논문 2010-47CI-6-10

액자와 콜라주를 이용한 주파수영역 기반 스테가노그래피

(A Frequency Domain based Steganography using Image Frame and Collage)

윤 은 준*, 안 해 순**, 부 기 동***, 유 기 영****

(Eun-Jun Yoon, Hae-Soon Ahn, Ki-Dong Bu, and Kee-Young Yoo)

요 약

본 논문에서는 디지털 커뮤니티 환경에서 사용자의 디지털 컨텐츠에 대한 저작권을 보호하며, 비밀 정보 교환을 안전하게 수행할 수 있는, 액자와 콜라주를 이용한 주파수영역 기반의 새로운 스테가노그래피 기법을 제안한다. 제안한 기법은 사용자가 다양한 액자와 콜라주를 이용하여 원본 사진을 꾸밀 때 해당 액자와 콜라주에 대한 주파수영역에 저작권과 관련된 정보 또는 비밀 정보를 숨길 수 있게 하였다. 제안한 기법의 장점은 액자를 포함한 콜라주의 개수를 조절하여 숨기고자 하는 정보의 량을 자유롭게 조절할 수 있으며, 다양한 이미지 왜곡 공격들에도 안전하며, 높은 PSNR을 유지할 수 있다. 따라서 제안한 기법은 디지털 저작권 관리, 비밀 메시지 통신, 디지털 워터마킹과 같은 다양한 멀티미디어 보안 분야에 실용적으로 적용되어질 수 있다.

Abstract

This paper proposes a new steganography scheme based on frequency domain using various image frames and collages that can protect the copyright of digital contents for users and securely perform to exchange the security information in the digital communication environments. The main idea of our proposed scheme is that the security informations related its copyright embed into the frequency domain of the image frame and collages when a user decorates the original image by using various image frames and collages. The strengths of our proposed scheme are as follows: (1) It allows to freely control the quantity of embedded information by changing the number of image frames and collages. (2) It is secure to variety image distortion attacks. (3) It maintains high PSNR(Peak Signal to Noise Ratio). As a result, the proposed steganography scheme can be used practically diverse multimedia security fields such as digital copyright protect, secure message communication and digital watermarking.

Keywords : Steganography, Information hiding, Digital watermarking, Image frame, Collage, Multimedia security

Ⅰ. 서 론

2001년 빈라덴의 9·11 연쇄 테러사건으로 인해 주목받게 된 스테가노그래피(Steganography)는 전달하려는 기밀 정보를 이미지 파일이나 MP3 파일 등 멀티미디어 데이터속에 비밀 메세지를 숨기는 기술이다[1~3]. 최근 애플사는 아이튠즈(iTunes)에서 구매한 음원의 불법복제를 막기 위해 사용한 DRM 기술을 포기한 대신에 스테가노그래피 기술을 사용하여 MP3 자체에 구매자의 이름, 계정 이름, 구입날짜, 구매 경로 등의 정보를 숨길

* 정회원, 경북대학교 전자전기컴퓨터학부
(School of Electrical Engineering and Computer Science, Kyungpook National University)
** 정회원, 대구대학교 교양대학
(College of General Education, Daegu University)
*** 정회원, 경일대학교 컴퓨터공학부
(School of Computer Engineering, Kyungil University)
**** 정회원-교신저자, 경북대학교 IT대학 컴퓨터학부
(School of Computer Science and Engineering, Kyungpook National University)
접수일자: 2010년7월22일, 수정완료일: 2010년10월25일

때 사용하였으며, 후지쯔사는 일본 최대 이동통신 사업자인 NTT 도코모와 기술제휴를 통해 일본 내 관광지에서 제공하는 관광정보를 전달하는 수단으로 스테가노그래피를 이용하고 있다고 한다[4].

최근 고급 디지털 카메라의 대중화로 개인이 직접 찍은 사진을 포토샵, 알씨와 같은 사진 편집 및 보정 프로그램들을 이용하여 액자(Frame) 및 콜라주(Collage) 등을 합성하여 다양한 형태로 사진을 예쁘게 꾸며서 디시인사이드(Digital camera inside)와 같은 디지털 카메라 전문 컨텐츠 사이트로 업로드하여 높은 로열티 등의 새로운 부가가치를 창출하고 있다[5].

