCT 계수	양자화 계수	Watermark	합성양자화 계수
F_{00} = 260	Fq_{00} = 16	1	Fq'_{00} = 17
F_{01} = 49	Fq_{01} = 4	0	Fq'_{01} = 4
F_{10} = -79	Fq_{10} = -7	1	Fq'_{10} = -7
F_{20} = 36	Fq_{20} = 3	1	Fq'_{20} = 3
F_{11} = -16	Fq_{11} = -1	0	Fq'_{11} = 0

4. 실험 및 평가

4.1 제안된 합성 알고리즘의 구현 및 실험

본 논문에서는 제안된 알고리즘을 평가하기 위하여 다음과 같은 환경에서 실험을 하였다. 우선 알고리즘은 C로 프로그래밍하여 구현하였다. 시스템은 Pentium-200MHz, RAM 128MB을 갖춘 PC를 이용하였다. 그리고 제안된 DCT를 기본으로 하는 JPEG에서 워터마크를 합성하는 방법에 대한 본 알고리즘의 적용을 위하여 256×256 화소 크기의 GIRL, LENA, BRIDGE 영상을 사용하였으며 블록의 크기를 8×8로 하여 각각의 영상에 대한 성능을 평가하였다.

화상의 열화가 시각적으로 심하지 않은 범위 내에서

합성량을 최대화시킬 수 있는 영역을 도출하기 위하여 각각의 화상에 영역별로 워터마크를 합성하였으며 영역별 범위는 지그재그 스캔을 기준으로 하여 P1=Fq_{00}, P2=Fq_{00}~Fq_{01}, P3=Fq_{00}~Fq_{10}, P4=Fq_{00}~Fq_{20}, P5=Fq_{00}~Fq_{11}, P6=Fq_{00}~Fq_{02}로 정의하여 실험하였다. 화상의 열화상태를 평가하기 위하여 객관적 평가인 아래의 식(5)와 같이 정의되는 RMS를 사용하였으며 영상에 합성한 암호화된 디지털 워터마크는 <표 3>과 같은 이진 데이터이다.

$$RMS = \sqrt{(1/L)\sum_{i=0}^{L}(x_i - x'_i)^2} \qquad (5)$$

〈표 3〉 암호화된 디지털 워터마크 데이터

1100101001101001000100101110001010110001011000010010101010011000
0010100000100100010010000101000000010111010001010100010100110010
0011101001010101011100000010010100000010000001010010100110001110
1001101000100101010001010101001100101001101001000100101110001010
1100010110000100101010100110000010101010111000000100101000000100
0000101001010011000111010011010001001010100010101010010100100010
0101110001010110001011000010010101010011000001010000010010001001
0000101000000010111010001010001010011001000111010010101010111 0
.....

본 실험에서는 준비된 세 개의 이미지, 즉 GIRL. DAT, LENA.DAT, BRIDGE.DAT에 대하여 <표 3>과 같은 디지털 워터마크를 삽입하였다. 이때 삽입되는 디지털 워터마크의 합성은 앞에서 설명했듯이 P1~P6까지의 영역별로 나누어 합성하였다. 준비된 영상은 256×256 크기의 영상으로 8×8 블록으로 나누었으므로 지그재그 스캔한 후 만들어진 테이블은 1024×64로 구성된다. 따라서 P1의 경우 각 행의 1열에만 합성하기에 1024bits가 합성될 수 있으며, P6의 경우에는 6144(=1024×6)bits가 합성되게 된다. 이와 같이 많은 양의 워터마크를 합성하는 것은 소유권과 저작권의 자세한 정보를 대량 합성 할 수 있다는 것이며 화상의 열화를 최소한으로 억제시키고 압축율에 영향을 주지 않는 범위 내에서 합성하는 방법이 요구된다. 다음의 <표 4>는 이와 같은 합성과정을 거친 후의 영상을 원 영상과 비교하여 RMS값을 측정한 결과이며, (그림 4)에서 (그림 6)은 실험결과를 나타내는 영상이다.

