

영상의 화질 개선과 열화측정 시간을 최소화하는 스테가노그래피 방법

최용수*, 김장환**

요약

본 논문에서는 기존의 데이터 은닉 기법들을 개선하는 스테가노그래피 방법을 제시한다. 이 방법은 이미지의 압축 도메인(JPEG)에서 동작한다. 현재 정보은닉 방법의 대부분은 일반적으로 정보를 숨길 계수를 변경한다. 그리고 몇 가지 방법은 매트릭스 인코딩을 포함하는 F5 같은 일반적인 스테가노그래피 방법의 성능을 향상시키기 위해 노력하였다. 이러한 논문들은 압축 도메인 계수에 데이터를 숨길 때 발생하는 왜곡을 감소시키는 목적을 달성하였다. 제안 논문에서는 압축 도메인에서 데이터를 숨기는 동안 양자화 테이블의 효과를 분석 하였다. 결과적으로, 스테가노그래피 기술의 적용에서 발생하는 왜곡을 양자화 테이블의 효율적 이용에 의해 감소시킬 수 있음을 알아냈다. 본 논문에서는 이미지 품질의 관점에서 일부(최대: 약 6.5%) 더 개선된 결과를 제공한다. 제안한 논문에서 개발한 알고리즘은 JPEG 외의 압축영역 정보 은닉 기법들의 성능 개선에 도움을 줄 수 있다.

키워드 : 스테가노그래피, 양자화, 정보 은닉, JPEG 압축, 행렬 인코딩

A Steganography Method Improving Image Quality and Minimizing Image Degradation

YongSoo Choi*, JangHwan Kim**

Abstract

In this paper, we propose a optimized steganography how to improve the image degradation of the existing data hiding techniques. This method operates in the compressed domain(JPEG) of an image. Most of the current information concealment methods generally change the coefficients to hide information. And several methods have tried to improve the performance of a typical steganography method such as F5 including a matrix encoding. Those papers achieved the object of reducing the distortion which is generated as hiding data in coefficients of compressed domain. In the proposed paper we analyzed the effect of the quantization table for hiding the data in the compressed domain. As a result, it found that can decrease the distortion that occur in the application of steganography techniques. This paper provides a little (Maximum: approximately 6.5%) further improved results in terms of image quality in a data hiding on compressed domain. Developed algorithm help improve the data hiding performance of compressed image other than the JPEG.

Keywords : Steganography; Quantization, Data hiding, JPEG compression, Matrix Encoding

1. 도입

※ Corresponding Author : JangHwan Kim

Received : October 10, 2016

Revised : October 25, 2016

Accepted : October 31, 2016

* Division of Liberal Arts & Teaching, Sungkyul Univ.

Tel: +82-10-9131-7383 ,

컴퓨터와 인터넷 환경의 발전에 따라, 텍스트, 이미지, 비디오 같은 많은 중요 정보들이 디지털 소스들로 변환/저장되어 질수 있고, 웹 페이지에

email: ciechoi@sungkyul.ac.kr

** Dept. of MediaSoftware, Sungkyul Univ.

개시되거나 네트워크를 통해서 전송된다. 디지털 정보들은 우리의 정보이용 환경에 공용성과 용이성을 제공해주지만 반대로 악의적인 의도에 의해 오남용(훼손, 변경)될 가능성도 높아지게 된다.

콘텐츠의 보호에 있어 전통적인 방법은 암호화라는 강력한 방법이 있었다. 암호화된 콘텐츠(이미지, 음악, 비디오 등)는 원래의 시청각 형태를 직관적으로 파악하기 어렵도록 원래의 파일포맷과는 다른 형태의 데이터구조로 바뀐다. 하지만 최근의 인터넷 환경에서의 대부분의 정보들은 보거나 듣거나 하는 것이 가능한 멀티미디어 데이터 들이다. 많은 연구자들은 시청각적 현상을 그대로 유지한 채 콘텐츠 보호를 할 수 있는 방법을 찾기 위해 많은 시간을 보냈다.

이러한 목적을 달성하기 위해 20세기 후반부터 많은 학자들이 지각적 정보은닉 방법의 일종으로 디지털 워터 마킹 방법을 개발하기 시작하였다. 디지털 워터마킹은 디지털 콘텐츠의 내용물에 정보(저작권, 저자의 서명, 회사 로고)를 소거하기 어렵도록 삽입하는 기술이다. 디지털 워터마킹의 주요 목적은 콘텐츠에 저작권과 같은 디지털 정보를 원본 콘텐츠의 시각적 품질에 영향을 미치지 않는 범위 내에서 표시하는 방법이다.