본 논문에서는 위와 같은 디지털 커뮤니티 환경에서 사용자의 디지털 컨텐츠에 대한 저작권을 보호하며 비밀 정보 교환을 안전하게 수행할 수 있는 액자와 콜라주를 이용한 주파수영역 기반의 새로운 스테가노그래피 기법을 제안한다. 원본 이미지 전체를 사용하는 기존의 방법들[3~13]과 비교하여, 제안한 기법은 사용자가 다양한 액자와 콜라주를 자유롭게 선택하여 원본 사진을 꾸밀 때, 해당 액자와 콜라주에 대한 주파수영역에 저작권과 관련된 정보 또는 비밀 정보를 숨길 수 있게 하였다. 제안한 방법은 기존에 고려되지 않은 독창적인 방법으로 영상의 어느 부분에 기밀 정보가 은닉되었는지를 공격자가 쉽게 인지하지 못하게 하는 스테가노그래피의 목적에 아주 부합한다고 할 수 있다.

제안한 액자와 콜라주를 이용한 주파수영역 기반 스테가노그래피 기법은 다음과 같은 장점들을 가진다.

(1) 액자와 콜라주를 이용한 새로운 스테가노그래피 기법으로 현대 인터넷 환경에 아주 적합하다.
(2) 공간영역이 아닌 Haar Wavelet Transform 기반 주파수영역[6]에 원하는 정보를 숨김으로 이미지 왜곡 등과 같은 공격에 대해서도 견고하다.
(3) 스테고(Stego)된 영상이 원본 영상과 비교하여 이미지 왜곡율이 낮아 높은 PSNR(Peak Signal to Noise Ratio)을 유지할 수 있다.
(4) 콜라주의 개수를 조절하여 숨기고자 하는 정보의 량을 자유롭게 조절할 수 있다.
(5) 기밀 메시지에 대한 은닉(Embedding)과 추출(Extracting) 알고리즘이 간단하여 디지털 저작권 관리, 비밀 메시지 통신, 디지털 워터마킹과 같은 다양한 멀티미디어 보안 분야에 실용적으로 적용되어질 수 있다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 관련연구로 Haar Wavelet Transform 주파수영역 변환 기법과 Modulus Function 은닉 및 추출 알고리즘을 소개한다. Ⅲ장에서 액자와 콜라주를 이용한 주파수영역 기반 스테가노그래피 스킴을 제안하며, Ⅳ장에서 그 실험 결과를 분석한다. 마지막으로 Ⅴ장에서 결론을 도출한다.

Ⅱ. 관련 연구

본 장에서는 관련연구로 제안한 방법에 적용되는 Haar Wavelet Transform 주파수영역 변환 기법[6]과 Modulus Function 은닉 및 추출 알고리즘[7~8]에 관해 간단히 설명한다.

1. Haar Wavelet Transform

Haar Wavelet Transform 주파수영역 변환 기법은 그림 1과 같이 공간영역 상의 이미지 I를 수식(1)을 이용하여 수평 방향 변형(Horizontal transform)을 수행한 결과에 다시 수식(1)을 이용하여 수직 방향 변형(Vertical transform)을 수행한 n-레벨 주파수영역으로 변환하여 주는 기법이다.

$$L = \left\lfloor \frac{x+y}{2} \right\rfloor, H = x - y \tag{1}$$

여기에서 x와 y는 인접한 두 픽셀 값을 의미하며 L과 H는 저주파 필터(Low-pass filter)와 고주파 필터(High-pass filter)를 각각 의미한다. 그림 1은 Lena 이미지에 대한 1-레벨 Haar Wavelet Transform 주파수영역 변환 결과를 보여준다.

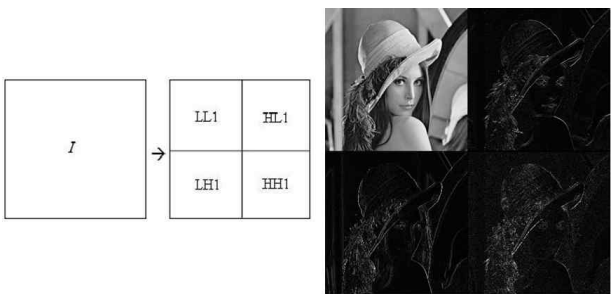


그림 1. Haar 웨이블릿 변환
Fig. 1. Haar Wavelet Transform.

2. Modulus Function 알고리즘

Modulus Function 은닉 및 추출 알고리즘은 다음과 같이 동작한다.