위의 실험결과 그림에서 (그림 4)는 원 영상이며 (그림 5)는 원 영상을 워터마크 삽입과정 없이 JPEG 압축을 거친 후 다시 복원한 그림이다. 그리고 (그림 6)

〈표 4〉 영역별 RMS, 합성량

비교항목 \ 합성영역		P1	P2	P3	P4	P5	P6	일반 JPEG
RMS	GIRL	2.123	2.285	2.440	2.621	3.117	3.493	1.971
	LENA	2.424	2.572	2.889	3.341	3.748	3.912	2.121
	BRIDGE	2.217	2.454	2.717	3.184	3.436	3.715	1.968
합성량 (bit)	GIRL	1024	2048	3072	4096	5120	6144	-
	LENA	1024	2048	3072	4096	5120	6144	-
	BRIDGE	1024	2048	3072	4096	5120	6144	-

(그림 4) 원영상(Girl.dat)

(그림 5) 복원된 일반 JPEG 영상

(그림 6) P6영역 합성된 영상

은 원 영상을 JPEG 압축과정 중 DCT 후에 양자화 계수에 워터마크를 삽입한 후 나머지 압축과정을 거친 JPEG 영상이다. 특히 (그림 6)은 본 실험과정 중 가장 많은 양의 워터마크 데이터를 삽입한 경우로서 이때의 영상이 원 영상과 큰 차이가 없음을 알 수 있다. 더불어 워터마크가 가장 많이 합성된 (그림 6)과 단순히 JPEG 압축과정을 거친 후 복원된 (그림 5)와는 인간의 시각으로는 크게 차이를 느끼지 못한다.

4.2 구현된 워터마크 삽입 알고리즘의 고찰

본 논문에서는 JPEG 과정에서 암호화된 워터마크를 합성하는 기법을 제안하면서 저작권 보호를 위해 디지털 워터마크가 기본적으로 갖추어야 할 특성들 즉, 영상에 디지털 워터마크가 포함되었는지를 시각적으로 알아보기가 어려워야 하며, 원 영상의 화질을 최소한으로 유지하면서 가능한 한 많은 워터마크를 합성 할 수 있는 기법을 설계하고 이를 구현하였다. 표준 JPEG 알고리즘은 양자화과정에서 반올림 오차에 의해 복원 화상에 왜곡이 존재하는 비가역 압축 방식이며 이러한 양자화 계수와 워터마크가 합성되었을 때의 양자화 계수 사이에는 약간의 오차가 생기게 되며, 이것은 압축된 영상을 복호화 할 경우에 영향을 미치게 되어 재생 화상의 열화를 초래하게 된다. 그러나 합성시킬 양자화 계수의 위치를 적절히 선택하게 되면 영상의 왜곡을 최소화하면서 대량의 워터마크를 합성 할 수 있다.

JPEG 알고리즘에 워터마크를 합성하는 과정을 기존의 제안방식과 본 논문에서 제안된 방식을 비교하면 첫 번째로 기존의 Matsui 연구 그룹의 KTNM 방식 [12]의 경우 양자화 계수가 0이 아닌 모든 곳에 합성함으로써 많은 정보를 합성 할 수 있지만 용도에 따른 합성량의 제한이 불가능하며, 영상 및 양자화 값에 따라 합성 데이터의 크기가 달라지게 된다. 또한 단순히 합성만 함으로써 합성 알고리즘이 공개가 되면 기밀정보가 누출이 되고 저작권 및 소유권을 보호할 수 없게 된다. 그러나 본 논문에서는 양자화 계수의 일정 영역을 선택하여 암호화된 정보를 합성하기 때문에 용도에 따른 합성 량을 조절 할 수 있고, 영상 및 양자화 값과 상관없이 합성 데이터를 고정시킬 수 있으며 보안성을 강화하여 합성 알고리즘이 공개되어도 정보를 쉽게 검출 할 수 없게 된다. 두 번째로 위의 제안방식을 개선한 JPEG 알고리즘에 기밀 데이터 합성법 [11, 13]을 살펴보면 압축하고자 하는 영상의 크기와 DCT를 위한 블록 크기가 정해지면 합성되는 기밀 데이터의 길이가 고정되는 방식을 제안하였다. 즉, 1블럭에 1비트씩 기밀 데이터를 합성하는 방식으로써 합성하고자 하는 위치는 0이 아닌 양자화 계수 중에서 선정 할 수 있으나, 제 3자의 공격에 대비하여 랜덤함수에 의해 임의로 선택 되게 한다. 또한 복원 화상의 열화를 최소화하기 위해서는 DC성분과, AC성분 중 최대값 및 최소 값 등을 선택하여 기밀 정보를 합성하였다. 그러나 이 방식은 1블록에 1비트씩 기밀 데이터를 합성하기 때문에 영상의 큰 열화 없이 기밀 데이터를 합성 할 수 있지만 저작권 정보를 위한 대량의 정보를 합성 할 수가 없으며 정보 보안 측면에서는 크게 기대할 수가 없다.

