通信情報保護學會誌
第6卷 第1號, 1996. 3

JPEG 알고리즘에 기밀 데이터 합성법[1)]

Embedding Method a Secret Data into JPEG Algorithm

박 지 환*, 박 태 진*

요 약

본 논문에서는 JPEG 알고리즘을 이용하여 화상데이터를 부호화할때 디지털 서명문과 같은 기밀 데이터를 몰래 집어넣어 합성하는 방식에 대하여 고찰한다. 그 기본원리는 DCT 계수를 양자화할 때 필연적으로 생기는 오차를 이용하는 것으로 0이 아닌 양자화 계수를 합성하고자 하는 기밀 데이터에 따라 근처의 정수로 조절하는 것이다. 이 방식을 SIDBA 표준화상에 적용하여 화상의 열화는 무시할 정도로 작으면서 원하는 크기의 기밀 데이터를 합성할 수 있음을 보인다. 또한, 화질의 열화를 최소화시키면서 일정량의 기밀 데이터를 합성시키기 위하여 블록당 1화소를 적절히 선택하여 제3자의 공격에 대한 안전성을 향상시키는 방법을 제시하고 컴퓨터 시뮬레이션을 통하여 성능을 분석한다.

1. 서 론

정보화 사회가 진전되면서 수치, 문자, 음성, 화상 및 영상 등의 다양한 데이터를 상호 유기적으로 관련시키면서 통합하는 멀티미디어 기술이 요구되고 있다. 이 가운데 화상 데이터는 인간의 시각 특성을 이용하기 때문에 정보 전달의 효과가 크지만, 데이터 량이 방대하기 때문에 고속전송 방법과 물리적으로 그 양을 줄이는 데이터 압축 방법들이 강구되어 왔다. 그 중에 칼러 정지 화상의 압축을 위한 JPEG (Joint Photographic Expert Group) 부호화 알고리즘이 널리 사용되게 되었다[1]. JPEG 알고리즘은 입력신호를 주파수 영역으로 변환하는 DCT(Discrete Cosine Transform)가 중심적인 역할을 수행하고 있으며, 데이터 압축율은 1/20로도 실용상 충분한 화질을 얻고 있다. JPEG 방식 이외에도 흑백 화상을 위한 JBIG (Joint Bi-level Image Group)[2]과 동화상을 다룬 MPEG(Moving Picture Experts Group)[3]이 표준안으로 규정되어 있다. JPEG과 MPEG은 원화상을 DCT(Discrete Cosine Transform)로 변환한 계수를 양자화 테이블을 사용하여 정수로 양자화 한다. 이때 양자화 오차가 필연적으로 생기게 되므로 복원된 화상은 원화상에 대하여 왜곡이 발생하며, 왜곡의 정도는 RMS(Root Mean Square) 및 MOS(Mean Opinion Score)등에 의해 평가된다.

* 부산수산대학교 전자계산학과

1) 이 연구는 1995년도 한국과학재단 연구비 지원에 의한 결과임. 과제번호 951-0915-023-1

기존의 화상 데이터 압축에서는 화질을 고려하면서 물리적 크기를 최대한 줄일 수 있는 압축의 입장에서만 연구되어 왔으나, 최근 오류제어나 정보 보안의 기능을 고려한 새로운 응용이 주목되고 있다. 특히, 네트워크의 확산에 따른 보안문제는 정보 시스템 구축의 중요한 요소이다. 이를 위한 기법에는 기존의 DES나 RSA 등의 암호화 방식에 의해 기밀 데이터를 적극적으로 보호하는 방법[4]과 비밀로 하고자 하는 데이터를 다른 목적으로 전송하는 데이터에 몰래 집어넣어 비밀통신 자체를 감추어 소극적으로 보호하는 방법[5]이 있다. 전자는 이른바 암호학의 입장에서 연구되어 높은 안전성은 확보되지만 시스템 구성이 복잡해지거나 부가적인 처리에 의한 데이터 량의 증대를 가져오게 된다. 이에 비해 화상 심층 암호로 불리는 후자는 암호학적 안전성은 떨어지지만, 데이터 압축과 정보 보안의 기능을 동시에 추구할 수 있는 이점이 있어 새로운 응용이 기대된다.

예를 들면, 화상의 저작자가 가치가 있는 자신의 작품을 네트워크 등을 통하여 발표하고자 하는 경우, 제3자에 의해 전부 또는 그 일부를 도용 당할 염려가 있다. 따라서, 화상의 저작권을 보호하는 수단으로서 제안되어 있는 저작자 인증방식[6]은 화상 부호화 시에 몰래 기밀 데이터를 감춰 넣는 것이다. 이와 같은 응용에 있어서 중요한 사항은 원화상의 화질을 떨어뜨리지 않고 가능한 한 많은 기밀 데이터를 합성시킬 수 있는 방법과 제3자가 화질의 대폭적인 열화 없이는 기밀 데이터를 제거할 수 없도록 하는 것이다.