은닉 알고리즘:

① k 종류의 심볼들을 비밀 정보로 사용한다.

② 숨겨져야 되는 비밀 정보를 의미하는 디지털 시스템을 $\{0,1,2,...,k-1\}$로 둔다.

③ 비밀 데이터의 i번째 디지트 $x_i(0 \le x_i < k)$가 커버 이미지내의 그레이 값인 y_i 픽셀 내에 숨겨진다고 가정한다.

④ 아래 수식 (2)와 (3)의 결과 값인 b_i와 d_i를 각각 구한다.

$$b_i = \mathrm{mod}(y_i, k) \tag{2}$$

$$d_i = x_i - b_i \tag{3}$$

⑤ d_i와 k를 이용하여 아래 수식 (4)의 규칙을 기반으로 d_i^*를 구한다.

$$d_i^* = \begin{cases} d_i, & \mathrm{if}(-\left\lfloor \frac{k-1}{2} \right\rfloor \le d_i \le \left\lceil \frac{k-1}{2} \right\rceil) \\ d_i + k, & \mathrm{if}(-k+1 \le d_i < \left\lfloor \frac{k-1}{2} \right\rfloor) \\ d_i - k, & \mathrm{if}(\left\lceil \frac{k-1}{2} \right\rceil < d_i < k) \end{cases} \tag{4}$$

⑥ 아래 수식 (5)를 이용하여 새로운 그레이 값인 y_i^*를 구한다.

$$y_i^* = y_i + d_i^* \tag{5}$$

⑦ 만약 위 수식 (5)의 결과 값인 y_i^*가 [0, 255]의 범위를 벗어나면 아래 수식 (6)을 이용하여 값을 조절하여 준다.

$$y_i^* = \begin{cases} y_i + d_i^* + k, \mathrm{if}(y_i + d_i^* < 0) \\ y_i + d_i^* - k, \mathrm{if}(y_i + d_i^* > 255) \end{cases} \tag{6}$$

추출 알고리즘:

아래 수식 (7)을 이용하여 스테고 된 이미지로부터 비밀 데이터 디지트 값인 x_i를 구한다.

$$x_i = \mathrm{mod}(y_i^*, k) \tag{7}$$

Ⅲ. 제안한 스테가노그래피 스킴

본 장에서는 제안하는 액자와 콜라주를 이용한 주파수영역 기반 스테가노그래피 스킴을 설명한다. 제안한 스킴은 그림 2의 은닉(Embedding) 단계와 그림 3의 추출(Extracting) 단계의 두 알고리즘으로 구성된다.

1. 은닉(Embedding) 단계

제안하는 은닉 알고리즘은 다음의 8단계로 수행된다.

단계 1. 액자와 콜라주를 이용하여 꾸미고자 하는 커버 이미지(Cover image) I를 가져온다.

단계 2. 커버 이미지 I에 다양한 액자와 콜라주를 이용하여 자유롭게 꾸민 콜라주된 이미지 CI를 완성한다. 이때, 삽입된 액자와 콜라주의 위치를 저장한다.

단계 3. 콜라주된 이미지 CI로부터 단계 2에서 저장한 삽입된 액자의 콜라주의 위치 정보를 이용하여 커버 이미지 공간이 포함된 사각형 형태의 액자와 콜라주를 분리 추출한다. 이때, 액자와 콜라주가 추출된 콜라주된 이미지 CI의 위치정보를 저장한다.

단계 4. 저작권 정보 등 비밀 정보를 담고 있는 숨기고자 하는 비밀 이미지 SI를 가져온다.

단계 5. 분리 추출한 사각형 형태의 액자와 콜라주 각각에 대해 위 Ⅱ.1에서 소개한 1-레벨 Haar Wavelet Transform을 수행한다.

단계 6. 위 단계 5의 결과로 생성된 주파수영역 기반 액자와 콜라주에 위 Ⅱ.2에서 소개한 Modulus Function 은닉 알고리즘을 적용하여 위 단계 4의 비밀 이미지 SI를 숨긴다.

단계 7. 위 단계 6의 결과로 생성된 액자와 콜라주 각각에 대해 1-레벨 Inverse Haar Wavelet Transform을 수행하여 공간영역 기반의 액자와 콜라주를 얻는다.

