DOI: 10.3745/KIPSTC.2008.15-C.3.149

코드블록 노이즈 분산의 변화를 최소화하는 안전한 JPEG2000 스테가노그라피

윤 상 문[†] · 이 해 연[††] · 주 정 춘[†††] · Cong-Nguyen Bui[†††] · 이 흥 규[††††]

요 약

JPEG2000은 차세대 이미지 압축 포맷으로 JPEG에 비하여 우수한 압축률과 화질을 제공할 수 있다. JPEG2000 이미지를 커버 오브젝트로 사용하는 lazy-mode 스테가노그라피는 압축과정에서 발생하는 정보 손실에 의해 메시지가 손실되지 않도록 제안된 알고리즘으로 많은 양의 메시지 삽입이 가능하다. 그러나 이 방법은 메시지 삽입으로 인하여 코드블럭 노이즈 분산의 변화를 발생하게 되고, 이러한 특징을 기반으로 하는 Hilbert-Huang 변환 (HHT) 기반의 스테거낼리시스에 의하여 메시지 삽입여부가 탐지될 수 있다. 본 논문에서는 코드블럭 노이즈 분산의 변화를 예측하고, 이를 최소화하도록 메시지를 삽입하여 HHT 기반 스테거낼리시스에 의해 탐지되지 않는 새로운 JPEG2000 스테가노그라피 알고리즘을 제시한다. 코드블록 노이즈 분산의 변화를 예측하기 위하여 low precision code-block variance와 low precision code-block noise variance를 활용하였다. 또한 메시지 삽입 후의 높은 영상 화질을 유지하기 위하여 JPEG2000의 quality layer 정보를 활용하였다. 제안한 알고리즘의 성능을 보이기 위하여 2048장의 다양한 영상에 대하여 분석을 수행하였고, 이를 통하여 HHT 기반 스테거낼리시스 방법에 안전함을 증명하였다.

키워드 : JPEG2000, 스테가노그래피, 레이지모드, 스테거낼리시스, Hilbert-Huang 변환

Secure JPEG2000 Steganography by the Minimization of Code-block Noise Variance Changes

Sang Moon Yoon[†] · Hae-Yeoun Lee[††] · Jeong-Chun Joo[†††] · Cong-Nguyen Bui[†††] · Heung-Kyu Lee[††††]

ABSTRACT

JPEG2000 is the upcoming image coding standard that provides better compression rate and image quality compared with JPEG. Lazy-mode steganography guarantees the safe communication under the two information loss stages in JPEG2000. However, it causes the severe changes of the code-block noise variance sequence after embedding and that is detectable under the steganalysis using the Hilbert-Huang transform (HHT) based sequential analysis. In this paper, a JPEG2000 lazy-mode steganography method is presented. The code blocks which produce the sudden variation of the noise variance after embedding are estimated by calculating low precision code-block variance (LPV) and low precision code-block noise variance (LPNV). By avoiding those code-blocks from embedding, our algorithm preserves the sequence and makes stego images secure under the HHT-based steganalytic detection. In addition, it prevents a severe degradation of image quality by using JPEG2000 quality layer information. On various 2048 images, experiments are performed to show the effective reduction of the noise variation after message embedding and the stable performance against HHT-based steganalysis.

Key Words : JPEG2000, Steganography, Lazy-Mode, Steganalysis, Hilbert-Huang Transform

1. 서 론

비밀통신에 사용되는 암호화는 메시지 자체를 키를 이용하여 제 3자가 해독할 수 없는 형태로 만들고 이를 통신경로를 통해 전송하는 방법이다. 이에 반해 스테가노그라피 (steganography) 는 콘텐츠에 비밀 메시지 존재여부 자체를 숨기는 것을 목적으로 하는 비밀통신 방법이다. 따라서 스테가노그라피는 단순 추측에 의한 확률(50%)보다 높은 판단 요소를 제공한다면 실패한 것으로 간주된다.

현재 인터넷 등에서 많이 사용되는 JPEG 이미지는 특정 크기의 화소 블록을 단위로 하는 DCT를 사용하므로 높은 압축률에서는 블록 경계면에서 화질의 열화가 심해지는 블

† 정 회 원 : 금융결제원 연구원
†† 정 회 원 : 국립금오공과대학교 컴퓨터공학부 교수
††† 준 회 원 : 한국과학기술원 전자전산학과 박사과정
†††† 정 회 원 : 한국과학기술원 전자전산학과 교수

논문접수 : 2008년 1월 25일
수 정 일 : 2008년 3월 20일
심사완료 : 2008년 3월 24일

록효과가 발생한다. 이를 보완하여 DWT기반 차세대 이미지 압축방법인 JPEG2000이 표준화되었고 사용분야가 증가하고 있다[1]. 따라서, JPEG2000을 커버 이미지로 활용하는 스테가노그라피에 대한 연구가 증가하고 있는 추세이고, 이에 대한 연구는 중요하다[2].

현재까지 발표된 JPEG2000 스테가노그라피는 양자화된 계수를 이용하는 BPCS 스테가노그라피 방법과 raw 코딩되는 비트를 이용하는 lazy-mode 스테가노그라피 방법이 있다[3, 4, 5]. 이들 각 방법에 대하여 다음 절에서 설명하고, 문제점에 대하여 정리하였다. 정보손실을 최소화하며 높은 메시지 삽입용량을 제공하는 lazy-mode 스테가노그라피는 메시지 삽입으로 변경되는 MRP 스트림에 의해 코드 블록의 노이즈가 증가하는 것에 착안한 Hilbert-Huang 변환(HHT) 기반의 스테거낼리시스에 의해 탐지될 수 있다[6].