본 논문에서는 압축을 수행하고자 하는 화상을 DCT로 변환하여 양자화 할 때 반올림 과정에 있어서 양자화 계수의 값이 일정한 문턱치 보다 큰 모든 계수에 기밀 데이터를 합성하는 방법을 고안한다. 나아가, 기밀 데이터의 크기가 일정량일 때 화질의 열화를 최소한으로 유지하면서 제3자의 공격에 대비한 안전성을 확보하는 기법을 제시한다.

화상 압축방식으로 JPEG 알고리즘을 이용하지만, 양자화 과정에서 기밀 데이터를 합성하므로 양자화 과정을 포함하는 MPEG등의 압축방식에도 적용할 수 있다. 또한, 문자형태의 기밀 데이터에 국한하지 않고 음성 및 또 다른 화상 데이터 등도 합성할 수 있으므로 정보 보안의 기능이 요구되는 멀티미디어 응용에 폭 넓게 활용될 수 있다.

먼저, 2장에서 DCT를 기본으로 하는 JPEG 알고리즘의 개요에 대하여 기술한다. 3장에서는 DCT에서 얻어지는 양자화 계수에 기밀 데이터를 합성시키는 방법을 나타내며, 4장에서 그 성능을 컴퓨터 시뮬레이션을 통하여 비교 분석한다.

2. JPEG 알고리즘

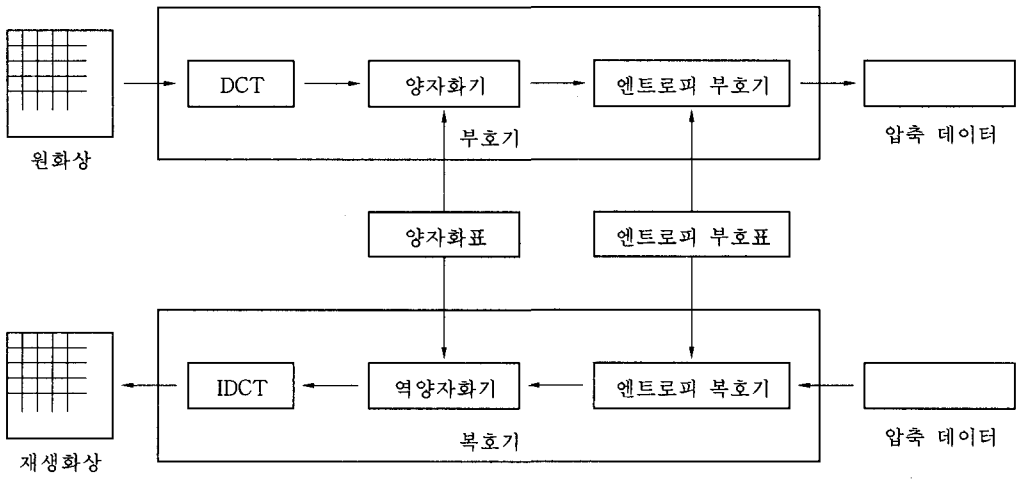
JPEG은 화상 데이터 베이스, 칼러 팩시밀리 및 인쇄등의 분야에 적용하기 위한 칼러 정지화상 부호화 방식으로 범용성이 넓은 응용을 위하여 4가지의 동작 모드를 사용자가 선택할 수 있도록 설계되어 있다. 그 가운데 순차(sequential) 처리를 위한 베이스 라인 시스템, 단계적(progress build-up)처리를 위한 확장 시스템 및 계층적(hierarchical) 전송을 위한 방식은 DCT를 기본으로 하고 있다.

JPEG은 그림 1에 나타낸 바와 같이 2차원 DCT를 수행한 계수를 양자화 한 후에 Run-length Huffman 부호나 산술부호와 같은 엔트로피 부호화로 압축한다. DCT계수의 양자화는 화질과 압축량을 제어하는 중요한 파라메터로

서 부호화 하고자 하는 화상에 의존하기 때문에 최적 양자화 값이 다르며, 응용에 따라 사용자가 임의로 선택할 수 있다. 또한, DCT는 양자화에 의한 나눗셈에 의해서 뿐만이 아니라 부동 소수점 연산이 이루어지기 때문에 연산의 반올림 오차에 의해 복원 화상에 왜곡이 존재하는 비가역 압축 방식이다. 그러나, JPEG은 시각적으로 지장이 없는 왜곡의 범위 내에서 충분한 압축의 효과를 얻을 수 있어 멀티미디어 기술에 폭 넓게 이용되고 있다.