단계 8. 위 단계 3에서 저장한 액자와 콜라주가 추출된 콜라주된 이미지 CI의 위치정보를 이용하여 비밀 이미지 SI를 담고 있는 단계 7의 액자와 콜라주를 제자리에 삽입하여 최종 스테고 된 이미지(Stego image) FSI를 얻는다. 이때, 액자와 콜라주가 삽입된 위치정보는 공유비밀키로 안전하게 보관한다.

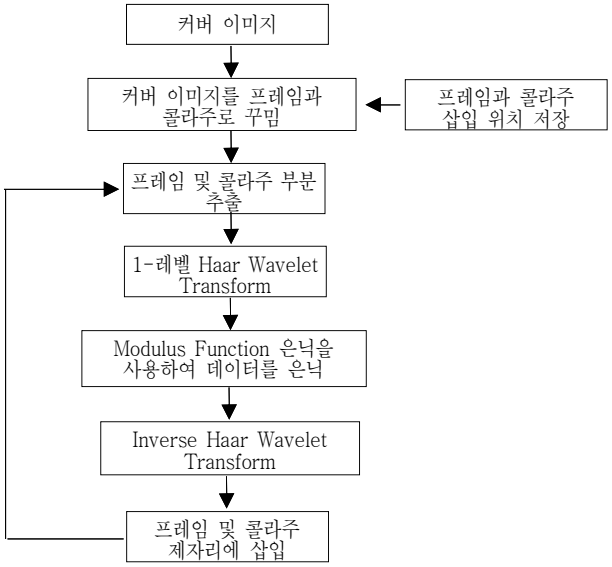


그림 2. 제안한 은닉 단계
Fig. 2. Proposed embedding phase.

2. 추출(Extracting) 단계

제안하는 추출 알고리즘은 다음의 5단계로 수행된다.

단계 1. 제안한 은닉단계로부터 얻어진 스테고 된 이미지 FSI를 가져온다.

단계 2. 액자와 콜라주가 삽입된 위치정보인 공유비밀키를 이용하여 스테고 된 이미지 FSI로부터 액자와 콜라주 부분을 추출한다.

단계 3. 분리 추출한 사각형 형태의 액자와 콜라주 각각에 대해 1-레벨 Haar Wavelet Transform을 수행한다.

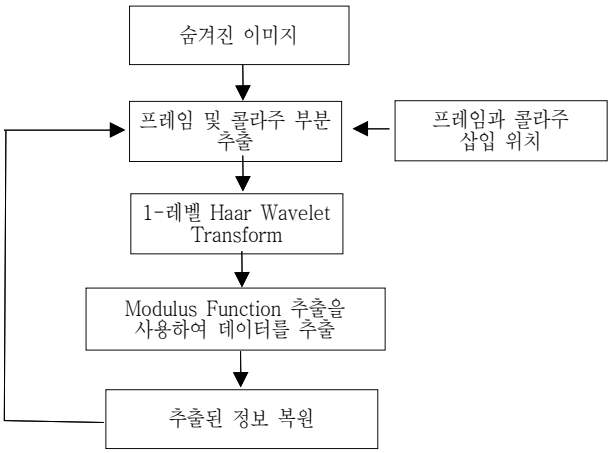


그림 3. 제안한 추출 단계
Fig. 3. Proposed extracting phase.

단계 4. 위 단계 3의 결과로 생성된 주파수영역 기반 액자와 콜라주에 위 II.2에서 소개한 Modulus Function 추출 알고리즘을 적용하여 모든 숨겨진 비밀 값을 구한다.

단계 5. 위 단계 4에서 추출된 비밀 값을 이용하여 비밀 이미지 SI를 복원한다.

Ⅳ. 실험 결과

본 장에서는 제안하는 액자와 콜라주를 이용한 주파수영역 기반 스테가노그래피 스킴의 실험 결과들을 살펴보며 이를 분석한다. 본 실험은 Pentium 4 CPU 2.80GHz 컴퓨터 환경에서 개발 툴은 Matlab 7.0으로 구현하였다.

1. 제안한 스킴 구현 결과

그림 4와 그림 5는 (a)의 512×512 크기의 커버 이미지에 액자와 다양한 코믹 관련 콜라주들을 이용하여 (c)의 190×190 크기의 비밀 심볼과 비밀 이미지를 제안

(a) (b) (c)

(a) 커버 이미지 (512×512)
(b) 스테고 된 이미지 (544×576)
(c) 추출된 비밀 심볼 (190×190)

그림 4. Woman 이미지에 비밀 심볼 은닉
Fig. 4. Hiding Secret Symbol into Woman Image.