정보은닉의 또 다른 방법으로 스테가노그래피 방법이 있다[1, 5]. 이 방법은 정보 은닉의 존재를 숨긴 채 원본 콘텐츠에 저작권과 같은 정보들을 콘텐츠에 삽입하게 된다. 스테가노그래피는 의심의 여지가 없는 커버객체에 정보를 삽입함으로써 비밀통신(메시지 은닉/전송)의 노출이 최소화된다. 이러한 비밀통신은 암호화와 다르게 악의적인 의도를 가진 제3의 관찰자나 공격자에 의한 인지가 쉽지 않으므로 비밀성을 높여주는 효과를 가진다. 스테가노그래피 기술에서의 커버객체는 영상, 오디오, 비디오 그리고 문서 등 대부분의 디지털 미디어를 포함하게 된다[2, 3].

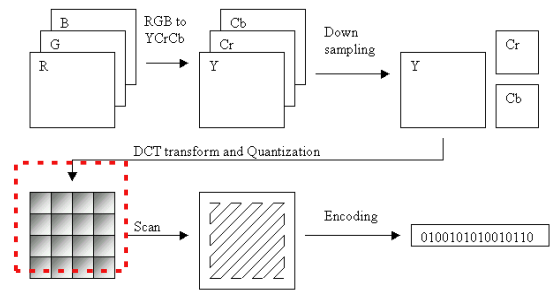
위에서 대표적으로 예를 든 디지털 워터마킹과 스테가노그래피의 근본적 차이는 정보 은닉의 여부에 대한 노출과 은폐이다.

영상을 대상으로 한 초기의 정보 은닉은 압축되지 않는 영역에 대해 이루어지기도 하지만 압축된 영역에서의 은닉이 요구되는 경우가 더 많다. 최근의 미디어 이용 환경을 보면 네트워크의 제한된 대역폭 때문에 파일 또는 멀티미디어 압축을 이용하여 전송량을 줄이고 전송시간은 단

축한다.

정보가 은닉된 콘텐츠를 압축할 경우 은닉 정보의 손실이 발생할 가능성이 있으므로 본 논문에서 사용하는 것과 같이 압축된 영역에 정보를 삽입하는 기술의 필요성이 높아지게 되었고 많은 연구가 이루어진다. 새로운 정보은닉기술의 개발에 있어 은닉 용량을 올리고, 보안성을 높이는 것이 매우 중요한 요구사항이라 할 수 있다.

(그림 1) JPEG 압축과정



(Figure 1) JPEG Compression Process

아래는 지각적 정보은닉기술에서 요구되는 중요한 특성들이다[14].

- 비지각성: 원본과 정보가 삽입된 콘텐츠는 지각적인 차이를 가지지 않아야 한다.
- 강인성: 대부분의 신호처리연산에서 삽입된 정보의 손실이 발생하지 않고 신뢰성을 제공할 수 있어야 한다.
- 은닉용량: 지각적 차이를 보이지 않는 범위 내에서 은닉정보의 양을 최대한 높여야 한다.
- 보안성: 은닉정보의 표시가 제거되지 않거나 은닉여부의 노출이 최소화 되어야 한다.

최근에 개발된 많은 스테가노그래피 방법은 이러한 요구 사항[4,6,7,8,10,11]을 만족시키기 위해 개발되었다. 최신 알고리즘 중 JPEG(Joint Picture Expert Group)영상의 DCT(Discrete Cosine Transform)계수에 정보은닉(삽입) 시 발생하는 열화(반올림 오차)를 고려하여 정보은닉 기법을 설계하는 MME (영: Modified Matrix

Encoding, 즉: 변형된 매트릭스 인코딩) 방법이 있다. 실제로 MME 알고리즘은 이전의 알고리즘 (F5)에 대해 우수한 성능을 나타낸다[8]. 저자의 파일럿 논문[9]에서 양자화 테이블이 가지는 영향력에 대한 타당성을 이미 검증하였으며 본 논문에서는 압축영상에서 동작하는 스테가노그래피 과정에서 발생하는 화질 저하를 최소화하기 위한 여지가 여전히 존재함을 증명하였다.