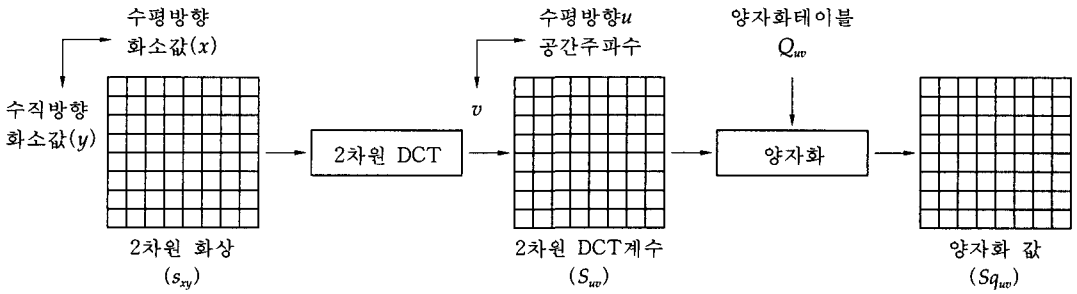
2.1 DCT에 의한 공간주파수의 변환

JPEG의 DCT[7]에서는 입력 화상을 $N * N$ 화소로 구성되는 블록의 집합인 MCU (Minimum Code Unit)라는 단위로 분할한다. 이렇게 분할된 한 블록은 그림 2에 나타낸 바와 같은 변환이 이루어진다. 블록내의 2차원 데이터를 $s_{xy}(x, y = 0, 1, \cdots, N\text{-}1)$, DCT 변환 계수를 $S_{uv}(u, v = 0, 1, \cdots, N\text{-}1)$이라 하면 DCT와 그 역변환인 IDCT는 식(1), (2)와 같이 정의된다.



〈그림 1〉 DCT 베이스의 JPEG 부호기 및 복호기의 구성

〈Fig.1〉 Construction of JPEG encoder/decoder based on DCT



(그림 2) DCT 부호화 과정

(Fig.2) DCT coding process

DCT :

$$S_{uv} = \frac{1}{\sqrt{2N}} C_u C_v \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} s_{xy} \cos \frac{(2x+1)u\pi}{2N} \cos \frac{(2y+1)v\pi}{2N} \quad (1)$$

IDCT :

$$s_{xy} = \frac{1}{\sqrt{2N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} C_u C_v S_{uv} \cos \frac{(2x+1)u\pi}{2N} \cos \frac{(2y+1)v\pi}{2N} \quad (2)$$

단, $C_u, C_v = \begin{cases} 1/\sqrt{2}, & u, v = 0 \\ 1, & \text{otherwise} \end{cases}$

따라서, DCT 변환계수 S_{uv}는 1개의 블록에 대하여 $N \times N$개 존재하는데 이 중에 S_{00}를 DC 성분, 나머지는 AC 성분이라 부른다. 이 때, u와 v가 커질수록 각각 수평 및 수직의 높은 공간주파수 성분이 포함된다.

2.2 양자화

DCT 변환에서 얻어진 $N \times N$개의 DCT 계수 S_{uv}는 양자화 조작에 의해 취할 수 있는 레벨수가 제한된다. 각 DCT 계수의 양자화는 2차원 DCT 계수의 양자화 폭(step size)을 Q_{uv}, 양자화된 2차원 DCT 계수를 Sq_{uv}라 하면 다음 식과 같이 정의된다.

$$\text{양자화} : Sq_{uv} = round(\frac{S_{uv}}{Q_{uv}}) \quad (3)$$

$$\text{역양자화} : R_{uv} = Sq_{uv} \times Q_{uv} \quad (4)$$

여기서, $round(x)$는 x에 가장 가까운 정수값에 반올림함을 나타낸다. 양자화 폭의 최적치는 입력화상 및 화상 표시장치의 특성에 의존하여 정해지기 때문에 JPEG에서는 규정하고 있지 않다. 그러나, 사전에 약속된 양자화 테이블을 규정하든지 어떤 규칙에 의해 생성시키든지 관계없이 공간주파수가 높을수록 Q_{uv}가 큰 값이 되도록 한다. 이것은 높은 공간주파수의 왜곡일수록 시각 특성상 잘 인식되지 않는 성질을 이용하고 있기 때문이다. JPEG 알고리즘의 테스트용으로 제시된 휘도 성분에 대한 양자화 테이블의 일예와 식(5)에 있어서 임의의 값 q에 의해 생성할 수 있는 양자화 테이블을 〈표 1〉에 나타낸다.

〈표 1〉 양자화 테이블의 일예

〈Table 1〉 Examples of quantization table

(a) 휘도 성분용

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	104	92
49	64	78	87	103	121	121	101
72	92	95	98	112	100	103	99

(b) q = 2 의 경우

3	5	7	9	11	13	15	17
5	7	9	11	13	15	17	19
7	9	11	13	15	17	19	21
9	11	13	15	17	19	21	23
11	13	15	17	19	21	23	25
13	15	17	19	21	23	25	27
15	17	19	21	23	25	27	29
17	19	21	23	25	27	29	31

$$Q_{uv} = (u+v+1)q + 1,$$
$$0 \le u, v < N \qquad (5)$$

따라서, 양자화 계수 Sq_{uv}는 일반적으로 DC 및 AC 성분의 저주파 영역은 0이 아닌 값으로, 고주파 영역은 0이 되기 쉽다. 이때, 합성하고자 하는 기밀 데이터는 양자화 계수 Sq_{uv}가 0이 아닌 곳에 집어넣게 되며, 삽입위치는 화질의 열화를 최소화 할 수 있도록 설정해야 한다. 구체적인 기밀 데이터의 합성 방법에 대해서는 3장에서 나타낸다.