(a) (b) (c)

(a) 커버 이미지 (512×512)
(b) 스테고 된 이미지 (544×576)
(c) 추출된 비밀 이미지 (190×190)

그림 5. Woman 이미지에 비밀 이미지 은닉
Fig. 5. Hiding Secret Image into Woman Image.

한 은닉 알고리즘을 적용하여 (b)와 같이 544×576 크기의 스테고 된 이미지를 생성하였으며, (b)로부터 제안한 추출 알고리즘을 적용하여 (c)의 비밀 심볼을 완벽하게 복원함을 각각 보여준다.

2. PSNR을 이용한 이미지 노이즈 측정

본 논문에서는 원본 이진 커버 이미지(I)와 스테고 된 이미지(FSI)의 이미지의 픽셀 값 차이, 즉, 노이즈를 측정하기 위해 PSNR(Peak Signal To Noise Ratio)을 사용하였다[14~18]. PSNR은 두 이미지의 노이즈 차이를 사람이 알 수 있는 측정치로 표현한 것으로, PSNR을 구할 때, M×N 크기의 두 이미지 사이의 차이를 누적하는 MSE(Mean Squared Error)를 통하여 쉽게 계산할 수 있다. MSE와 PSNR은 수식 (8)과 (9)로 각각 표현되어 진다.

$$MSE = \frac{1}{MN}\sum_{1=0}^{M-1}\sum_{1=0}^{N-1}(|I(i,j) - FSI(i,j)|)^2 \quad (8)$$

$$PSNR = 10 \times \log_{10}\left(\frac{MAX_C^2}{MSE}\right) \quad (9)$$

표 1은 위 그림 4의 (b) 스테고 된 이미지에 보여지는 모든 액자와 콜라주에 LSB 2bit와 3bit에 각각 제안한 은닉 알고리즘을 적용한 결과에 대한 최대 데이터 은닉 용량과 원본 이미지에 대비 스테고 된 이미지와 비교한 PSNR 결과를 보여준다. 결과로써 제안한 방법은 숨기는 데이터 용량이 많더라도 이미지 왜곡을 최소화하여 높은 PSNR을 유지할 수 있다.

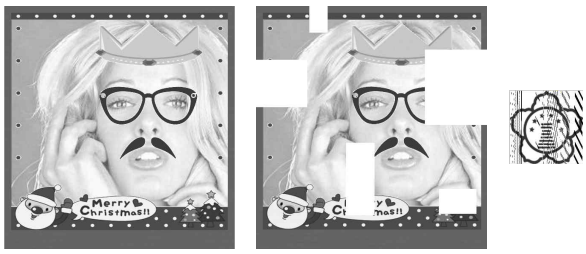
표 1. 데이터 은닉 용량과 PSNR
Table 1. Data hiding capacity and PSNR/

	LSB 2Bit 기반 Modulus Function 기법 활용	LSB 3Bit 기반 Modulus Function 기법 활용
데이터 은닉 용량	38,208 Byte	57,311 Byte
PSNR	43.8283	38.3665

3. 다양한 공격들에 대한 실험 결과

그림 6과 그림 7은 (a)의 544×576 크기의 스테고 된 이미지에 (b)와 같이 자르기 공격을 수행하였을 때도 (c)의 190×190 크기의 비밀 심볼과 이미지가 제안한 추출 알고리즘에 의해 저작권을 보호할 수 있는 수준의 비밀 심볼과 비밀 이미지로의 복원력을 가짐을 각각 보여준다.

그림 8, 그림 9, 그림 10은 (a)의 544×576 크기의 스테고 된 이미지에 (b)와 같이 각각 이미지 밝음, 어둠, 반전 공격 등을 수행하였을 때도 (c)의 190×190 크기의 비밀 심볼과 이미지가 제안한 추출 알고리즘에 의해 완벽하게 저작권을 보호할 수 있을 정도로 비밀 심볼과 비밀 이미지가 복원됨을 각각 보여준다.



(a) (b) (c)

(a) 스테고 된 이미지 (544×576)
(b) 자르기 공격 된 이미지 (544×576)
(c) 추출된 비밀 심볼 (190×190)

그림 6. 자르기에 공격 대한 실험 결과-1
Fig. 6. Experimental results of cutting attack-1.