결론적으로 본 논문에서는 양자화된 각각의 블록을 random shuffling algorithm을 이용하여 치환한 후 기밀 데이터를 합성하기 때문에 보안을 최대한 유지할 수 있으며 실험을 통해서 RMS를 측정한 결과 양자화 계수의 고주파 부분인 0에도 합성하여 화상의 열화상태가 JPEG과정만 거친 영상과 거의 비슷하여 대량의 정보를 합성할 수 있으며 합성 량을 임의로 조절할 수 있다.

5. 결 론

본 논문에서는 암호화된 디지털 워터마크를 JPEG 과정 중에 주파수의 우기성을 이용하여 일정영역에 합성하는 새로운 기법을 제시하였다. 제안된 디지털 워터마킹 방법은 보안성을 보다 강화하면서 대량의 정보를 합성하여 압축할 수 있으며, 워터마크가 합성된 영상이 JPEG 과정만 거친 영상과 거의 비슷하여 정보가 합성되었는지를 거의 알 수 없다. JPEG 영상에 워터마크를 합성하여 전송하기 때문에 인터넷에서 모든 사람들이 영상을 볼 수 있으며 불법복사에 의해 저작권 시비가 일어 날 경우 정보를 추출하여 저작권 및 소유권을 주장 할 수 있다. 지금까지는 정지영상이나 음성정보에 대한 워터마크 기술이 주로 연구되어 왔으나 요즈음에는 VOD와 같은 동영상을 제공하는 서비스나 비디오 데이터가 디지털화 되어 전송 및 저장되면서 동영상에 적용할 수 있는 워터마크 기술에 대한 연구가 추후로 진행되어야 할 것이다. 또한 대부분 네트웍을 통해 전송이 이루어지기 때문에 영상이 전송 도중 불법으로 내용의 일부가 바뀌지 않았다는 것을 수신자

가 확인 할 수 있도록 하는 디지털 영상정보의 인증을 위한 서명에 대해서도 연구가 이루어져야 할 것이다.

참 고 문헌

[1] Wong, S., "Image security," http://www.ece.curtin.edu.au/~wongsc/digital.htm, 1997.

[2] Craver S., et al., "Can invisible watermarks resolve rightful ownership?," In International Proceedings of SPIE, Vol.3022, pp.310~321, 1997.

[3] 박일남, "차분 부호장 혼합 알고리즘을 이용한 문서 화상에 대한 보안 체계 연구", 경희대학교 박사학위 논문, 1997.

[4] J. Zhao, "Look. it's not there." http://www.byte.com/art/9701/sec18/art1.htm

[5] R. G. van Schyndel. A. Z. Tirkel. and C. F. Osborne. "A digital watermark," In International Conference on Image Processing, Vol.2. pp.86-90, 1994.

[6] Bender W., et al., "Techniques for data hiding," In International Proceedings of SPIE, Vol.2420. pp.164~173, 1995

[7] G.C. Langelaar, J.C.A. van der Lube, and J. Biemond, "Copy Protection for Multimedia Data based on Labeling Techniques," *17th Symposium on information theory in the Benelux, Enschede, The netherlands,* May 1996.

[8] Cox I. J., et al., "Secure spread spectrum watermarking for multimedia," NEC Research Institute, Technical Report 95~100, 1995.

[9] ORuanaidhJ J. K., et al., "Watermarking digital images for copy right protection," In International Proceedings of Vis.Image Signal Process, Vol.143, No.4, pp.250~256, 1996.

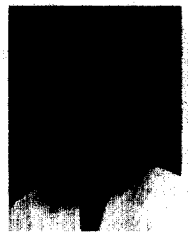
[10] Hartung F. and Girod B., "Copyright protection in video delivery networks by watermarking of pre-compressed video," *Lecture note in computer science*, Vol.1242, pp.423~436, Springer, Heidelberg, 1997.

[11] 박지환, 박태진, "JPEG 알고리즘에 기밀 데이터 합성법", 통신정보보호학회 제6권, 제1호, pp.65~77, 1996. 3.

[12] T. kataoka et al., "Embedding a Document into Color Picture Data under Adaptive Discrete Cosine Transform Coding," In International Proceedings of IEICE, Vol.J72-B-I, No.12, pp.1210-1216, 1989. 12.

[13] E. Koch and J. Zhao, "Towards robust and hidden image copyright labeling," IEEE workshop on Nonlinear Signal and Image Processing, 1995.

[14] 이경호, 정지원, 원동호, "영상 정보의 보호에 관한 소고", 통신정보보호학회 제3권, 제1호, pp.42~53, 1993. 3



박 은 숙

e-mail : euns@cjcnet.chongjunc.ac.kr

1992년 한국방송통신대학교 전자계산학과 졸업(학사)

1999년 충북대학교 대학원 정보통신공학과(공학석사)

1992년~현재 청주과학대학 근무

관심분야 : 영상압축, 컴퓨터 그래픽스, 컴퓨터 네트워크

우 종 원

e-mail : sunsuso@pretty.chungbuk.ac.kr

1997년 충북대학교 정보통신공학과(공학사)

1999년 충북대학교 대학원 정보통신공학과(공학석사)

관심분야 : 정보검색, 영상처리, 보안

이 석 희

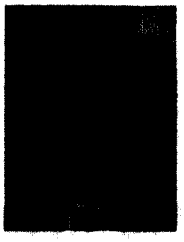
e-mail : seoklee@pretty.chungbuk.ac.kr

1994년 충북대학교 정보통신공학과(공학사)

1998년 충북대학교 대학원 정보통신공학과(공학석사)

1998년~현재 충북대학교 대학원 정보통신공학과 박사과정

관심분야 : 데이터베이스 시스템, 정보검색, 영상처리, 분산 객체 컴퓨팅



허 윤 석

e-mail : hys@cccc.chch-c.ac.kr

1987년 경희대학교 전자공학과 졸업(공학사)

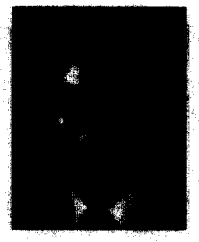
1990년 경희대학교 대학원 전자공학과(공학석사)

1996년~현재 경희대학교 대학원 전자공학과 박사과정(수료)

1989년~1996년 (주)신도리코 기술연구소 선임연구원

1997년~현재 충청대학 메카트로닉스학부 전자공학과 전임강사

관심분야 : 디지털 영상/신호처리 시스템, 암호화, 전력선 통신 시스템



조 기 형

e-mail : khjoe@cbucc.chungbuk.ac.kr

1966년 인하대학교 전기공학과(공학사)

1984년 청주대학교 대학원 산업공학과(공학석사)

1992년 경희대학교 대학원 전자공학과(공학박사)

1981년~1988년 충주대학교 조교수

1996년~1999년 충북대학교 국책실무단장 및 전기전자공학부장

1988년~현재 충북대학교 전기전자공학부 교수

관심분야 : 데이터베이스시스템, 화상처리 및 통신, 통신 프로토콜, 분산 객체 컴퓨팅