본 논문은 다음과 같이 네 개의 섹션으로 구성되어 있다. 2장에서는 주파수 영역에서 동작하는 스테가노그래피 기술에 대해 소개한다. 3장에서는 제안하는 MME 방법을 설명하고 4장에서는 실험 및 결과를 보여준다. 마지막으로 5장에서는 논문의 기여도, 실험의 결과에 대한 정리와 결론을 제시한다.

2. 관련 연구

JPEG은 인터넷에 범용적으로 이용되는 이미지 포맷이다. 대부분의 응용 프로그램은 데이터 저장공간의 효율성을 높이기 위해 이와 같은 압축형식(포맷)을 사용한다. 또한 JPEG 파일 형식에서 정보를 삽입하는 많은 스테가노그래피 알고리즘은 (그림 1)에서 빨간색 점선으로 표시된 단계에서 수행된다.

JSteg 알고리즘은 JPEG 계수의 LSB(Least Significant Bit)를 덮어쓰기(Overwrite) 함으로써 0과 1로 구성된 이진 비밀 메시지를 은닉한다. JSteg는 특정한 계수를 만났을 때는 메시지 삽입 동작을 건너뛴다. F3 알고리즘에서는 비밀 메시지 비트와 JPEG 계수의 LSB가 매치될 때 계수의 절댓값을 감소시키는 알고리즘이다. 계수를 감소시켰을 때 0이 되는 계수는 예외적으로 삽입 동작을 중지하고 다음 계수의 은닉 가능성을 고려한다. F4 알고리즘은 F3 알고리즘의 약점을 보완하기 위해 개발되어지고 반전 동작 후에, 계수의 LSB와 비밀 메시지 비트를 일치시키기 위해 비밀 메시지 bit에 따라 음수인 계수는 증가되고 양수인 계수는 감소한다.

F5 알고리즘은 F4 알고리즘에 비해 몇 가지 특징의 향상을 보여준다. F5 알고리즘의 Permutative Staraddling 처리는 지각적인 특성의 개선과 보안성 향상을 위해 채용되어진다. 더

욱이, 메시지 삽입의 효율성을 증가시키기 Matrix Encoding을 포함하였다.

제안하는 변형된 Matrix Encoding의 개선방법은 영상의 압축영역(계수)에 대한 메시지 삽입 이후에도 영상의 화질저하가 최소가 되도록 양자화 오류 예측기법에 의해 메시지삽입을 수행하였다. 위에서 살펴본 대부분의 스테가노그래피 방법들은 히스토그램 분석과 같은 통계적 공격수단에도 검출이 되지 않도록 고안되었다. 각각의 알고리즘들에 대한 영상 화질저하를 평가하기 위해 메시지 은닉된 스테고영상(압축영역)은 공간영역(비 압축 영역)으로 되돌려지고 원본(비 압축)영상과 비교함으로써 압축영역에서의 계수 변환에 의한 열화를 계산해 내는 것이 가능하다.

3. 제안하는 Modified Matrix Encoding의 개선

3.1. JPEG 계수의 정보 은닉[4]

기존의 논문[8]에서 보인 것과 같이, JPEG에 대한 정보 은닉과정에서 발생하는 양자화 오류는 다음과 같이 정의 된다.

$$e(u,v) = f''(u,v)Q(u,v) - F(u,v)$$

여기서, $F(u,v)$ 는 압축영역의 계수이고 $Q(u,v)$ 는 양자화 테이블 이며 $f''(u,v) = Round(F(u,v)/Q(u,v))$ 이며 압축영상의 계수로 저장되는 값을 말한다. 이러한 동작들은 JPEG에서 사용하는 블록의 크기인 8X8 블록 단위로 반복적으로 사용된다.

하지만, JPEG영상에 대한 정보 은닉에서는 반올림 오류(왜곡)외에도 부가적인 왜곡이 발생된다. C' 와 C'' 을 각각 반올림 전후의 DCT계수들의 벡터라고 정의하자.

$$\begin{aligned} C' &= (c'_1, c'_2, \dots, c'_i) \\ C'' &= \delta(C') = (c''_1, c''_2, \dots, c''_i) \\ R &= C'' - C' = (r_1, r_2, \dots, r_i) \end{aligned} \tag{1}$$

위에서 보인 C' 의 LSB들을 변경함으로써 스테고 계수인 S 가 생성되어진다. 즉, S 의 LSB는

은닉정보 비트와 동일해진다. 변형된 matrix encoding에서 삽입 방법의 선택은 반올림(∂) 오류의 양에 따라 선택되어진다.