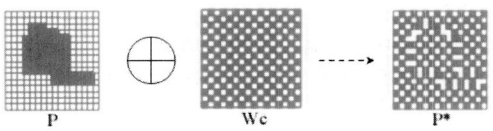
본 논문에서는 기존의 lazy-mode 스테가노그라피의 메시지 삽입용량과 이미지 화질은 그대로 보존하면서 HHT 기반의 스테거낼리시스에 안전한 JPEG2000 스테가노그라피 알고리즘을 제안한다. 제안한 방법에서는 각 코드 블록에 대하여 메시지 삽입시 발생할 수 있는 코드 블록의 노이즈 영향을 추정하여 영향이 작은 코드 블록부터 메시지를 삽입함으로써 HHT 기반의 스테거낼리시스 방법에 탐지되지 않도록 보안성을 향상시켰고, JPEG2000의 quality layer 정보를 사용함으로써 메시지 삽입 후 영상 화질의 저하를 방지하였다. 이와 같은 보안성 및 화질향상을 위한 방법들에 대하여 3장에서 구체적으로 설명하도록 하겠다.

본 논문의 구성은 다음과 같다. 2장에서는 JPEG2000 기반의 스테가노그라피 및 스테거낼리시스 기술을 분석한다. 3장에서는 이를 바탕으로 보다 안전한 새로운 JPEG2000 스테가노그라피 알고리즘을 제시하고, 4장에서 다양한 실험결과를 통해 제안한 알고리즘의 성능을 평가한다. 마지막으로 5장에서는 결론과 향후 연구과제에 대하여 살펴본다.

2. JPEG2000 기반의 스테가노그라피 및 스테거낼리시스 기술 분석

2.1 JPEG2000 BPCS 스테가노그라피

BPCS(Bit-Plane Complexity Segmentation) 스테가노그라피는 먼저 이미지를 비트 플레인에 따라 나누고, 각 플레인을 일정 크기의 블록으로 분리한다. 분리된 블록 복잡도가 임계값 T보다 클 경우 같은 크기를 가지는 메시지 블록으로 대체한다. 만일 메시지 블록의 복잡도가 T보다 작을 경우에는 (그림 1)에 나타난 것과 같이 삽입할 메시지(P)를



(그림 1) 비트 블록 P에 대한 conjugation P* 연산의 예

마스크 패턴(Wc)와 conjugation 연산을 적용하여 비트플레인으로 삽입한다[3, 7]. conjugation이 수행된 메시지 블록은 따로 위치를 명시해야만 수신자가 메시지를 올바로 복원할 수 있으므로, 메시지 헤더로 구성하여 정해진 위치(첫 번째 블록 등)에 저장해야 한다.

BPCS 스테가노그라피 기법을 JPEG2000에 적용하기 위해서는 공간 영역의 픽셀 값이 아니라 양자화된 DWT 계수(quantization index)를 대상으로 한다. 하지만 JPEG2000의 압축률 제어(rate control) 과정에서 최종 비트 스트림으로부터 제외되는 계수가 존재하기 때문에, 커버 이미지를 Tier-2 코딩까지 수행하여 압축 스트림을 생성하고, 이를 다시 압축 해제하여 얻은 DWT 계수들을 이용하여 앞서 설명한 BPCS 방식에 따라 메시지를 삽입한다. 하지만 이 기법은 메시지 삽입 후에는 무손실 압축으로 최종 스트림을 생성하여야 하므로 최초의 이미지 사이즈보다 더 커지게 된다.

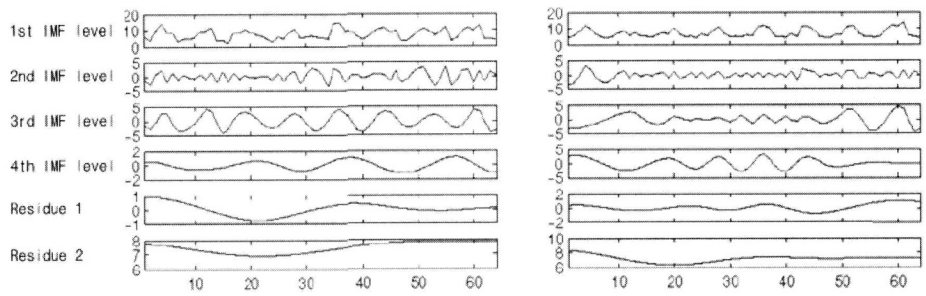
2.2 Lazy-mode 스테가노그라피

Su가 제안한 lazy-mode 스테가노그라피는 raw 코딩되는 비트에 메시지를 삽입하는 접근 방식을 이용하였다[4]. JPEG2000에서는 하위 플레인들에 속하는 비트들은 균일분포를 따르기 때문에 엔트로피 코딩으로 비트 스트림 단축의 효과를 거의 볼 수 없기 때문에 복잡도 감소와 속도 향상을 위해 이 부분을 raw 코딩하는 lazy-mode를 지원하고 있다. 즉, 상위 4개의 비트 플레인을 엔트로피 코딩하고, 나머지 하위 비트 플레인의 SPP(Significance Propagation Pass)와 MRP(Magnitude Refinement Pass)를 거치는 비트는 raw 코딩한다.

Lazy-mode 스테가노그라피에서는 오직 MRP를 타깃으로 하는데, CUP(Cleanup Pass)는 모드에 상관없이 항상 run-length 코딩이 적용되고, SPP는 significance와 sign 정보를 생성하기 때문에 이를 변경하는 것은 디코딩시 큰 에러를 유발할 수 있기 때문이다. MRP의 비트를 변경하는 것 역시 이미지의 품질 저하를 유발할 수 있지만, backward embedding 기법을 통해 적절한 MRP의 subset을 찾아내어 메시지 삽입에 이용하였다. 즉, 되도록 많은 메시지 데이터를 이미지 품질에 영향을 덜 주는 방향으로 삽입하는 것이다. JPEG2000에서는 생성된 코드 블록별 스트림이 중요도에 따라 레이어에 나누어 배치되고, 높은 우선순위를 가지는 레이어가 우선적으로 전송된다. 다시 말하면, 먼저 배치되는 스트림은 이미지 품질에 큰 영향을 미치는 부분이고, 나중 레이어에 위치하는 데이터일수록 상대적으로 이미지 품질에 작은 영향을 미치는 부분이다. 따라서 lazy-mode 스테가노그라피에서는 tier-2 코딩에서 레이어에 해당 MRP 스트림이 배치된 이후, 낮은 우선순위의 레이어에 위치하는 MRP 스트림부터 우선 변경하여 메시지를 삽입한다.

2.3 Hilbert-Huang 변환 기반 스테거낼리시스

Hilbert-Huang 변환(HHT) 기반의 스테거낼리시스는 JPEG2000 lazy-mode 스테가노그라피를 대상으로 하는 탐



(그림 2) (a) 스테고 이미지의 IMF 및 (b) 가우시안 잡음이 들어간 정상 이미지의 IMF

지 기법으로, 변경되는 MRP 스트림에 의해 코드 블록의 노이즈가 증가하는 것에 착안한 방법이다[6]. Backward embedding에 따라 우선순위가 낮은 레이어에 배정되는 MRP가 많으면 많을수록 해당 코드 블록의 변경이 커지고, 이는 해당 코드 블록과 이웃하는 블록의 노이즈 분산으로 이루어진 시퀀스(noise variance sequences)의 변동이 커지는 경향을 보이게 된다. 다시 말하면, 스테고 이미지의 코드 블록 노이즈 분산의 시퀀스가 정상 이미지의 것보다 변동이 크게 될 것이다. 단, 두 코드 블록의 서브밴드 노이즈 분산은 같다고 가정한다.

Tan은 이 차이를 계산하기 위하여 HHT를 도입하였다[6, 8]. HHT는 Empirical mode decomposition (EMD)와 Hilbert spectral analysis로 구성되는데, EMD는 복합성분의 주어진 시퀀스를 다음 조건을 따르는 단일성분의 신호인 IMF(Intrinsic Mode Functions)로 나타낸다: (1) 극점(extrema)과 zero-crossing의 개수가 같거나 최대 하나만 차이가 난다, (2) local maxima에 의해 정의되는 곡선과 local minima에 의한 곡선의 평균값이 어느 순간 0이 되는 점이 존재한다.

IMF들을 $\{imf_i(t), i \in N\}$ 으로 나타낸다면, $imf_i(t)$의 Hilbert 변환 $imf_i^H(t)$는 다음과 같이 계산한다.

$$imf_i^H = \frac{1}{\pi} P \int_{-\infty}^{\infty} \frac{imf_i(u)}{t-u} du$$

여기서 P는 Cauchy principal value를 뜻한다. 따라서 $imf_i(t)$의 진폭(amplitude) $a(t)$와 위상(phase) $\theta(t)$는 다음과 같다.

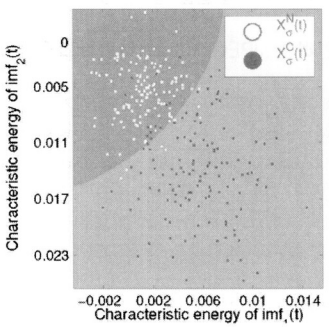
$$a(t) = \sqrt{(imf_i(t))^2 + (imf_i^H(t))^2}$$

$$\theta(t) = \tan^{-1}\left(\frac{imf_i^H(t)}{imf_i(t)}\right)$$

$X_\sigma^C(t)$를 스테고 이미지의 코드 블록 노이즈 분산 시퀀스(noise variance sequence)라 하고, $X_\sigma^N(t)$를 노이즈가 첨가된 정상 이미지의 것이라고 하자. 그리고 $imf_i^C(t)$와 $imf_i^N(t)$을 각각 $X_\sigma^C(t)$와 $X_\sigma^N(t)$의 IMF라 하자. 만약 두 시퀀스의 서브밴드 노이즈 분산(noise variance)이 같다면, $X_\sigma^C(t)$의 변동이 더 커야 한다. (그림 2a)는 lazy-Mode 스테가노그라피 방식으로 5% 메시지를 삽입한 스테고 이미지의 4개 IMF 레벨과 나머지(residue)이다. (그림 2b)는 스테고 이미지와 서브밴드 노이즈 분산을 맞추어 주기 위해 가우시안 잡음을 첨가한 이미지에 대한 같은 결과이다. 예상한 것과 같이 (그림 2a)의 변동이 (그림 2b)보다 큰 것을 확인할 수 있다.

(그림 2)에서 보는 것처럼 첫 번째와 두 번째 IMF에서의 차이는 식별이 가능하고, 나머지 낮은 주파수 영역에 있는 IMF들은 차이를 식별하기가 쉽지 않다. 따라서, 첫 번째와 두 번째 IMF의 진폭에 대한 평균을 구하여 2차원 특성 벡터(feature vector)로 만들고, SVM(Support Vector Machine) 알고리즘을 통해 학습시킨다[9]. (그림 3)를 보면 스테고와 노이즈를 첨가한 정상 이미지 간의 영역이 비교적 명확하게 나누어진다는 것을 알 수 있다.

420개의 샘플을 사용하여 훈련한 SVM에 대한 180개 실험 샘플을 분류한 결과 평균 탐지율(AC), 스테고 이미지를 스테고 이미지로 판별할 확률 (TP), 정상 이미지를 스테고 이미지로 판별할 확률 (FP)은 <표 1>과 같다.