3. 기밀 데이터의 합성법

2장에서 기술한 JPEG에 기밀 데이터를 합성하는 방법에 대하여 기술한다. 화상 부호화에 의한 데이터 압축과정에 기밀 데이터를 몰래 집어 넣을 때 화상의 열화를 최소한으로 억제시키고 압축율에 영향을 주지 않는 범위 내에서 보다 많은 기밀 데이터를 합성하는 방법이 요구된다. JPEG 알고리즘의 중심부인 DCT는 비가역 부호화이기 때문에 이 요구를 충족시킬 수 있는 여지가 남아 있다. DCT 계수의 양자화 과정인 식(3)에 있어서 0이 아닌 Sq_{uv}에 대하여 반올림 과정을 약간 수정하여 기밀 데이터 계열 $M = m_1 m_2 \cdots m_n$, $m_i \in B = \{0, 1\}$의 해당 비트 $m_i (1 \le i \le n)$를 합성시킨다. 즉, M으로 부터 합성하고자 하는 1비트 m_i를 취한 후, 그것이 0이면 Sq_{uv}에 가장 가까운 홀수에, 1이면 짝수에 근사화 시킨다. 따라서, 양자화 계수 Sq_{uv}와 기밀 데이터 m_i를 파라메터로 하는 합성함수 $f(Sq_{uv}, m_i)$에 의한 출력 $Sq_{uv}^{(i)}$가 얻어진다. 이 $Sq_{uv}^{(i)}$의 집합에 대해 엔트로피 부호화를 수행하는 것은 기존의 JPEG 알고리즘과 동일하다.

한편, 수신 측에서는 압축계열로부터 복원을 수행할 때 $Sq_{uv}^{(i)}$가 0 이외의 짝수이면 1을, 홀수이면 0을 추출하여 기밀 데이터인 M을 복원할 수 있다. 물론, $Sq_{uv}^{(i)}$에 대해 역양자화와 역DCT(IDCT)를 수행하면 재생화상이 복원된다. DCT 계수 S_{uv}, 양자화 테이블 Q_{uv}와 기밀 데이터 M = 10110 …의 일부에 대한 합성 및 복호과정의 일예를 〈표 2〉에 나타낸다.

단, 기밀 데이터 m_i는 0이 아닌 양자화 계수 Sq_{uv}의 지그재그 순서에 차례로 대응함을 가정한다. 이때, 표준 JPEG 알고리즘에 의한 양자화 계수 Sq_{uv}와 기밀 데이터가 합성되었을 때의 양자화 계수 $Sq_{uv}^{(i)}$ 사이에는 약간의 오차가 생기게 되며, 이 영향은 복호화 과정에도 미치게 되어 재생화상의 열화를 초래하게 된다. 그

〈표 2〉 합성 및 추출 예

〈Table 2〉 Example of embedding and extraction

DCT 계수	양자화 값	기밀 데이터	양자화 계수	합성 양자화 계수
$S_{00} = 260$	$Q_{00} = 16$	$m_1 = 1$	$Sq_{00} = 16$	$Sq_{00}^{(1)} = 16$
$S_{01} = 49$	$Q_{10} = 11$	$m_2 = 0$	$Sq_{01} = 4$	$Sq_{01}^{(2)} = 5$
$S_{10} = -79$	$Q_{10} = 12$	$m_3 = 1$	$Sq_{10} = -7$	$Sq_{10}^{(3)} = -6$
$S_{20} = 36$	$Q_{20} = 14$	$m_4 = 1$	$Sq_{20} = 3$	$Sq_{20}^{(4)} = 2$
$S_{11} = -16$	$Q_{11} = 12$	$m_5 = 0$	$Sq_{11} = -1$	$Sq_{11}^{(5)} = -1$

(a) 부호화 및 합성과정

합성 양자화 계수	양자화 값	기밀 데이터	합성 역양자화 값	역양자화 값
$Sq_{00}^{(1)} = 16$	$Q_{00} = 16$	$m_1 = 1$	$Sq_{00}^{(1)} \times Q_{00} = 256$	$R_{00} = 256$
$Sq_{01}^{(2)} = 5$	$Q_{01} = 11$	$m_2 = 0$	$Sq_{01}^{(2)} \times Q_{01} = 55$	$R_{01} = 44$
$Sq_{10}^{(3)} = -6$	$Q_{10} = 12$	$m_3 = 1$	$Sq_{10}^{(3)} \times Q_{10} = -72$	$R_{10} = -84$
$Sq_{20}^{(4)} = 2$	$Q_{20} = 14$	$m_4 = 1$	$Sq_{20}^{(4)} \times Q_{20} = 28$	$R_{20} = 42$
$Sq_{11}^{(5)} = -1$	$Q_{11} = 12$	$m_5 = 0$	$Sq_{11}^{(5)} \times Q_{11} = -12$	$R_{11} = -12$

(b) 복호화 및 추출과정

러나, 합성시킬 양자화 계수의 위치를 적절히 선택하게 되면 화질의 열화를 최소화시키면 보다 많은 기밀 데이터를 합성할 수 있다.

여러 가지의 합성방법이 고려되어 질 수 있다. Matsui 연구 그룹에서 제안된 방식[8](이하 KTNM 방식이라 부르기로 한다)에서는 양자화 계수가 0이 아닌 모든 곳에 합성시키기 때문에 화상 및 양자화 값에 따라 합성 데이터의 크기가 가변적이 되며, 용도에 따른 합성량의 제한이 불가능하다. 또한, 합성 알고리즘의 공개에 따른 기밀 정보의 누설이 용이해지는 결점이 있다.

따라서, 압축하고자 하는 화상의 크기와 DCT를 위한 블록 크기 N이 주어지면 합성되는 기밀 데이터의 길이가 고정되는 방식을 고안한다. 즉, $N \times N$ 화소로 이루어지는 1블록에 1비트씩 기밀 데이터를 합성하는 방식이다. 합성하고자 하는 위치는 0이 아닌 양자화 계수 중에서 선정할 수 있으나, 제 3자의 공격에 대비하여 랜덤함수에 의해 임의로 선택되게 한다. 또한, 복원 화상의 열화를 최소화하기 위해서는 Sq_{uv}가 DC 성분, 최대값 및 최소값 등을 선택하게 할 수 도 있다.

4. 실험 및 고찰

JPEG 알고리즘의 DCT 과정에 기밀 데이터를 합성하는 3장에서 제시된 방식들의 성능을 평가하기 위하여 컴퓨터 시뮬레이션을 수행한다. 압축에 사용되는 원화상은 256×256 화소, 8[비트/화소]로 이루어진 SIDBA[9]의 GIRL 데이터와 512×512 화소 크기의 MANDRI 데이터를 대상으로 한다. 합성 알고리즘은 IBM-PC/Pentium에서 Turbo-C Version 2.0으로 구현하였으며, 합성하고자 하는 기밀 데이터는 임의로 선택한 키워드를 RSA 암호화 한 계열이다. 식 (5)에서 사용하는 양자화 인수 q는 1부터 5까지 사용한다. 그 성능은 화질의 열화 상태를 평가하기 위하여 식 (6)과 같이 정의되는 RMS와 주관평가 기준인 MOS를 사용한다.

$$RMS = \sqrt{\frac{1}{M}\sum_{i=1}^{M}(x_i - x_i')^2} \qquad (6)$$

단, M은 원화상의 총 화소수, x_i는 원화상의 i번째 화소값, x_i'은 복호화상의 i번째 화소값을 나타낸다. 또한, 압축의 효과를 평가하기 위한 압축율 ρ는 식 (7)과 같이 정의한다.

$$\text{압축율}(\rho) = \left[1 - \frac{\text{출력 데이터 길이}}{\text{입력 데이터 길이}}\right] \times 100(\%) \qquad (7)$$

4.1 실험1: 문턱치에 의한 합성량의 조절

Matsui 연구 그룹에 의한 KTNM 방식에 문턱치의 개념을 도입하여 합성량과 RMS의

관계를 살펴보았다. 즉, 양자화 계수 Sq_{uv}가 임의로 설정한 고정된 문턱치 Th보다 클 때만 기밀 데이터를 합성하고, 그 이외의 양자화 계수에 대해서는 합성하지 않도록 한다. 따라서, Th를 0으로 한 경우는 KTNM 방식에 해당한다. 그 결과를 〈표 3〉과 그림 3, 4, 5에 나타낸다. 또한, 기밀 데이터를 합성하지 않은 JPEG의 결과도 비교를 위하여 함께 제시한다.

〈표 3〉과 그림 3, 4의 결과, 양자화 요소의 값을 결정하는 q의 값이 커질수록 DCT 계수의 양자화가 거칠게 되므로 복원 화상의 화질은 떨어짐을 알 수 있다. q의 값이 커지면 고주파 영역의 양자화 계수 Sq_{uv}가 0으로 되기 쉽기 때문에 압축율은 향상되지만, 합성할 대상 계수의 수가 줄어들며, 복원 화질의 열화를 초래하는 상반관계에 봉착하게 된다. JPEG의 RMS에 비하여 Th가 0일 때의 KTNM 방식의 열화는 상대적으로 크지만, Th에 의한 본 방식에서는 합성량과 열화의 관계를 선택적으로 이용할 수 있다. Th = 8일때 JPEG에 거의 떨어지지 않는 상태에서 저작권 등의 기밀 정보를 표현하기에 충분함을 알 수 있다. 한편, Th의 변화에 따른 압축율의 변동은 거의 없으나, q값은 양자화 폭에 영향을 미치기 때문에 압축율에 변화가 있음을 알 수 있다.

그림 5는 복원 화상의 화질을 평가한 결과이다. 즉, 원화상 (a)에 대하여 양자화 폭을 결정하는 파라메터 q와 문턱치 Th의 변화에 따른 복원 화상의 화질의 비교이다. 원화상과 JPEG (b)의 비교 결과는 육안으로 거의 구별할 수 없음을 알 수 있으며, 기밀 데이터를 합성한 q = 1에서 Th가 0과 1인 (c)와 (d)도

〈표 3〉 합성량, RMS 및 압축율의 비교

〈Table 3〉 Comparison of embedding data, RMS and compression ratio

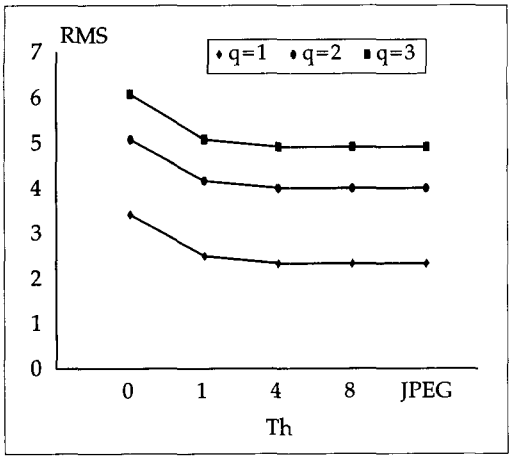
Th / q	RMS					합성량[byte]				압축율(ρ)	
	0	1	4	8	JPEG	0	1	4	8	0,1,4,8	JPEG
1	3.454	2.559	2.416	2.397	2.383	1,470	554	229	131	77	77
3	5.056	4.193	4.032	4.006	3.997	611	262	101	53	86	86
5	6.021	5.090	4.856	4.831	4.819	416	180	65	28	89	89

(a) GIRL (256×256, 8bpp)

Th / q	RMS					합성량[byte]				압축율(ρ)	
	0	1	4	8	JPEG	0	1	4	8	0,1,4,8	JPEG
1	4.391	3.367	2.858	2.765	2.717	10,811	5,956	2,466	1,313	55	55
3	9.177	6.905	6.316	6.258	6.238	6,312	2,741	941	489	76	76
5	12.073	9.225	8.691	8.646	8.634	4,479	1,755	585	320	83	83

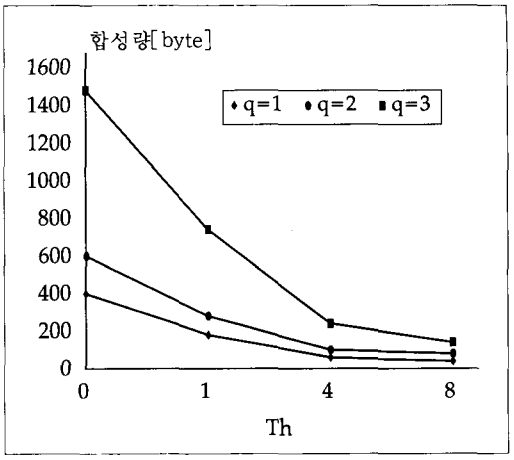
(b) MANDRI (512×512, 8bpp)

(a)와의 차이점을 식별할 수 없는 양호한 화질을 얻었다. 그러나, $q = 3, 5$로 하였을 때의 (e), (f)는 왜곡을 인지할 수 있을 정도의 열화를 보이고 있다.



〈그림 3〉 Th의 변화에 따른 RMS(GIRL)

〈Fig.3〉 RMS according to Th



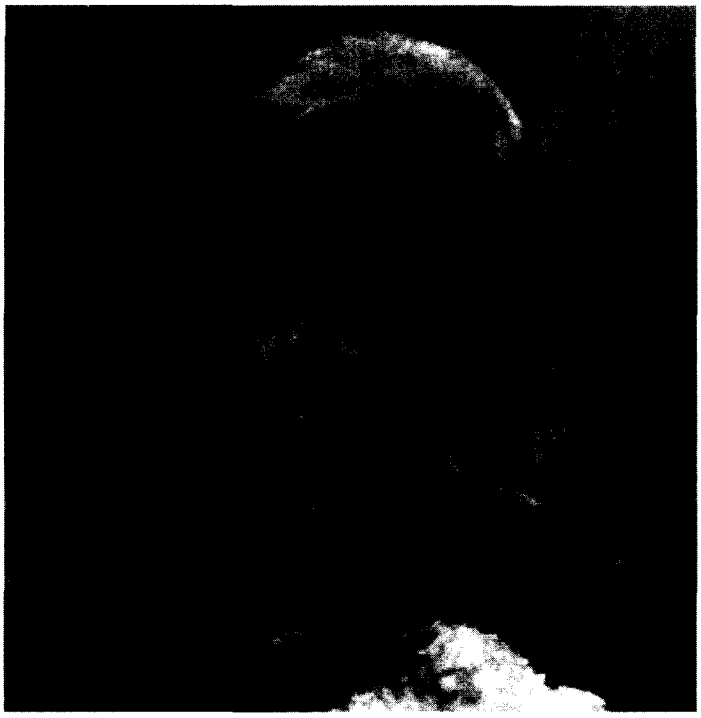
〈그림 4〉 Th의 변화에 따른 합성량(GIRL)

〈Fig.4〉 Embedding quantity according to Th

(a) 원 화상(original image)

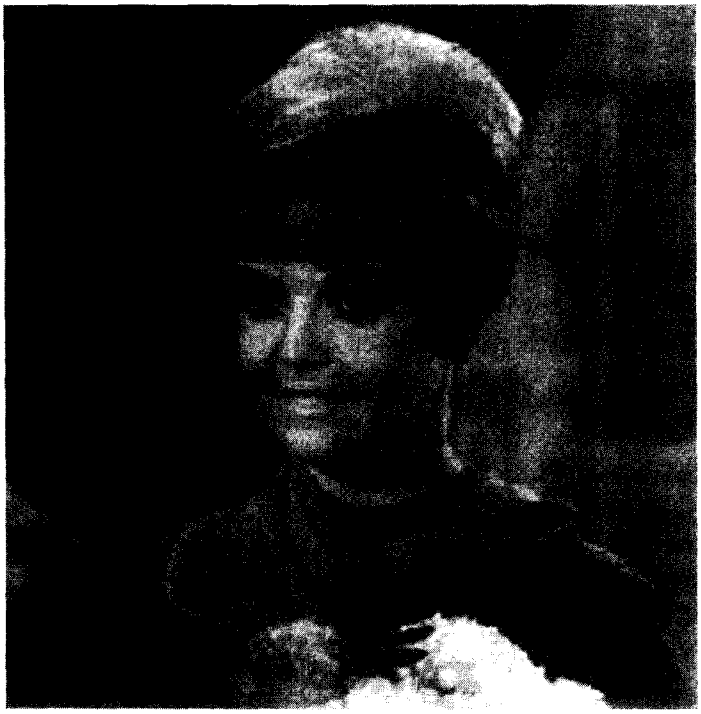
(b) JPEG [q, RMS] = [1, 2.383]

(c) Embedding method [q, Th, RMS]=[1, 0, 3.454]



(d) Embedding method [q, Th, RMS]=[1, 1, 2.559]

(e) Embedding method [q, Th, RMS]=[3, 0, 5.056]



(f) Embedding method [q, Th, RMS]=[5, 0, 6.021]

〈그림 5〉 복원 화상의 비교

〈Fig.5〉 Comparison of decoded images

4.2 실험2: 고정 크기의 데이터 합성

응용에 따라서는 기밀 데이터의 크기가 고정되어 있을 수도 있다. 이 경우, 화질의 열화를 최소화시키고 알고리즘의 구성이 간단하면서도 제3자의 공격에 강인성을 부여 하기 위하여 1블럭 중의 0이 아닌 Sq_{uv} 중 1개를 선택하여 합성시키는 방법이 고려되어 질 수 있다. 양자화 계수 중 DC 성분에 해당하는 Sq_{00}, 최대값인 Sq_{max} 및 최소값인 Sq_{min} 중에 선택하여 합성시키는 방법이다. 일반적으로 DCT 계수중 DC 성분은 그 블럭의 대표값으로써 휘도값에 영향을 미치기 때문에 열화를 최소화할 수 있다. 그러나, 제3자의 공격에 대비하기 위하여 적절히 설계된 랜덤함수에 의한 계수 Sq_{ran}를 선택하게 한다. 따라서, 원화상과 블럭의 크기가 정해지면 합성 가능한 기밀 데이터의 크기도 고정된다. 이 실험의 결과를 〈표 4〉에 나타낸다.

〈표 4〉의 결과, 가장 양호한 화질을 달성할 수 있는 것은 DC 성분(Sq_{00})에 기밀 데이터를 합성하는 경우이지만, 랜덤함수에 의해 임의로 선택된 양자화 계수 Sq_{ran}에 합성하여도 큰 열화없이 동등한 량의 기밀 데이터를 합성할 수 있음을 알 수 있다.

〈표 4〉 합성위치에 따른 성능 비교

〈Table 4〉 Performance comparisons according to embedding position

합 성 위 치	q	GIRL(256×256)			MANDRI(512×512)		
		RMS	합성량(byte)	압축률(ρ)	RMS	합성량(byte)	압축률(ρ)
Sq_{00}	1	3.159	128	77	4.283	512	55
	3	4.941	128	86	8.960	512	76
	5	5.952	128	89	11.802	512	82
Sq_{max}	1	3.160	128	77	4.283	512	55
	3	4.942	128	86	8.960	512	76
	5	5.953	128	89	11.803	512	82
Sq_{min}	1	3.162	128	76	4.286	512	55
	3	4.956	128	86	8.967	512	76
	5	5.970	128	89	11.817	512	82
Sq_{ran}	1	3.163	128	76	4.287	512	55
	3	4.975	128	86	8.971	512	76
	5	5.968	128	89	11.839	512	82

5. 결 론

이 논문에서는 칼러 정지화상 압축을 위해 표준화 방식으로 제정된 JPEG 알고리즘을 이용하여 기밀 데이터를 몰래 집어 넣는 이른바 화상 심층암호 기법에 대하여 살펴 보았다. 기존의 데이터 압축 알고리즘은 저장공간의 유효이용과 전송시간의 단축을 위한 압축의 관점에서만 고려되어 왔으나, 저작권 보호를 비롯한 기밀 데이터를 제3자가 인지할 수 없는 형태로 동시에 처리할 수 있는 새로운 응용이 요구되고 있다.

DES나 RSA로 대표되는 현대암호와 같이 공개된 알고리즘 만큼의 암호학적 안전성은 기대할 수 없지만, 간단한 알고리즘으로 비밀통신 자체를 인식할 수 없도록 목적정보에 잡음의 형태로 기밀 데이터를 숨겨 넣는 기법의 실용성이 크게 기대된다. 만약, 높은 강도의 기밀이 유지되어야 하는 경우, 기밀 데이터 자체에 기존의 암호화 기법을 수행한 후에 합성 알고리즘에 적용하면 암호학적 안전성도 보장될 수 있다.

고정 문턱치를 도입하여 합성되는 기밀 데이터의 양과 복원 화상의 화질과의 관계를 살펴 보았으며, 기존의 JPEG 알고리즘에 의한 성능과 비교평가 하였다. 또한, 고정 크기의 기밀 데이터를 합성시키기 위하여 블럭당 1비트의 데이터를 합성하는 방법을 제시하여 그 성능을 평가하였으며, 알고리즘의 공개에 따른 제3자의 공격에 대비하기 위하여 합성 위치를 랜덤하게 선정하여도 큰 열화없이 수행가능함을 보였다. 향후, 이와같은 화상 심층암호에 관한 연구는 네트워크화가 진전됨에 따라 정보보안과 데이터 압축의 기능을 동시에 수행할 수 있는 새로운 정보통신 서비스에 응용되기를 기대한다.

참 고 문 헌

[1] G.K. Wallace, "The JPEG Still Picture Compression Standard", Comm. of the ACM, Vol.34, No.4, pp.30-44, (Apr. 1991)

[2] JBIG, "Coded Representation of Picture and Audio Information Progressive Bi-level Image Compression", ISO / IEC JTC1 / SC29 / WG29 (Dec. 1991)

[3] D.L. Gall, "MPEG : A Video Compression Standard for Multimedia Application," Comm. of the ACM, Vol.34, No.4 pp.46-58 (Apr. 1991)

[4] J.Seberry, J.Pieprzyk, "Cryptography: An Introduction to Computer Security", Prentice Hall (1989)

[5] H. Suzuki, S.Arimoto, "Embedding-in-Image Data Encryption with Arithmetic Coding", The 1986 Symposium on Cryptography and Information Security (SCIS) (in Japanese)

[6] N.Koike, T. Matsumoto, H.Imai, "A Scheme for Copyright Protection of Digital Images", The 1993 SCIS93-13C (in Japanese)

[7] K.R.Rao, P.Y, "Discrete Cosine Transform Algorithms, Advantages, Application", Academic Press Inc. (1990)

[8] T.kataoka et al, "Embedding a Document into Color Picture Data under Adaptive Discrete Cosine Transform Coding", IEICE, Vol.J72-B-I, No.12, pp.1210-1216 (1989.12) (in Japanese)

[9] M.Onoe, et al, "SIDBA:Standard Image Data Base", Multidimensional Image Processing Center Report 79, Institute of Industrial Science, Univ. of Tokyo (Mar. 1979)

□ 著者紹介

박 지 환(Ji Hwan Park) 정회원

1984년 경희대학교 전자공학과 졸업(공학사)
1987년 日本國立電氣通信大學 情報工學科 修了 (工學修士)
1990년 日本橫浜國立大學 電子情報工學科 修了 (工學博士)
1990년～현재 부산수산대학교 전자계산학과 전임강사, 조교수, 부교수
1994년～1995년 日本東京大學生產技術研究所 客員研究員

※ 주관심 분야 : 멀티미디어 압축, 암호학 응용, 오류제어부호 등

박 태 진(Tae Jin Park)

1991년 동의대학교 물리학과 졸업 (이학사)
1994년 부산수산대학교 전산정보학과 (이학석사)
1994년～현재 밀양산업대학교 강사

※ 주관심 분야 : 멀티미디어 압축, 암호학 응용, 화상처리 등