$$S_i = \begin{cases} -2 & ,if r_i \leq 0 \text{ and } c'_i = -1 \\ \partial(c'_i) + 1, & ,if r_i \leq 0 \text{ and } c'_i \neq -1 \\ 2 & ,if r_i > 0 \text{ and } c'_i = 1 \\ \partial(c'_i) - 1, & ,if r_i > 0 \text{ and } c'_i \neq 1 \end{cases} \quad (2)$$

그러면 삽입에서 발생하는 왜곡은 아래와 같이 계산되어진다.

$$d_i = |S_i - c'_i| \quad (3)$$

$$d_i = \begin{cases} 1 + |r_i|, & ,if c''r_i > 0 \text{ and } c'' = \pm 1 \\ 1 - |r_i|, & ,otherwise \end{cases} \quad (4)$$

결과적으로, C' 비트 하나를 변경할 때 발생하는 부가적인 왜곡의 크기는 다음 식과 같이 계산되어진다.

$$e_i = \begin{cases} 1, & ,if c''r_i > 0 \text{ and } c'' = \pm 1 \\ 1 - 2|r_i|, & ,otherwise \end{cases} \quad (5)$$

실제로, 정보 삽입단계에서 발생하는 전체왜곡(E)를 최소화 하도록 설계되어야 하므로 위의 동작들은 블록의 수만큼 반복 누적되어진다.

3.2. Matrix Coding[6]

Crandall은 메시지 삽입 시 발생하는 비트 변화의 수를 줄이기 위한 효율적 삽입방법을 만들기 위해 Matrix Coding을 제안하였다[12].

Westfeld는 Matrix Coding을 구현하는 F5 알고리즘을 제안하였으며 이 알고리즘에서는 양자화된 값의 반올림 단계 이후에 양자화된 DCT 계수의 LSB 세트를 변경한다[10].

$n = 2^k - 1$ 일 때, notation($1, n, k$)는 계수의 열에서 한 비트를 변경함으로써 k 개의 메시지 비트를 메시지 비트가 길이 n 인 블록으로 삽입됨을 의미한다. C 는 길이가 n 인 블록으로 구성되며 m 은 길이 k 인 블록들로 구성된다. i 번째 메시지 블록 $\{m_{k(i=1)+1}, \dots, m_{ki}\}$ 을 삽입하기 위해 커버블록 $\{c_{n(i=1)+1}, \dots, c_{ni}\}$ 이 사용된다. MB 와 CB 는 각각 메시지 블록과 커버블록이라고 가정한다.

$$b(CB) = \bigoplus_{j=1}^n (cb_j) \cdot j \quad (6)$$

커버블록의 변경 위치 α 를 찾기 위해 아래와 같이 MB 와 CB 에 대한 연산을 수행한다.

$$\alpha = MB \oplus b(CB) \quad (7)$$

만약, $\alpha = 0$ 이라면, 커버블록에는 아무런 변화가 없다. $\alpha \neq 0$ 경우라면, 커버블록의 α 번째 비트가 반전(flipping: 0->1 or 1->0)되어야 한다.

$$SB = \begin{cases} CB & if \alpha = 0 \\ cb_1, \dots, -cb_\alpha, \dots, cb_n & if \alpha \neq 0 \end{cases} \quad (8)$$

디코더 측에서는 동일한 연산에 의해 n 비트 크기의 커버 블록으로부터 k 메시지 비트가 얻어진다.

$$MB = b(SB) \quad (9)$$

3.3. Modified Matrix Encoding[8]

2절에서 n 비트의 LSB 블록에 k 비트를 삽입하기 위해 F5 알고리즘에서 (l, n, k) code를 사용하는 방법을 보였다. Y. Kim 등은 각 커버블록 별로 선택적인 비트 변화의 가능성을 증가시키기 위해 (t, n, k) 코드를 제안하였다.

MME(Modified Matrix Encoding)에서의 연산은 다음과 같다.

1) 삽입부

$t=2$ 인 경우, $(\beta \oplus \gamma = \alpha)$ 를 만족하는 숫자 쌍 (β, γ) 를 찾는다. α 하나에 대해 생성 가능한 위치의 쌍은 $(n-1)/2$ 개가 있다. 우리가 F5에서 사용한 matrix encoding을 사용하여 삽입을 수행한다면 수식 (7)을 통해 α 가 계산가능하고

$$\beta_i \oplus \gamma_i = \alpha, i = 1, 2, \dots, (n-1)/2$$

를 만족하는 위치의 쌍이 아래처럼 구해진다.

$$(\beta_1, \gamma_1), (\beta_2, \gamma_2), \dots, (\beta_{(n-1)/2}, \gamma_{(n-1)/2})$$

주어진 위치 r_α 에서의 삽입 오류는 $e_0 = 1 - 2|r_\alpha|$ 이 된다. (β_i, γ_i) 쌍에 대해 LSB

의 변경으로 발생하는 오류는 다음과 같이 계산이 가능하며 e_i 로 놓는다.

$$e_i = \begin{cases} 2 & \text{if } c''_{\beta_i} r_{\beta_i}, c''_{\gamma_i} r_{\gamma_i} > 0 \\ & \text{and } c''_{\beta_i}, c''_{\gamma_i} = \pm 1 \\ 2 - 2|r_{\gamma_i}| & \text{, if } c_{\beta_i} r_{\beta_i} > 0 \text{ and} \\ & c''_{\beta_i} = \pm 1 \text{ and } c''_{\gamma_i} \neq \pm 1 \\ 2 - 2|r_{\beta_i}| & \text{, if } c''_{\gamma_i} r_{\gamma_i} > 0 \text{ and} \\ & c''_{\gamma_i} = \pm 1 \text{ and } c''_{\beta_i} \neq \pm 1 \\ 2 - 2|r_{\beta_i} + r_{\gamma_i}| & \text{, otherwise} \end{cases}$$

(10)

(β_i, γ_i) 의 쌍에 따라 왜곡의 오류가 틀리므로 최적의 위치쌍을 선택하기 위해 최소 왜곡오류를 다음과 같이 정의할 필요가 있다.

$$\mu = \min_j (e_j), 0 \leq j \leq (n-1)/2$$

결국, 주어진 μ 를 이용하여 SB의 계산이 가능하다.

$$SB = \begin{cases} CB, & \text{if } \alpha = 0 \\ cb_1, \dots, -cb_{\alpha}, \dots, cb_n, & \text{if } \mu = e_0 \\ cb_1, \dots, -cb_{\beta}, \dots, cb_n, & \text{if } \mu = e_i, i = 1, \dots, (n-1)/2 \end{cases}$$

(11)

3.4. 제안하는 Modified Matrix Encoding의 개선 과정

앞의 절들에서 JPEG의 계수들을 변경할 때 양자화 테이블의 영향을 측정하기 위한 수식을 유도하였다. 계수 변경의 영향을 체크하기 위한 실험 과정을 정의하였으며 DCT 계수에 대한 동일한 양의 변경은 양자화 요소들의 제곱을 취한 것과 같은 멱승 오류(PE: Powered Error)를 지속적으로 생성함을 알 수 있었다. 계수 변경의 크기는 항상 1이다. PE는 수식(12)를 따르고 상수 τ 에 의해 계수들을 변경할 때, PE는 수식(14)로 계산이 된다.

$$PE = \sum_{i=1}^m \sum_{j=1}^n |I(i,j) - K(i,j)|^2 = \sum Q_x^2 \quad (12)$$

I 는 비압축된 원본영상이고 K 는 비압축된 스테고 영상이다.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} |I(i,j) - K(i,j)|^2 = \frac{1}{mn} PE$$

(13)

$$PE = \sum_{i=1}^m \sum_{j=1}^n |I(i,j) - K(i,j)|^2 = \sum (\tau Q_x^2) \quad (14)$$

즉, MSE와 PE는 블록의 크기만큼 연산을 반복하는 과정을 최소화한 예측이 가능해진다. 결국 화질의 척도인 PSNR(Peak Signal to Noise Ratio) 값도 낮은 연산량으로 계산하는 것이 가능하다. 이와 같은 사실은 변경되는 계수에 상응하는 양자화 요소가 공간영역의 왜곡에 영향을 미친다는 것을 증명한다.

$$PSNR = 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \quad (15)$$

실제로, modified matrix encoding에 이러한 접근방법을 적용하면, 위치 α 가 있을 때, 대응하는 $PE(=q_0)$ 는 $q_0 = q_{\alpha} 2$ 가 된다. 그리고 최소왜곡 오류는

$$\mu = \min_k (q_{\beta_k}^2 + q_{\gamma_k}^2), 0 \leq k \leq (n-1)/2 \quad (16)$$

이다.

최소왜곡오류를 가지는 위치 쌍의 연산이 가능하므로 다음식과 같은 비트의 반전을 통해 정보 은닉이 수행된다.

$$SB = \begin{cases} CB, & \text{if } \alpha = 0 \\ cb_1, \dots, -cb_{\alpha}, \dots, cb_n, & \text{if } \mu = q_0 \\ cb_1, \dots, -cb_{\beta}, \dots, cb_n, & \text{if } \mu = q_i, i = 1, \dots, (n-1)/2 \end{cases} \quad (17)$$

4. 실험 및 결과

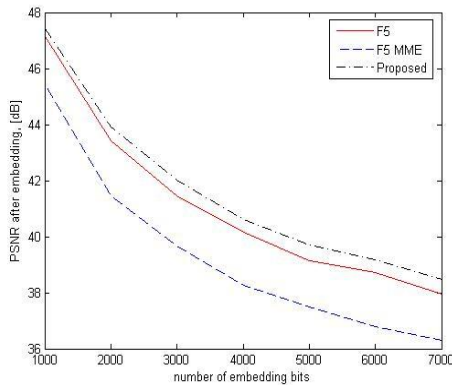
제안된 아이디어를 증명하기 위해, 우리는 MATLAB 프로그램을 사용하여 제안된 알고리즘을 구현하였다. 구현된 알고리즘은 그레이와 컬러 영상들에 적용이 가능하다. 하지만 논문의 실험 결과에서는 그레이 영상[13]에 대해서만 개선가능성을 측정하였다. 샘플이미지로서 Lena를 비롯한 영상처리에서 참조영상으로 많이 사용되는 영상들을 사용하였다. 양자화 스텝에서는 luminance를 위한 표준 양자화 테이블을 사용하였다. 실험결과에 따르면 제안된 알고리즘은 계

수 값의 총 오류와 PSNR의 지표에서 원래의 modified matrix encoding과 F5 modified matrix encoding보다 개선된 결과를 보여주었다.

만약 우리가 계수의 변경에 대한 오류를 고려한다면, modified matrix encoding이 더 나은 성능을 보인다.

반대로, 영상의 화질척도로서 PSNR을 고려한다면, modified matrix encoding이 기존 F5나 제안된 방법보다 화질저하를 더 생성함을 알 수 있다. 결국, F5 modified matrix encoding은 여전히 좋은 알고리즘이다. 반면 제안된 알고리즘을 통해 계수 변경에 따른 오류를 예측함으로써 효과를 개선할 수 있음을 증명하였다.

(그림 2) 데이터 삽입 후의 PSNR 그래프



(Figure 2) Comparison of PSNRs after Data Embedding

<표 1> 데이터 삽입 후의 PSNRs

	1002 bits	2001 bits	3003 bits	4002 bits	5001 bits	6003 bits	7002 bits
F5	47.15	43.42	41.46	40.16	39.13	38.73	37.95
F5 MME	45.46	41.44	39.65	38.25	37.48	36.79	36.31
Proposed	47.46	43.91	42.00	40.63	39.72	39.18	38.46

<Table 1> PSNRs after data embedding

그리고 기존의 F5와 F5 MME 화질대비 개선 효과를 아래표와 같이 비교해 보았다. 데이터 삽입량에 따라 변화하기는 하지만 F5 알고리즘 대비 대체적으로 1% 내외로 개선이 되었다. 하지만 F5 MME 알고리즘 대비 최소 약 4.4~6.5% 정도

의 개선을 보임을 알 수 있었다.

<표 2> 기존의 MME 알고리즘 대비 화질개선 비교

	1002 bits	2001 bits	3003 bits	4002 bits	5001 bits	6003 bits	7002 bits
F5 대비	0.65	1.15	1.33	1.17	1.51	1.16	1.33
F5 MME 대비	4.39	5.96	5.94	6.20	5.96	6.49	5.91

<Table 2> PSNR Comparisons against F5 and F5 MME

5. 결론

제안된 방법에서는 높은 영상 화질을 보장하는 스테고(정보은닉을 포함하는) 객체를 생성 방법(스테가노그래피)을 제안하였다. JPEG과 같은 압축영역에 데이터를 은닉할 때, 대응(변경되는 DCT계수에 대응하는)하는 양자화 요소의 효과를 고려하는 것이 계수의 변경에 의해 발생하는 오류의 양을 고려할 때 보다 높은 화질을 유지할 수 있음을 보여주었다. 본 논문에서는 JPEG의 DCT계수에서 동작하는 정보은닉 알고리즘을 목표로 하였으며 동종의 알고리즘에서 중요한 기준이 되는 화질보장의 방향성을 제시하였다.

우리가 정보 은닉 방법에서 영상의 화질을 보존할 필요가 있다면, 계수의 변형에 따른 오류를 최소화하기 보다는 작은 양자화 요소를 가진 계수를 선택하는 것이 더 중요함을 증명하였다. 추가적으로, 이러한 사실은 정보은닉 처리시간을 줄이는데도 기여를 하였음을 알 수 있다. 현재까지는 영상의 화질저하를 측정하기 위하여 PSNR을 계산하였다. 하지만, PSNR은 데이터 삽입 과정에서 사용하는 대응하는 양자화 요소의 크기로 추정 가능함을 논문에서 밝혔고 왜곡측정의 시간 또한 매우 획기적으로 줄일 수 있었다.

References

[1] George Berg, Ian Davidson, Ming-Yuan Duan and Goutam Paul, "Searching For Hidden Message: Automatic Detection of Steganography," American Association of Artificial Intelligence, pp.51-56, 2003

- [2] J. Fridrich, M. Goljan and D. Hoge, "Attacking the OutGuess," Proc. of the ACM Workshop on Multimedia and Security. Juan-les-Pins, France, December 6, 2002.
- [3] J. Fridrich, M. Goljan and D. Hoge, "New Methodology for Breaking Steganographic Techniques for JPEGs," Proc. SPIE Electronic Imaging, Santa Clara, CA, USA, pp.143-155, Jan 2003.
- [4] Andreas Westfeld, "F5-A Steganographic Algorithm: High Capacity Despite Better Steganalysis," 4th Information Hiding International Workshop, Pittsburgh, USA, April 2001.
- [5] Bret Dunber, "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment.", SANS Institute, January 2002.
- [6] J. Fridrich and D. Soukal, "Matrix Embedding for Large Payload," IEEE Tran. on Information Forensics and Security. Vol 1, pp.390-295, September 2006.
- [7] M. Chen, R. Zhang, X. Niu and Y. Yang, "Analysis of Current Steganography Tools: Classification & Features," Proc. of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Pasadena, CA, USA, December 2006.
- [8] Y.H. Kim, Z. Duric and D. Richards, "Modified Matrix Encoding Technique for Minimal Distortion Steganography," Proc. of Information Hiding 2006, pp.314-327, 2007
- [9] Y.S. Choi, H.J. Kim, and C.M.Park, "The Influence of Quantization Table in view of Information Hiding Techniques Modifying Coefficients in Frequency Domain," Journal of IEEK, Vol.46, pp.56-63, January 2009.
- [10] Andreas Westfeld: The Steganographic Algorithm F5, 1999, <http://www.wwrn.inf.tu-dresden.de/~westfeld/f5.html>
- [11] Derek Upham: Jsteg, 1997, e.g. <http://www.tiac.net/users/korejwa/jsteg.htm>
- [12] Crandall, R.: Some Notes on Steganography. Posted on Steganography Mailing List <http://os.inf.tu-dresden.de/westfeld/crandall.pdf>, 1998
- [13] The USC-SIPI Image Database, <http://sipi.usc.edu/database/>
- [14] H. Y. Hwang and H. J. Kim "Reversible Watermarking for Audio Using Recompression Method," J. of Digital Contents Society, Vol. 14, No. 2, pp. 199-206, 2013

최 용 수



1998년 강원대학교
제어계측공학과 공학사

2000년 강원대학교
제어계측공학과 공학석사

2006년 강원대학교
제어계측공학과 공학박사

2006년~2007년 연세대학교 첨단융합건설연구단 연구교수

2007년~2013년 고려대학교 정보보호대학원 연구교수

2013년~현재 성결대학교 교양교직부 (멀티미디어) 조교수

관심분야 : Multimedia Hashing, Information Hiding, Watermarking, Steganography, Image Forensics, Forgery Detection 등

김 장 환



1980년: 서울대학교 (공학사)

1997년: KAIST (공학석사)

2003년: 충북대학교 (공학박사)

2005년~현재 성결대학교 교수

관심분야: 데이터베이스, 영상처리, 인공지능