(a) (b) (c)

(a) 스테고 된 이미지 (544×576)
(b) 자르기 공격 된 이미지 (544×576)
(c) 추출된 비밀 이미지 (190×190)

그림 7. 자르기 공격에 대한 실험 결과-2
Fig. 7. Experimental results of cutting attack-2.

(a) (b) (c)

(a) 스테고 된 이미지 (544×576)
(b) 밝기 공격 된 이미지 (544×576)
(c) 추출된 비밀 심볼 (190×190)

그림 8. 밝음 공격에 대한 실험 결과
Fig. 8. Experimental result of brightness attack.

(a) (b) (c)

(a) 스테고 된 이미지 (544×576)
(b) 어둡기 공격 된 이미지 (544×576)
(c) 추출된 비밀 이미지 (190×190)

그림 9. 어둠 공격에 대한 실험 결과
Fig. 9. Experimental results of darkness attack.

(a) (b) (c)

(a) 스테고 된 이미지 (544×576)
(b) 반전 공격 된 이미지 (544×576)
(c) 추출된 비밀 이미지 (190×190)

그림 10. 반전 공격에 대한 실험 결과
Fig. 10. Experimental result of invert attack.

V. 결론 및 향후연구

본 논문에서는 디지털 커뮤니티 환경에서 사용자의 디지털 컨텐츠에 대한 저작권을 보호하며 비밀 정보 교환을 안전하게 수행할 수 있는 액자와 콜라주를 이용한 주파수영역 기반의 새로운 스테가노그래피 기법을 제안하였다. 제안한 기법은 사용자가 다양한 액자와 콜라주를 이용하여 원본 사진을 꾸밀 때 해당 액자와 콜라주에 대한 Haar Wavelet Transform 주파수영역 변환 기법을 적용한 주파수영역에 저작권과 관련된 정보 또는 비밀 정보를 Modulus Function 은닉 및 추출 알고리즘을 적용하였다. 결론적으로 제안한 기법은 기존에 연구되지 않은 액자와 콜라주를 이용한 새로운 스테가노그래피 기법으로 현대 인터넷 환경에 아주 적합할 뿐만 아니라, 숨기고자 하는 정보의 량을 자유롭게 조절할 수 있으며, 이미지 왜곡과 같은 공격에 대해서도 견고하고 높은 PSNR을 보장한다. 이에 디지털 저작권 관리, 비밀 메시지 통신, 디지털 워터마킹과 같은 다양한 멀티미디어 보안 분야에 실용적으로 적용되어질 수 있을 것으로 기대한다.

향후 연구로는 SF 영화에서 활용되어지는 3차원 동영상 합성 등에 제안한 기법을 적용하여 안전한 저작권 보호 등을 제공할 수 있도록 응용 가능한 방법을 개발하는 데 목적을 둔다.

참 고 문 헌

[1] K. Curran, K. Bailey, “An Evaluation of Image based Steganography Method,” International Journal of digital Evidence, Vol. 2, pp. 1-40, 2003.

[2] H. Yuan, X.P. Zhang, “Multiscale Fragile Watermarking based on the Gaussian Mixture Model,” IEEE Trans. on Image Processing, Vol. 15, No. 8, pp. 3189-3200, 2006.

[3] J.L. Dugelay, S. Roche, C. Rey et al. “Still-image Watermarking Robust to Local Geometric Distortions,” IEEE Trans. on Image Processing, Vol. 15, No. 7, pp. 2831-2842, 2006.

[4] A. Rocha, S. Goldenstein, “Steganography and Steganalysis in Digital Multimedia: Hype or Hallelujah?,” Journal of Theoretical and Applied Computing, Vol. 15, pp. 83-110, 2008.

[5] S.M. Shahreza, S.S. Shahreza, “Collage Steganography,” Proceedings of the 5th IEEE/ACIS International Conference on Computer and Information Science, pp. 316-321, 2006.

[6] M. Antonini, M. Barlaud, P. Mathieu, and I. Daubechies, “Image Coding using Wavelet Transform,” IEEE Trans. Image Processing, Vol. 1, pp. 205-221, 1992.

[7] C.C. Thien, J.C. Lin, “A Simple and High-hiding Capacity Method for Hiding Digit-by-digit Data in Images based on Modulus Function,” Pattern Recognition, Vol. 36, No. 10, pp. 2875-2881, 2003.