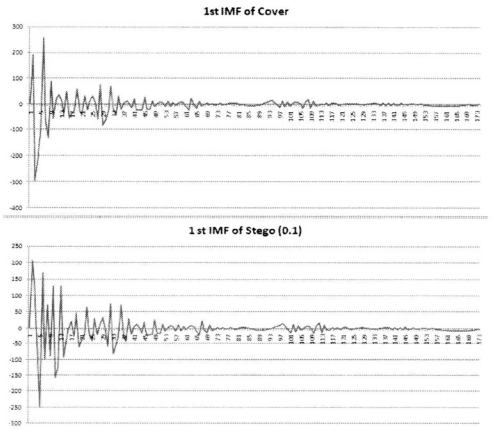


(그림 3) 420개의 샘플을 사용하여 훈련한 SVM에 대한 180개의 실험 샘플의 분류

〈표 1〉 180개 이미지에 대한 테스트 결과

	AC	TP	FP
Classification Probability	90.6%	90%	8.9%

HHT 기반 lazy-mode 스테거낼리시스는 각 코드 블록의 노이즈 분산을 추정한 후 이를 하나의 시퀀스로 만들어서 HHT 변환 후 첫 번째와 두 번째의 IMF에 대한 주파수를 분석하여 메시지 탐지 여부를 결정한다. 하지만 실제 탐지 절차는 커버와 스테고 이미지가 동일한 서브밴드 노이즈 분산을 가질 때를 가정한 결과이기 때문에 실용적이라 할 수 없다. 하지만 기본 아이디어인 메시지 삽입(노이즈 첨가) 후의 각 코드 블록 노이즈 분산 시퀀스의 변동이 커지게 되는 것은 사실이기 때문에, 이 점을 이용하여 스테거낼리시스 연구자들의 공격이 가능하다. 메시지 삽입 후에 노이즈 분산 시퀀스의 고주파수 성분이 커지게 되며, 이 점을 통해 첫 번째와 두 번째 IMF의 Hilbert 변환의 에너지가 전보다 더 커질 것이라는 예측이 가능하다. (그림 4)에서 알 수 있는 것처럼 메시지를 10% 랜덤하게 삽입한 경우 IMF 변동이 더 커진다.



(그림 4) 메시지를 삽입 전(위) 및 후(아래) IMF 변동

3. 제안하는 JPEG2000 스테가노그라피 알고리즘

본 절에서는 기존의 lazy-mode 스테가노그라피의 메시지 삽입용량과 이미지 화질은 그대로 보존하면서 HHT 기반의 스테거낼리시스에 안전한 JPEG2000 스테가노그라피 알고리즘을 설명한다. 각 코드 블록에 대하여 메시지 삽입시 발생할 수 있는 코드 블록의 노이즈 영향을 추정하여 영향이 작은 코드 블록부터 메시지를 삽입함으로써 보안성을 향상시켰고, JPEG2000의 quality layer 정보를 사용함으로써 메시지 삽입 후 영상 화질의 저하를 방지하였다. 이들 방법에 대하여 각각 설명한 후에 메시지 삽입 및 검출 기법에 대하여 기술하도록 한다.

3.1 노이즈 분산을 최소화하는 코드 블록 추정 기법

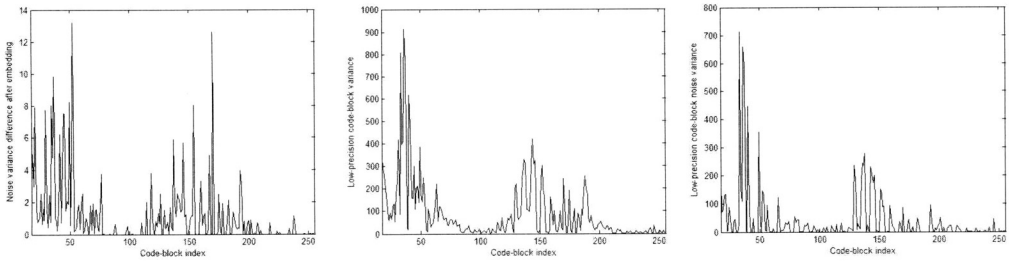
메시지 삽입은 곧 노이즈를 첨가하는 효과와 같기 때문에 원래 값들이 비슷했던 영역에서는 노이즈 분산이 증가할 것이고, 값들의 차이가 심한 영역에서는 오히려 노이즈 분산이 감소할 수도 있다. 또한 같은 크기의 영역에 같은 비율의 메시지를 삽입하더라도 각 영역의 특성에 따라 노이즈 분산의 증감폭은 차이가 난다. 이 점을 이용해 노이즈 분산의 변동이 되도록 작게 일어나는 영역을 찾아서 메시지를 먼저 삽입한다면, 코드 블록의 노이즈 분산 시퀀스의 변동을 줄일 수 있고, HHT 기반 스테거낼리시스에 안전하다.

노이즈 분산은 지역 분산을 기초로 추정된다[10]. 분산은 평균과의 거리를 제곱한 값에 대한 평균으로 계산하므로, 약간의 노이즈 첨가로 인해 이 값이 더욱 커지는 경우는 원래부터 코드 블록 내의 값들이 평균과 상당히 차이 났던 영역에서 가능할 것이다. 따라서 각 코드 블록의 분산이 메시지 삽입후의 노이즈 분산과 비슷한 형태일 것이므로, 코드 블록 내의 분산이 큰 지역이 메시지 삽입 후에 노이즈 분산의 변동폭이 커지게 될 것이다. 따라서 노이즈 분산의 변동폭을 최소화하기 위해서는 이런 부분들이 메시지 삽입시 낮은 우선순위를 가지게 할 필요가 있다. 하지만 단순히 각 코드 블록의 분산을 계산한 다음 역순으로 메시지를 삽입할 수는 없다. 왜냐하면, 메시지를 삽입함으로서 코드 블록의 분산이 변하게 되고, 이는 수신자 측에서 처음에 메시지를 넣은 것과 다른 순서로 메시지를 추출하게 만들기 때문이다. 따라서 임베딩 과정에 영향을 받지 않으면서 노이즈 분산 증감폭이 작은 코드 블록을 예측하여 송수신측에서 동일한 순서를 결정할 수 있는 다른 측정 기준이 필요하다. 본 논문에서는 low precision code-block variance(LPV)와 low precision code-block noise variance(LPNV)를 활용하여 노이즈 분산의 증감폭을 예측하고, 이를 이용하여 증감폭이 작은 코드 블럭부터 메시지를 삽입함으로써 HHT 기반 JPEG2000 스테거낼리시스에 안전성을 달성하였다.

3.1.1 Low Precision Code-Block Variance

JPEG2000의 lazy-mode는 상위 4개 비트 플레인을 제외한 하위 비트 플레인에 대해서 raw 코딩을 수행한다. 그리고 메시지 삽입은 오직 raw 코딩된 MRP에서만 일어나기 때문에 이보다 상위 비트 플레인의 값은 메시지 삽입으로 변하지 않는다. 그러므로 압축률 제어 과정 이후 상위 4개 비트 플레인을 이용하여 계산한 low precision code-block variance (LPV)를 이용해서 코드 블록의 순서를 결정하고 그 순서에 따라 메시지를 삽입할 수 있다. 메시지 삽입 후에도 코드 블록의 LPV는 변하지 않기 때문에 수신자 측에서 동일하게 계산하여 송신자 측과 정확히 같은 순서로 다시 원래의 메시지를 추출해낼 수 있다.

(그림 5)서 Baboon 커버 이미지와 스테고 이미지의 노이즈 분산 차이를 LPV와 비교해 보면, 노이즈 분산 차이가 큰 부분에서 LPV 값도 큰 것을 확인할 수 있다. 따라서, 각



(a) (b) (c)

(그림 5) (a) 메시지 삽입 후의 노이즈 분산 차이, (b) LPV, 및 (c) LPNV

코드 블록의 LPV를 이용하여 메시지 삽입 후의 노이즈 분산의 변동을 효과적으로 예측할 수 있으며, LPV가 작은 것부터 메시지 삽입 우선순위를 정한다면 메시지 삽입 후의 노이즈 분산의 변동을 최소화할 수 있다. LPV를 계산하는 과정을 pseudo 코드로 표현하면 다음과 같다.

```
Calculate the maximum number of raw-coded MRPs
(= nm) in a code-block
For each location m, n in a code-block {
    // Read a value at (m, n)
    val = Code_Block_Value[m, n]
    // Set all zeros to nm bits of the value from
right
    mask = ~((0x1 << nm) - 1)
    val = val & mask
    Store the low precision code-block value
}
Calculate a variance of the low presicion
code-block values
```

한가지 고려할 사항은 LPV가 0인 코드블럭은 완전한 flat area(모든 pixel value가 동일)를 의미하므로 이러한 코드블록에 메시지를 삽입한다면 노이즈 분산이 굉장히 크게 증가한다. 따라서, 본 논문에서는 LPV가 일정(δ=0.5) 이상인 코드 블록에 대해서만 메시지를 삽입한다.

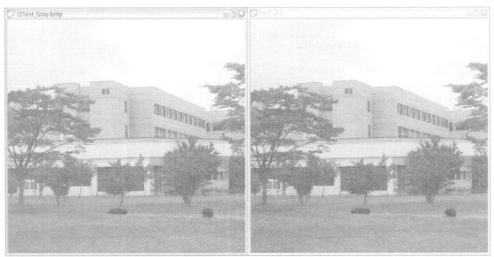
3.1.2 Low Precision Code-Block Noise Variance

노이즈 분산이 급격하게 증가하는 코드 블록을 LPV로 예측할 수 있다면, low precision code-block noise variance (LPNV)도 고려해볼 수 있다. 왜냐하면 지역 분산의 히스토그램을 통해 노이즈 분산을 추정하기 때문에 그 값이 크다는 것은 곧 큰 값을 가지는 지역 분산이 많다는 뜻이기 때문이다. (그림 5)에서 메시지 삽입 전후의 노이즈 분산 차이와 LPNV를 비교해 보면 LPV 때보다는 상관관계가 다소 떨어지지만 LPNV가 큰 코드 블록에서는 노이즈 분산의 변동폭 역시 크다는 것을 알 수 있다. 따라서, LPNV 역시 코드 블록 노이즈 분산의 변동폭을 예측하기 위한 요소로 활용이 가능하다.

3.1.3 화질 개선의 필요성

LPV와 LPNV는 코드 블록의 노이즈 분산 변동 폭의 크기를 예측하는데 좋은 측정 기준이다. 하지만 DWT의 LL 서브밴드가 공간 영역의 정보를 포함하고 있는 것으로 미루어볼 때 LPV와 LPNV가 작은 코드 블록은 곧 픽셀 값의 변화가 많지 않은 영역을 나타내므로, 이 부분에 메시지를 삽입한다면 (그림 6)와 같이 눈에 띄게 화질이 저하될 수 있다. 따라서 메시지 삽입이 화질에 미치는 영향을 고려하기 위한 요소가 필요하며, 본 논문에서는 JPEG2000의 quality layering을 사용하였다.

기존 lazy-mode 스테가노그라피에서는 quality layering을 이용해 backward embedding을 제안했는데, 가장 높은 레이어에 속하는 (즉, 덜 중요한) raw 코딩된 MRP부터 차례대로 메시지를 삽입하여 원하는 화질 수준을 얻을 때까지 점점 낮은 레이어에 있는 패스들까지 사용하는 것이다[4]. 이처럼 화질 개선을 위해 LPV, LPNV와 더불어 해당 raw 코딩된 MRP의 레이어 정보까지 고려해서 메시지를 삽입할 코드 블록을 선택하도록 한다면, 코드 블록 노이즈 분산 변동폭을 줄이면서 화질 개선의 효과까지 기대할 수 있다.



(그림 6) LPV와 LPNV만을 고려하여 5% 메시지 삽입 전 및 후의 화질 비교

3.2 메시지 삽입 절차

본 논문에서는 압축률 제어에 의해 메시지가 제외되거나 이미지 크기가 증가하는 등의 단점을 극복할 수 있는 JPEG2000 lazy-mode를 이용하여 메시지를 삽입하는 방법을 채택하였다. 즉, tier-2 코딩 과정과 압축률 제어까지 완

료된 후 raw 코딩된 MRP에 메시지를 삽입한다. 또한, 코드 블록 노이즈 분산 변동폭을 최소화하도록 코드 블록의 순서를 결정하여 HHT기반 JPEG2000 스테거낼리시스에 의해 탐지되지 않도록 한다. 코드 블록의 순서는 앞서 살펴본 LPV, LPNV와 quality layering 정보를 이용해 다음과 같이 순서 가중치(PWV, Position Weight Value)를 계산하여 결정한다.

$$PWV = \alpha \cdot \text{LPV} + \beta \cdot \text{LPNV} + \gamma \cdot \text{Layer\_No}$$

이와 같이 계산한 순서 가중치별로 정렬한 후 순서 가중치가 가장 작은 코드 블록의 raw 코딩된 MRP부터 차례대로 비트 스트림에 메시지를 삽입한다. 이러한 순서로 메시지를 삽입한다면 코드 블록 노이즈 분산 변동폭을 최소화함으로써 HHT 기반 스테거낼리시스 방법을 극복할 수 있다. 메시지 삽입 과정을 pseudo 코드로 표현하면 다음과 같다.

```
After Tier-1, 2 coding and rate control in
 JPEG2000 compression stages,
For each code-block {
    LPN = Low Precision Variance;
    LPNV = Low Precision Noise Variance;
    // Avoid the code-block whose LPN is smaller
 than δ
    if (LPN < δ) {
        continue;
    }
    For each raw-coded MRP {
        PWV = α · LPV + β · LPNV + γ · Layer_No
        Store an index of the pass and the PWV
    }
}
Sort by PWV increasingly
For each ordered pass {
    Embed message bits into bit-stream of the
 pass
}
```

3.3 메시지 추출 절차

삽입된 비밀 메시지의 추출 절차는 코드 블록 데이터를 읽어온 후에 일어난다. 먼저 메시지 삽입 때와 같은 방식으로 LPN, LPNV를 계산하고 JPEG2000 헤더를 통해 각 코드 블록 내의 raw 코딩된 MRP가 속한 레이어 번호를 읽어온 다음 LPV, LPNV와 quality layering 정보를 이용하여 메시지 삽입 절차 때와 같은 방식으로 코드 블록의 순서 가중치(PWV)를 구한다. 이 값에 따라서 삽입 시와 정확히 같은 순서로 코드 블록을 선택하고, 해당 패스를 가져와 비트 스트림에서 메시지를 추출한다.

4. 실험결과

제안한 JPEG2000 스테가노그라피 알고리즘의 실험을 위하여 NRCS[2]에서 제공하는 2024개의 TIFF 이미지와 Kodak[3]에서 제공하는 24개의 이미지를 사용하였다. 모든 이미지들은 512×512 픽셀로 변환된 후, 32×32 픽셀 코드블록/0.5bpp/4-레벨 DWT/4 quality layer의 조건으로 Jasper[4]를 이용하여 lazy-mode로 압축하였다. 코드블록 노이즈 분산을 계산하기 위한 변수들의 계수값은 각각 α=1.0, β=0.1, γ=-10.0으로 결정하였다. 제안한 알고리즘(ME)의 성능을 평가하기 위하여 기존 메시지 삽입 방법(RE, BE)과 비교를 수행하였다. RE[6]는 pseudo-random한 방법으로 각 코드블록 내 비트들을 변경하는 방법이며, BE[4]는 Su가 제안한 backward embedding 방법을 활용한 lazy-mode JPEG2000 스테가노그라피 방법이다. HHT에 기반한 JPEG2000 Lazy-mode 스테가노그라피에 대한 스테거낼리시스 기법[6]은 커버 이미지와 스테고 이미지의 서브밴드 노이즈 분산이 같아야만 한다는 가정 하에서 얻어낸 실험 결과이기 때문에 실용적이지 않다. 따라서 본 논문에서는 메시지 삽입 후에 커버 이미지의 노이즈 분산 시퀀스에 대한 첫 번째와 두 번째 imf (Hilbert transformed IMF)의 진폭(amplitude)이 클수록 탐지될 가능성이 높은 것으로 판단하였다.

먼저 커버 이미지의 노이즈 분산 시퀀스(NV_C)와 스테고 이미지의 노이즈 분산 시퀀스(NV_S)의 차이를 다음의 Mean Square Error (MSE)를 사용해서 분석하였다.

$$\sigma_{ms}^2 = E[|NV_c(x) - NV_s(x)|^2]$$

MSE가 0에 가까울수록 원본 시퀀스와의 차이가 없는 것이며, 클수록 차이가 심해지므로 스테거낼리시스에 의해 탐지될 가능성이 높은 것을 뜻한다. <표 2>에 다양한 메시지 삽입률(ER: embedding ratio)에 대해 커버 이미지와 스테고 이미지의 코드 블록 노이즈 분산에 대해 MSE를 비교한 결과를 정리하였다. 제안한 알고리즘(ME)에 의한 평균과 분산이 가장 작으므로 코드 블록 노이즈 분산의 증가를 파악하여 스테고 여부를 판별하는 스테거낼리시스 방법에 대해 안전하다고 할 수 있다.

〈표 2〉 커버 이미지와 스테고 이미지의 코드블록 노이즈 분산 시퀀스의 MSE

ER	Averages		Variances	
0.1	RE	896.59	RE	15377619.25
	BE	23.79	BE	40140.59
	ME	0.19	ME	0.40
0.2	RE	1395.77	RE	21211166.59
	BE	26.35	BE	41200.59
	ME	0.83	ME	7.93
0.3	RE	1774.66	RE	18223508.98
	BE	29.41	BE	43724.41
	ME	2.10	ME	37.51

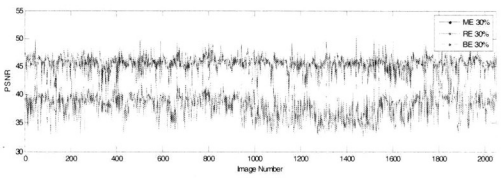
2) http://photogallery.nrcs.usda.gov 에서 이용 가능
3) http://r0k.us/graphics/kodak 에서 이용 가능
4) http://www.ece.uvic.ca/~mdadams/jasper 참고

〈표 3〉 커버 이미지와 스테고 이미지의 특성 벡터의 차이

ER		Averages			Variances	
		1st imf	2nd imf		1st imf	2nd imf
0.1	RE	-0.30	0.95	RE	89.11	475.51
	BE	0.62	0.73	BE	1859.86	1152.57
	ME	-0.05	-0.03	ME	2.35	6.06
0.2	RE	-0.41	0.89	RE	119.32	308.21
	BE	0.51	0.68	BE	1856.56	1190.55
	ME	-0.12	-0.01	ME	5.52	24.03
0.3	RE	-0.41	0.78	RE	84.77	333.21
	BE	0.51	0.75	BE	1868.45	1258.35
	ME	-0.22	-0.02	ME	7.84	31.02

또한, 각 이미지의 다양한 특성으로 인하여 노이즈 분산의 시퀀스에 대한 첫 번째, 두 번째 imf의 진폭(amplitude)은 이미지에 따라 큰 차이를 보인다. 뿐만 아니라, 메시지 삽입 후 imf 진폭의 변화가 항상 증가하는 것이 아니고 때로는 감소하기도 하기 때문에 단순한 증감 여부를 조사하는 것보다 커버 이미지 진폭의 변화량을 가지고 성능을 측정하여야 한다. lazy-mode의 HHT 기반 스테거낼리시스는 메시지 삽입 후에 커버와의 HHT 차이를 이용해 탐지를 시도하기 때문에 만약 HHT 변화를 효과적으로 줄인다면 이 스테거낼리시스를 피할 수 있다. <표 3>에서는 메시지 삽입으로 인하여 두 개의 특성 벡터값이 변화된 차이를 보여주고 있다. RE는 코드 블록 노이즈 시퀀스 전체에 영향을 미치기 때문에 BE보다 분산이 작은 것을 알 수 있다. 특히, 제안한 알고리즘(ME)은 평균과 분산이 RE보다 훨씬 더 작기 때문에 변화를 효과적으로 줄였다고 할 수 있으며, HHT를 기반으로 하는 스테거낼리시스에 안전하다고 할 수 있다.

마지막으로 30%의 메시지를 삽입(ER=0.3)했을 경우 2048 영상에 대하여 화질의 변화를 측정한 결과를 (그림 7)에 나타내었다. 그림에서 보이는 것처럼, 제안한 알고리즘(ME)는 노이즈 분산의 변동폭을 최소화하기 위하여 LPV와 LPNV를 동시에 고려했음에도 불구하고, 화질 저하를 방지하기 위하여 quality layering 정보만을 이용하여 메시지를 삽입한 BE와 비슷한 화질을 유지하고 있으며, RE보다는 우수한 결과를 나타내었다.



(그림 7) 30% 메시지 삽입한 스테고 이미지의 PSNR

5. 결 론

비밀 통신을 위해 고안된 스테가노그라피는 겉으로 보기에 정상적인 커버 오브젝트에 원하는 메시지를 삽입하고 공개된 채널을 통해 전송한다. 스테거낼리시스는 이와 반대로 아무 이상 없어 보이는 오브젝트에서 메시지가 삽입된 흔적, 데이터가 변경된 작은 증거라도 찾으려 한다.

본 논문에서는 널리 쓰이고 있는 DCT 기반의 JPEG 이미지의 뒤를 이어 차세대 영상압축 표준으로 사용될 JPEG2000을 기반으로 하는 스테가노그라피와 스테거낼리시스에 대해 알아보았다. 또한 JPEG2000 도메인을 기반으로 하며 노이즈 분산 시퀀스의 변동을 최소화하는 새로운 스테가노그라피 알고리즘을 제안하였으며, 실험을 통해 제안한 알고리즘의 성능을 테스트하였다. 실험 결과에 따르면 기존의 스테가노그라피 기법보다 우수하며, 최근의 스테거낼리시스에 의해 탐지되지 않는 보다 안전하고 뛰어난 성능을 가지고 있음을 확인할 수 있었다.

JPEG2000은 JPEG보다 우수한 성능을 가지지만, 상대적으로 복잡한 코딩 구조를 가지기 때문에 JPEG2000을 커버 오브젝트로 사용하는 스테가노그라피와 이에 대한 스테거낼리시스의 연구는 아직 시작단계에 있다고 할 수 있다. 본 논문에서 제안한 알고리즘 외에도 다양한 연구 결과가 나올 것으로 기대한다. 향후 연구할 과제는 제안한 스테가노그라피 알고리즘이 다른 종류의 스테거낼리시스의 공격에도 안전한 지를 검증하는 것이다. 기존의 범용적인 스테거낼리시스(Universal Steganalysis) 기법들[11]에 의한 실험결과를 통하여 제안한 스테가노그라피 알고리즘을 보다 견고하고 안전하도록 발전시켜 나가야 한다.

Acknowledgements

This work was supported by the KOSEF grant NRL program funded by the Korea government(MOST) (No. R0A-2007-000-20023-0), NSRI, and the Ministry of Education and Human Resources Development (MOE), the Ministry of Commerce, Industry and Energy (MOCIE), and the Ministry of Labor (MOLAB) through the fostering project of the Lab of Excellency.

참 고 문 헌

[1] A. Skodras, C. Christopoulos, and T. Ebrahimi, "The JPEG2000 Still Image Compression Standard," IEEE Signal Processing Magazine, Vol.18(1), 2001, pp.36-58.

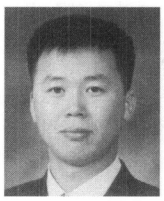
[2] H. Noda, Y. Tsukamizu, and M. Niimi, "JPEG2000 Steganography which Preserves Histograms of DWT Coefficients," IEICE Trans. on Information Systems, Vol. E90-D(4), 783-786.

[3] H. Noda, J. Spaulding, M. N. Shirazi, and E. Kawaguchi, "Application of Bit-Plane Decomposition Steganography to JPEG2000 Encoded Images," IEEE Signal Processing Letters, Vol.9(12), 2002, pp.410-413.

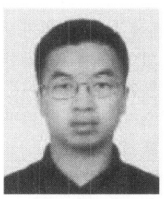
[4] P.-C. Su and C.-C. Jay Juo, "Steganography in JPEG2000 Compressed Images," IEEE Trans. on Consumer Electronics, Vol.49(4), 2003, pp.824-832.
[5] H. Jin, M. Fujiyoshi, Y. Seki, and H. Kiya, "A Data Hiding Method for JPEG 2000 Coded Images Using Modulo Arithmetic," Electronics and Communications in Japan, Vol. 90(7), 2007.
[6] S. Tan, J. Huang, Z. Yang, and Y. Q. Shi, "Steganalysis of JPEG2000 Lazy-Mode Steganography Using the Hilbert-Huang Transform Based Sequential Analysis," Proc. of Int. Conf. on Image Processing, 2006, pp.101-104.
[7] J. Spaulding, H. Noda, M. N. Shirazi, and E. Kawaguchi, "BPCS Steganography using EZW lossy compressed images," Pattern Recognition Letters, Vol.23(13), 2002, pp.1579-1587.
[8] N. E. Huang, Z. Shen, S. R. Long, M. C. Wu, H. H. Shih, Q. Zheng, N.-C. Yen, C. C. Tung, and H. H. Liu, "The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis," Proc. of the Royal Society of London, Vol.454, 1998, pp.903-995.
[9] R. Duda, P. Hart, and D. Stork, "Pattern Classification", 2nd edition. Wiley-Interscience, 2001.
[10] K. Rank, M. Lendl, and R. Unbehauen, "Estimation of image noise variance," IEE Proc. of Vision, Image and Signal Processing, Vol.146(2), 1999, pp.80-84.
[11] M. Kharrazi, H. T. Sencar, and N. Memon, "Performance study of common image steganography and steganalysis techniques," J. of Electronic Imaging, Vol.15(4), 2006.

윤 상 문
e-mail : pisces@mmc.kaist.ac.kr
2006년 서강대학교 컴퓨터공학과(학사)
2008년 한국과학기술원 전자전산학과 전산학전공(공학석사)
2008년~현 재 금융결제원 재직
관심분야 : 스테가노그라피, 스테거낼리시스, 영상처리, 디지털워터마킹 등

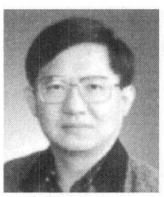
이 해 연
e-mail : haeyeoun.lee@kumoh.ac.kr
1997년 성균관대학교 정보공학과(학사)
1999년 한국과학기술원 전산학과 (공학석사)
2006년 한국과학기술원 전자전산학과 전산학전공 (공학박사)
2001년~2006년 (주)쎄트렉아이 선임연구원
2006년~2007년 코넬대학교 박사후연구원
2008년~현 재 국립금오공과대학교 컴퓨터공학부 교수
관심분야 : 멀티미디어, 영상처리, 콘텐츠보안, 디지털워터마킹 등



주 정 춘
e-mail : jcju@mmc.kaist.ac.kr
1996년 육군사관학교 전산학과(학사)
2002년 국방대학원 전산정보학과 (공학석사)
2007년~현 재 한국과학기술원 전자전산학과 전산학전공 박사과정
관심분야 : 스테가노그라피, 스테거낼리 시스, 정보보안 등



Cong-Nguyen Bui
e-mail : nguyen@mmc.kaist.ac.kr
2002년 베트남 하노이공과대학교(학사)
2005년 한국과학기술원 전자전산학과 전산학전공(공학석사)
2005년~현 재 한국과학기술원 전자전산학과 박사과정
관심분야 : 스테가노그라피, 스테거낼리시스 등



이 흥 규
e-mail : hklee@mmc.kaist.ac.kr
1978년 서울대학교 전자공학과(학사)
1981년 한국과학기술원 전산학과 (공학석사)
1984년 한국과학기술원 전산학과 (공학박사)
1984년~1986년 Univ. of Michigan 연구원
1986년~현 재 한국과학기술원 전자전산학과 교수
1999년~2008년 한국과학재단지정 첨단정보기술연구센터 부소장
2006년~현 재 융합형보안기술연구센터 소장
관심분야 : 정보은닉, 미디어 포렌식, 스테가노그라피