[8] K. Zhiwei, L. Jing, H. Yigang, “Steganography based on Wavelet Transform and Modulus Function,” Journal of Systems Engineering and Electronics, Vol. 36, No. 18, No. 3, 2007, pp. 628-632.

[9] 김천식, 윤은준, 홍유식, 김형중, “Secret Sharing Scheme using Gray Code based on Steganography,” 전자공학회논문지, 제46권 CI편, 제1호, 96~102쪽, 2009년 1월.

[10] 최용수, 김형중, 박춘명, “주파수 영역 계수 변경을 이용한 정보은닉기술에서의 양자화 테이블의 영향

력," 전자공학회논문지, 제46권 CI편, 제1호, 56~63쪽, 2009년 1월.
[11] 최용수, 김형중, 박춘명, "데이터 은닉 기법을 이용한 BTC(Block Truncation Coding) 영상의 압축," 전자공학회논문지, 제47권 CI편, 제1호, 51~57쪽, 2010년 1월.
[12] 정철호, 엄일규, 김유신, "웨이블릿 영역에서 히스토그램 수정을 이용한 무손실 정보은닉," 전자공학회논문지, 제43권 SP편, 제4호, 27~36쪽, 2006년 7월.
[13] 김천식, 조민호, 홍유식, 박현숙, "ODBTC를 위한 EMD 기법에 기반한 데이터 은닉," 전자공학회논문지, 제46권 CI편, 제6호, 27~34쪽, 2009년 11월.
[14] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for Data Hiding," IBM Systems Journal , Vol,. 35, No. 3-4, pp. 313-316, 1996.
[15] W. Bender, F.J. Paiz, W. Butera, S. Pogreb, D. Gruhl, R. Hwang, "Applications for Data Hiding," IBM Systems Journal Vol. 39, No. 3-4, pp. 547~568, 2000.
[16] E. Adelson, "Digital Signal Encoding and Decoding Apparatus," US Patent, No. 4939515, 1990.
[17] L.F. Turner, "Digital Data Security System," Patent IPN WO 89/08915, 1989.
[18] R.Z. Wang, C.F. Lin, J.C. Lin, "Image Hiding by Optimal LSB Substitution and Genetic Algorithm," Pattern Recognition, Vol. 34, No. 3, pp. 671-683, 2001.

저 자 소 개

윤 은 준(정회원)
1995년 경일대학교 졸업 (공학사)
2003년 경일대학교 컴퓨터공학과 (공학석사)
2007년 경북대학교 컴퓨터공학과 (공학박사)
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2009년~현재 경북대학교 대학원 전자전기컴퓨터학부 계약교수
2010년~현재 대한전자공학회 컴퓨터소사이어티 멀티미디어분과 위원장
<주관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜>

부 기 동(정회원)
1984년 경북대학교 전자공학과 (공학사)
1988년 경북대학교 전자공학과 (공학석사)
1996년 경북대학교 전자공학과 (공학박사)
1983년~1985년 포항종합제철 시스템개발실
2001년~2002년 일본 게이오대학 방문교수
1988년~현재 경일대학교 컴퓨터공학부 교수
<주관심분야: 데이터베이스, GIS, 시멘틱 웹, 데이터베이스 보안, RFID 보안>

안 해 순(정회원)
1996년 경일대학교 컴퓨터공학과 (공학사)
2001년 경일대학교 컴퓨터공학과 (공학석사)
2009년 대구대학교 컴퓨터정보공학과(박사수료)
2004년~2008년 경일대학교 컴퓨터공학부 전임강사
2008년~현재 대구대학교 교양대학 초빙교수
<주관심분야: 데이터베이스, 정보보안, 정보검색, 모바일 GIS, 데이터베이스 보안, RFID 보안>

유 기 영(정회원)
1976년 경북대학교 수학과 (이학사)
1978년 한국 과학 기술원 컴퓨터공학과 (공학석사)
1992년 미국 뉴욕 Rensselaer Polytechnic Institute 컴퓨터 과학과 (이학박사)
1978년~현재 경북대학교 컴퓨터공학과 교수
1997년~1998년 한국정보과학회 영남지부장
1999년~현재 한국정보과학회 이사
2006년~현재 제12대 한국정보보호학회 부회장
<주관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜>