

논문 2009-5-22

고용량 스테가노그래픽 방법 연구

High Capacity Steganographic Method

김기종*, 정기현*, 유기영**

Ki-Jong Kim, Ki-Hyun Jung, Kee-Young Yoo

요 약 본 논문은 이미지 픽셀의 픽셀값 차이(Pixel-value Differencing: PVD)와 최하위 비트(Least Significant Bit: LSB) 교체 방법을 이용하여 원본 이미지의 픽셀값 성질에 맞게 적용하여 고용량의 데이터를 이미지에 숨길 수 있는 방법을 제시한다. 기존에 LSB와 PVD 방법에 근거하여 비밀 자료를 숨기고, 숨겨진 자료를 감지할 수 없도록 하기 위해 많은 자료 은닉 방법들이 연구되었다. 두 연속된 픽셀값 차이가 적을 경우에는 부드러운 영역(Smooth Area)에 속하게 되고, 두 픽셀값 차이가 클 경우에는 경계 영역(Edge Area)에 속한 픽셀로 구별되는데, 본 논문에서 제시하는 방법은 이미지의 부드러운 영역과 경계 영역을 감지하여 부드러운 영역에는 LSB 교체 방법을 적용하고, 경계 영역에는 픽셀값 차이를 이용한 방법을 적용하였다. 실험 결과에서는 본 논문에서 제시한 방법이 기존의 LSB교체 기법을 이용하거나 픽셀값 차이를 이용한 자료은닉 방법에 비해 숨길 수 있는 자료량과 스테고 이미지(Stego-image)의 품질 측면에서 우수함을 보이고 있다.

Abstract This paper proposes a high capacity data hiding method using modulus function of pixel-value differencing (PVD) and least significant bit (LSB) replacement method. Many novel data hiding methods based on LSB and PVD methods were presented to enlarge hiding capacity and provide an imperceptible quality. A small difference value for two consecutive pixels is belonged to a smooth area and a large difference one is located on an edge area. In our proposed method, the secret data are hidden on the smooth area by the LSB substitution method and PVD method on the edge area. From the experimental results, the proposed method sustains a higher capacity and still a good quality compared with other LSB and modified PVD methods.

Key Words : Steganographic, PVD, LSB.

I. 서 론

컴퓨터와 통신기술의 급속한 성장으로 이미지, 오디오, 비디오 등과 같은 디지털 멀티미디어 콘텐츠들은 이전보다 매우 간단하고, 빠르게 확산되고 있다. 그러나 급속한 디지털 콘텐츠의 확산과 더불어 저작권 보호에 대한 문제점이 발생되어 실질적으로 재정적 손실을 초래되고 있는 실정이다. 권한이 없는 사용자로부터 디지털 콘텐츠를 보호하는 것은 정보보호 분야에서 중요하게 요구

된다. 자료은닉은 비밀 정보를 담고 있는 암호화되어 있는 미디어에 비밀 자료가 존재하는 것이 감추어지도록 하는 것과 관련된다. 자료은닉은 숨겨진 비밀 메시지에 대한 탐지를 방지하기 위한 정보 기술이다. 이것은 비밀 메시지의 존재 자체를 숨기는 것으로 비밀 통신을 위한 광대한 내용을 포함하고 있다[1,4,5,6,7,12].

일반적으로 자료는 다양한 방법으로 숨겨질 수 있다. 비밀 데이터를 숨기기 위하여, 직접적인 메시지 삽입 방법은 미디어로 사용되는 이미지의 정보를 나타내기 위한 모든 비트(bit)에 암호화되거나 직접적으로 인식하기 힘든 영역에 선택적으로 메시지를 포함할 수 있도록 하는

*정회원, 영진전문대학 컴퓨터정보계열

*정회원, 경북대학교 컴퓨터공학과

접수일자 2009.8.19, 수정일자 2009.9.20

것이다. 또한 비밀 데이터는 미디어 이미지에 다양한 방법으로 포함될 수 있다. 암호화, 필터링, 알고리즘, 전이 등을 포함한 자료은닉을 위한 일반적인 방법으로 최하위 비트 삽입(LSB) 방법을 포함한 다수의 방법이 존재한다 [1,2,3,5,9].

픽셀값 차이(PVD)와 최하위 비트(LSB)를 이용한 자료은닉 방법은 많은 비밀 자료를 숨길 수 있는 방법으로 연속된 두 픽셀의 차이값을 이용하여 부드러운 영역과 경계선 영역을 구별하여 숨기는 비밀 데이터의 크기를 가변적으로 처리한다[8,11]. 본 논문에서 제시된 방법은 부드러운 영역에서는 LSB교체 기법을 적용하고, 경계선 영역에서는 PVD방법을 이용하여 비밀 데이터를 숨김으로써 고용량의 비밀 데이터를 숨길 수 있도록 제안하고 있다.

이 논문의 다음과 같이 구성된다. 2절에서 본 논문과 관련된 방법을 간단하게 살펴보고, 3절에서는 본 논문에서 제시한 자료은닉 기법과 자료추출 알고리즘에 대해서 자세히 살펴본다. 또한 4절에서는 실험적 결과를 제시하고, 마지막으로 5절에서 결론을 맺는다.

II. 관련 연구

비밀자료를 숨기는 자료은닉 방법 중 잘 알려진 방법으로는 커버 이미지의 최하위 비트에 직접 비밀 데이터를 숨기는 LSB방법이다. 또한, 두 연속된 픽셀의 명암과 부드러움 정도에 따라 숨기는 비밀 데이터의 크기를 다르게 한 방법이 Wu 와 Tsai가 제안한 PVD 방법이다 [10]. 또한 Wu et al.은 커버 이미지의 부드러운 영역에 LSB 치환 방법을 적용한 향상된 PVD 방법을 제안하였다[11]. 그리고 Wang et al.은 계수함수를 적용하여 이미지의 품질을 개선한 스테가노그래픽 기법을 제안하였다 [9].

LSB치환은 커버 이미지 각 픽셀의 몇 개 비트에 중요 데이터를 감추는 일반적인 방법이다. 간단한 LSB 치환 방법을 이용하여 스테가노그래픽 처리를 하는 것은 일반적이다[2]. 비밀 데이터가 커버 이미지의 k-비트 LSB에 끼워 넣어진다고 가정을 하면, 먼저 비밀 데이터는 하나의 비트열의 집합 형태로 재구성되게 된다. 다음으로 재구성된 집합들은 커버 이미지에서 선택된 픽셀의 k-비트 LSB 영역의 값을 대체하여 숨겨지게 된다. 이러한 과정

을 거쳐서 k-비트 LSB 교체 방법이 완료되면 최종적으로 스테고 이미지 S를 얻을 수 있게 된다. 추출과정에서는 커버 이미지없이 스테고 이미지에서 직접 비밀 데이터를 추출할 수 있다. 스테고 이미지 S가 있으면, 순서적으로 한 픽셀마다 k-비트 LSB를 추출하고 비밀 데이터 비트열로 재구성하게 된다. 이러한 방법의 주요 결점은 픽셀별로 사용된 LSB의 숫자가 4보다 같거나 크게 되면 스테고 이미지의 품질이 저하되어 육안으로 이미지가 변경된 것을 쉽게 확인할 수 있다는 것이다. 이러한 문제를 해결하기 위한 방법이 최적화 LBS 치환 방법[2]과, 유전자 알고리즘에 기반한 접근적 최적화 LSB 치환 방법[3] 등이 제시되었다.

Wu와 Tsai는 비밀 데이터를 숨기는 과정에서 숨길 수 있는 비트의 크기를 결정하기 위해 두 연속된 픽셀의 차이를 계산하여 결정하는 픽셀값 차이 (Pixel-value differencing: PVD)방법을 제시하였다. 그레이 커버이미지에서 중복되지 않는 두 연속된 픽셀을 포함한 블록을 구성하고, 두 개의 연속된 픽셀 p_i 와 p_{i+1} 로부터 계산된 차이값을 d_i 라 정의할 경우, p_i 와 p_{i+1} 의 픽셀값을 g_i 와 g_{i+1} 와 라 하면, d_i 값은 -255 부터 255 범위의 값을 가지고, $g_{i+1} - g_i$ 로 계산되어질 수 있다. d 의 차이값을 가진 두 픽셀을 포함한 i 번째 블록 B 에 포함할 수 있는 비트 n 을 $n = \log_2(u_i - l_i + 1)$ 로 계산하게 되는데, 이때 u_i 와 l_i 는 정의된 범위 $R_i(i = 1, 2, \dots, w)$ 의 최저, 최고의 범위값을 의미한다. n 비트를 포함한 비밀 데이터의 비트열은 결정되게 되고 새로운 차이값 d' 이 수식 (1)에 의해 계산되게 된다. 이 때 b 는 n 값 계산을 위한 부분 비밀 데이터에 대한 정수 값이다.

$$d' = \begin{cases} l_i + b & \text{for } d \geq 0, \\ -(l_i + b) & \text{for } d < 0 \end{cases} \quad (1)$$

b 값은 0부터 $u_i - l_i$ 의 범위이기 때문에 d' 은 l_i 부터 u_i 까지의 범위이다. d' 을 계산한 후에, 스테고 이미지의 두 픽셀 블록 (p'_i, p'_{i+1}) 를 만들기 위한 새로운 그레이 값 (g'_i, g'_{i+1}) 계산을 위한 수식(2)에 의해 b 를 끼워 넣게 된다. 이 때 $m = d' - d$ 이다.

$$f((g_i, g_{i+1}), m) = (g'_i, g'_{i+1}) = \begin{cases} (g_i - \lceil m/2 \rceil, g_{i+1} + \lfloor m/2 \rfloor), & \text{if } d \bmod 2 = 1, \\ (g_i - \lfloor m/2 \rfloor, g_{i+1} + \lceil m/2 \rceil), & \text{if } d \bmod 2 = 0 \end{cases} \quad (2)$$

Wu et al.은 두 픽셀의 차이값이 작을 경우, LSB 방법을 사용하여 숨길 수 있는 비밀 데이터의 크기를 향상시킨 방법을 제안하였으나, 두 픽셀의 차이값이 클 경우에는 여전히 Wu와 Tsai의 방법을 사용하고 있다. PVD 방법을 이용해서 두 연속된 픽셀의 차이값을 얻고, 차이값에 따라서 LSB방법과 PVD방법을 결정하고 비밀 데이터를 숨기는 방법을 제시하였다. Wang et al.은 PVD와 계수함수를 사용하여 Wu 와 Tsai이 제시한 방법보다 스테고 이미지의 품질을 개선한 방법을 제안하였다. 차이값 대신에 두 연속된 픽셀의 나머지값을 조정함으로써, 동일한 비밀 데이터를 숨기면서 PSNR값을 2.5~3.3dB증가시켰다.

III. 제안 방법

본 절에서 커버 이미지의 부드러운 영역에는 비밀 데이터를 숨기기 위하여 최하위 비트를 사용하고, 경계 영역에는 기존의 Wang 방법을 적용하여 비밀 데이터를 더 많이 숨길 수 있는 개선된 알고리즘을 제안한다. 부드러운 영역에서는 두 연속된 픽셀로 구성된 각 블록에 6비트의 비밀 데이터를 감출 수 있으며, 그렇지 않은 영역에 대해서는 두 개의 픽셀값 차이값에 따라서 숨길 수 있는 비트수가 결정되게 된다. 이때 사용되어지는 범위 테이블을 R 라고 정의하고, R 는 0부터 255사이의 값을 범위로 가질 수 있는 테이블로 설계하였다. 본 논문에서 제시하는 자료 은닉 및 추출 알고리즘은 다음과 같다.

1. 자료 은닉 알고리즘

다음의 각 단계를 통하여 비밀 데이터를 커버 이미지에 숨기는 알고리즘이 완성된다.

단계1: p_i 와 p_{i+1} 을 연속된 두 개의 픽셀이라고 정의하고, 두 픽셀값을 각각 g_i 와 g_{i+1} 라고 정의하면, 두 픽셀로 구성된 블록의 차이값인 d_i 를 아래에 주어진 공식에 의해서 계산한다.

$$d_i = |g_{i+1} - g_i| \quad (3)$$

단계2: $R_i = \min(u_i - k)$ 일때 d_i 의 최적화된 R_i 를 찾는다. 이때 $u_i \geq k$ 이고 $k = d_i$ 이다. 또한 $R_i \in [l_i, u_i]$ 는 모든 $1 \leq i \leq n$ 에 대해서 최적화된 R_i 이다.

단계3: g_i 와 g_{i+1} 에 의한 나머지 값 Rem_i, Rem_{i+1} 를 계산한다.

$$\begin{aligned} Rem_i &= g_i \bmod b, \\ Rem_{i+1} &= g_{i+1} \bmod b, \\ T_i &= (g_{i+1} + g_i) \bmod b \end{aligned} \quad (4)$$

여기에서 b 는 n 값 계산을 위한 비밀 데이터의 정수 값이다.

단계4: 비밀 데이터의 n 비트를 다음의 두 가지 경우에 따라 g_i 와 g_{i+1} 에 포함한다.

경우 1: 만약 R_i 가 부드러운 영역에 속할 경우, 비밀 데이터 스트림에서 $n = 6$ 비트를 읽어와서 g_i 와 g_{i+1} 를 이진값으로 변환한다. 다음 절차에 의해 g_i 와 g_{i+1} 값을 변경하도록 하여 비밀 데이터를 매개체 이미지에 포함한다. $n = n_0n_1n_2n_3n_4n_5$ 라 할 때,

- (1) p_i 의 LSB 3비트를 $n_0n_1n_2$ 로 치환하여 g_i 를 g'_i 로 변환한다.
- (2) p_{i+1} 의 LSB 3비트를 $n_3n_4n_5$ 로 치환하여 g_{i+1} 를 g'_{i+1} 로 변환한다
- (3) 다음으로 새롭게 만들어진 두 픽셀값의 차이를 계산한다. $d'_i = |g'_{i+1} - g'_i|$
- (4) 만약 d'_i 이 범위 테이블의 범위 값보다 크다면 g'_i 과 g'_{i+1} 값을 다음과 같이 조정한다.

$$(g'_i, g'_{i+1}) = \begin{cases} (g'_i - 8, g'_{i+1} + 8), & \text{if } g'_i \geq g'_{i+1}, \\ (g'_i + 8, g'_{i+1} - 8), & \text{if } g'_i < g'_{i+1} \end{cases} \quad (5)$$

경우 2: 만약 R_i 가 경계선 영역에 속할 경우, Wu와 Tsai에 의해 제시된 $n = \log_2(u_i - l_i + 1)$ 을 만족하는 비밀 데이터 스트림에서 n 비트를 읽어와서 다음 절차에 의해 최적화되도록 g_i 와 g_{i+1} 를 변경한다.

- (1) $t = |T_i - b|$ 와 $t_1 = 2^b - t$ 를 계산한다.
- (2) 만약 $T_i > b$ 라면, g_i 와 g_{i+1} 값을 다음과 같이 계산한다.

$$(g_i', g_{i+1}') = \begin{cases} (g_i - \lfloor t/2 \rfloor, g_{i+1} - \lfloor t/2 \rfloor), & \text{if } t \leq 2^{b-1} \text{ and } g_i \geq g_{i+1} \\ (g_i - \lfloor t/2 \rfloor, g_{i+1} - \lceil t/2 \rceil), & \text{if } t \leq 2^{b-1} \text{ and } g_i < g_{i+1} \\ (g_i + \lfloor t_1/2 \rfloor, g_{i+1} + \lceil t_1/2 \rceil), & \text{if } t > 2^{b-1} \text{ and } g_i \geq g_{i+1} \\ (g_i + \lceil t_1/2 \rceil, g_{i+1} + \lfloor t_1/2 \rfloor), & \text{if } t > 2^{b-1} \text{ and } g_i < g_{i+1} \end{cases} \quad (6)$$

- (3) 만약 $T_i \leq b$ 이면, g_i 와 g_{i+1} 값을 다음과 같이 계산한다.

$$(g_i', g_{i+1}') = \begin{cases} (g_i + \lfloor t/2 \rfloor, g_{i+1} + \lceil t/2 \rceil), & \text{if } t \leq 2^{b-1} \text{ and } g_i \geq g_{i+1} \\ (g_i + \lceil t/2 \rceil, g_{i+1} + \lfloor t/2 \rfloor), & \text{if } t \leq 2^{b-1} \text{ and } g_i < g_{i+1} \\ (g_i - \lfloor t_1/2 \rfloor, g_{i+1} - \lceil t_1/2 \rceil), & \text{if } t > 2^{b-1} \text{ and } g_i \geq g_{i+1} \\ (g_i - \lceil t_1/2 \rceil, g_{i+1} - \lfloor t_1/2 \rfloor), & \text{if } t > 2^{b-1} \text{ and } g_i < g_{i+1} \end{cases} \quad (7)$$

단계5: 경계값 문제(Fall-off the boundary problem)를 고려하여 새로 구성된 픽셀값인 g_i' 과 g_{i+1}' 의 값이 $[0, 255]$ 에 속하지 않을 경우 다음과 같이 g_i' 과 g_{i+1}' 값을 조정한다.

- (1) 만약 $g_i' < 0$ 거나 $g_{i+1}' < 0$ 이면, 새로운 g_i' 과 g_{i+1}' 값을 다음과 같이 구한다.

$$(g_i', g_{i+1}') = (g_i' + 2^{b-1}, g_{i+1}' + 2^{b-1}) \quad (8)$$

- (2) 만약 $g_i' > 255$ 거나 $g_{i+1}' > 255$ 이면, 새로운 g_i' 과 g_{i+1}' 값을 다음과 같이 구한다.

$$(g_i', g_{i+1}') = (g_i' - 2^{b-1}, g_{i+1}' - 2^{b-1}) \quad (9)$$

- (3) 만약 매우 큰 명암대비 픽셀값이 존재할 경우, 아래와 같이 g_i' 과 g_{i+1}' 값을 조정한다. 즉, $d_i > 128$ 이면 g_i' 과 g_{i+1}' 값을 다음과 같이 구한다.

$$(g_i', g_{i+1}') = \begin{cases} (0, g_i' + g_{i+1}'), & \text{if } g_i' < 0 \text{ and } g_{i+1}' \geq 0 \\ (g_i' + g_{i+1}', 0), & \text{if } g_i' \geq 0 \text{ and } g_{i+1}' < 0 \\ (255, g_i' + g_{i+1}' - 255), & \text{if } g_i' > 255 \text{ and } g_{i+1}' \geq 0 \\ (g_i' + g_{i+1}' - 255, 255), & \text{if } g_i' \geq 0 \text{ and } g_{i+1}' > 255 \end{cases} \quad (10)$$

2. 자료 추출 알고리즘

원본 비밀 데이터를 추출하기 위해 다음과 같이 진행한다.

단계1: 비밀 데이터를 포함하고 있는 스테고 이미지를 두 연속된 픽셀로 구성된 블록으로 나눈다.

단계2: 스테고 이미지의 두 연속된 픽셀값인 g_i' 과 g_{i+1}' 의 차이값 d_i'' 을 계산한다.

$$d_i'' = g_{i+1}' - g_i' \quad (11)$$

단계3: 원본 범위 테이블로부터 d_i'' 에 의한 최적화된 R_i 를 찾는다. 그리고 범위 테이블의 영역값을 이용하여 최적화된 R_i 의 범위를 판단한다.

단계4: Wu와 Tsai의 방법과 LSB 치환 방법을 이용하여 비밀 데이터를 추출한다.

경우 1: 만약 R_i 가 경계선 영역에 속할 경우는 b 값을 다음과 같이 추출한다.

$$b = \begin{cases} d_i'' - l_i & \text{for } d_i'' \geq 0, \\ -(d_i'' + l_i) & \text{for } d_i'' < 0 \end{cases} \quad (12)$$

경우 2: 만약 R_i 가 부드러운 영역에 속할 경우는 숨겨진 매개체 이미지의 g_i' 과 g_{i+1}' 의 LSB 3비트가 숨겨진 비밀 데이터를 의미하기 때문에 g_i' 과 g_{i+1}' 의

LSB 각 3비트를 직접 추출한다.

IV. 실험 및 결과

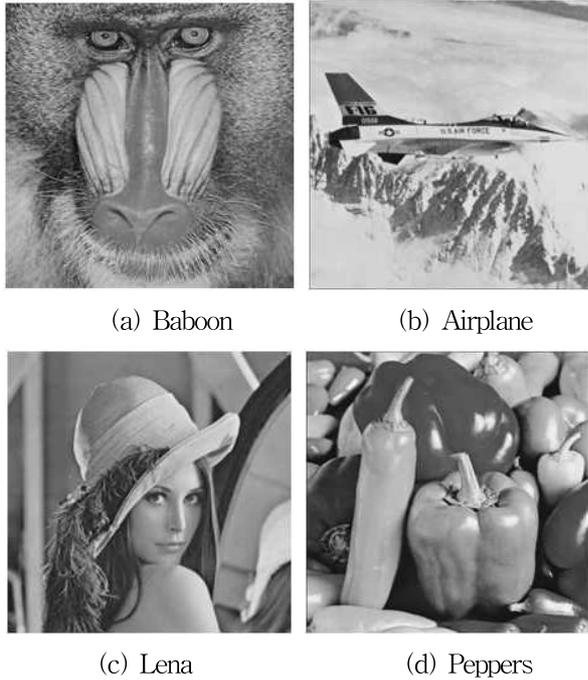


그림 1. 4개의 커버 이미지
Fig 1. 4 cover images

본 논문의 실험에서는 그림 1과 같이 512×512 크기 4개의 그레이 이미지(Gray image)를 사용하였다. 비밀 데이터는 의사 난수(Pseudo-random Number)로 생성하였고, 범위 테이블을 $R1 = [0, 7]$, $R2 = [8, 15]$, $R3 = [16, 31]$, $R4 = [32, 63]$, $R5 = [64, 127]$ 와 $R6 = [128, 255]$ 로 할당하였다. 또한 범위 테이블의 영역 값은 128로 설정하였다. 본 논문에서는 숨긴 데이터의 크기와 이미지 품질 (Visual image quality)을 측정하기 위해 PSNR(Peak signal-to-noise ratio)와 Q-인덱스(Universal image

quality index)를 사용하였다. PSNR은 직관적인 왜곡을 측정하고 계량화하기 위해 사용하였다. 또한 Q-인덱스는 숨겨진 스테고 이미지의 품질을 측정하기 위해 사용하였다. 인덱스값은 통계적인 측정치를 기반으로 하였고, Q 동적 범위는 $[-1, 1]$ 이다.



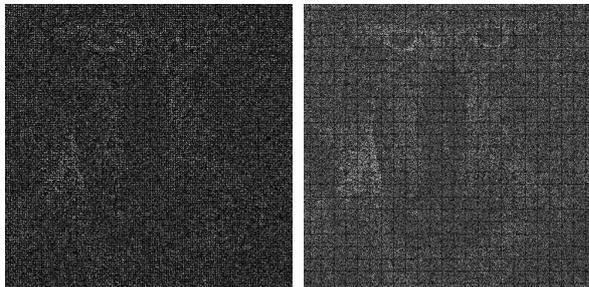
그림 2. Peppers 스테고 이미지: (a) Wu and Tsai의 방법 [10]; (b) Wu et al. 방법 [11]; (c) Wang et al. 방법[8]; (d) 제안 방법, C=Capacity
Fig 2. Peppers stego image : (a) Wu and Tsai's method (b) Wu et al.'s method (c) Wang et al.'s method (d) The proposed method, C=Capacity

그림2는 Peppers 이미지에 대한 스테고 이미지를 나타낸다. 결과를 분석하면 시각적으로는 모든 결과물에 가공된 느낌은 없다. 이것은 왜곡된 정도가 인지하지 못할 정도라는 의미가 된다. 특히, 경계선 영역의 변화는 육안으로 감지하기가 어렵기 때문이다.

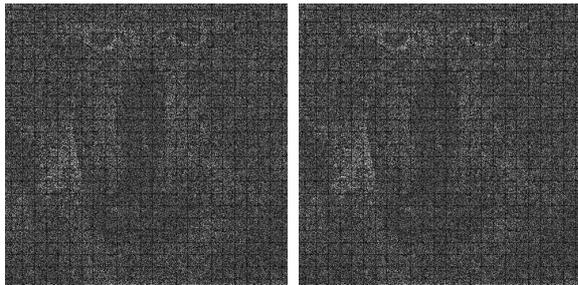
표 1. LSB와 PVD방법에 대한 비교
Table 1. About LSB and PVD methods comparison

커버 이미지	Wu et al. 방법			3-bit LSB 방법			제안 방법		
	용량(Bit)	PSNR	Q	용량(Bit)	PSNR	Q	용량(Bit)	PSNR	Q
Baboon	717,946	35.47	0.9928	786,432	37.92	0.9683	1,134,679	36.23	0.9819
Airplane	770,439	35.61	0.8796	786,432	37.95	0.7108	1,166,907	36.37	0.7858
Lena	765,889	36.20	0.9460	786,432	37.34	0.8194	1,172,587	36.29	0.8847
Peppers	770,253	35.99	0.8812	786,432	37.94	0.8460	1,173,939	36.15	0.8952

표1은 서로 다른 커버 이미지에 비밀 데이터를 포함한 결과에 대한 방법들을 비교한 결과를 보여준다. 표에서 비교된 방법은 LSB와 PVD방법 중에서 비밀 데이터를 많이 숨기는 방법에 대한 기법만을 포함하고 있다. 테이블 결과를 분석해 보면, 제안된 방법은 평균 1,162,028비트를 포함할 수 있었으며 PSNR 가치는 평균 36.26 dB이다. 비록 Wu 등의 방법으로도 PSNR값을 대신하여 많은 비밀 데이터를 숨길 수 있지만, 제안된 방법에서는 큰 왜곡을 가지지 않으면서 더 많은 데이터를 숨길 수 있음을 증명하고 있다. 또한, 이 실험 결과로부터 제시된 방법은 다른 PVD 방법들 보다 많은 비밀 데이터를 포함할 수 있다는 것을 알 수 있다.



(a) PSNR=38.03dB, Q=0.9851 (b) PSNR=35.47dB, Q=0.9763



(c) PSNR=43.11dB, Q=0.9973 (d) PSNR=36.23dB, Q=0.9819

그림 3. 차이값 이미지: (a) Wu and Tsai의 방법 [10]; (b) Wu et al. 방법 [11]; (c) Wang et al. 방법 [8]; (d) 제안 방법

Fig 3. Difference images : (a) Wu and Tsai's method (b) Wu et al.'s method (c) Wang et al.'s method (d) The proposed method

그림 3은 각 방법에 의해 Baboon 이미지를 활용한 숨겨진 스테고 이미지와 커버 이미지에 대한 차이를 나타내는 이미지이다. 결과로부터 모든 방법들은 각 픽셀값들의 차이가 유사함을 알 수 있다. 그림 2와 그림 3은 PVD에 기반한 3개의 다른 방법을 보여준다. 그 방법들 중 Wu et al. 방법은 높은 용량을 나타내고 있으나, 제안된 방법은 4개의 커버 이미지에서 평균 405,896비트를 더

포함할 수 있음을 알 수 있다.

V. 결론

본 논문에서는 픽셀값 차이와 최하위 비트를 이용하여 기존에 제시된 자료은닉 방법보다 숨길 수 있는 비밀 데이터의 크기를 향상시킨 방법을 제시하였다. 이 기법은 두 픽셀의 차이값에 따라서 숨길 수 있는 비밀 데이터의 크기를 변경하였고, 두 픽셀값의 차이가 작을 경우, 최하위 비트를 활용한 자료은닉 기법을 제안함으로써 육안으로 구별할 수 없는 범위 내에서 최대한 비밀 데이터를 숨길 수 있도록 알고리즘을 개선하였다. 실험 결과에서 제안된 방법이 인지할 수 없는 정도의 왜곡을 가지면서 다른 방법들보다 많은 비밀 데이터를 포함할 수 있다는 것을 보여주었다.

참 고 문 헌

- [1] R. J. Anderson and F. A. P. Petitcolas. "On the limits of steganography", *IEEE Journal on Selected Areas on Communications*, 16:474-481, 1998.
- [2] C.-K. Chan and L.-M. Cheng. "Hiding data in images by simple LSB substitution". *Journal of Pattern Recognition*, 37(3):469-474, 2004.
- [3] C.-C. Chang, M.-H. Lin, and Y.-C. Hu. "A Fast and Secure Image Hiding Scheme Based on LSB Substitution". *Proceedings of IJPRAI*, 16(4):399-416, 2002.
- [4] R. C. Gonzalez and R. E. Woods. *Digital Image Processing*. Prentice Hall, Upper Saddle River, NJ, 2002.
- [5] N. F. Johnson and S. Jajodia. "Exploring Steganography: Seeing the Unseen". *IEEE Computer*, 31(2):26-34, 1998.
- [6] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn. "Information hiding - a survey". *Proceedings of the IEEE, special issue on protection of multimedia content*, 87(7):

- 1062-1078,1999.
- [7] R.-Z.Wang and C.-H. Su. "Secret image sharing with smaller shadow images". *Journal of Pattern Recognition Letters*, 27(6):551-555, 2006.
- [8] C.-M.Wang, N.-I.Wu, C.-S. Tsai, and M.-S. Hwang. "A high quality steganographic method with pixel-value differencing and modulus function". *Journal of Systems and Software*, 81(1):150-158, 2008.
- [9] R.-Z. Wang, C.-F. Lin, and J.-C. Lin. "Image hiding by optimal LSB substitution and genetic algorithm". *Journal of Pattern Recognition*, 34(3):671-683, 2001.
- [10] D. C. Wu and W. H. Tsai. "A steganographic method for images by pixel-value differencing". *Journal of Pattern Recognition Letters*, 24(9-10):1613-1626, 2003.
- [11] H. C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang. "Image Steganographic Scheme based on Pixel-value Differencing and LSB replacement Methods". *IEEE Proceedings, Visual Image Signal Processing*, 152(5):611-615, 2005.
- [12] J. Zollner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf. "Modeling the Security of Steganographic Systems". *Proceedings of 2nd Workshop on In Information Hiding*, 1:345-355, 1998.

저자 소개

김 기 중(정회원)



- 1994년 경북대학교 전자공학과 졸업(공학사).
- 1999년 경북대학교 대학원 컴퓨터공학과 석사졸업(공학석사).
- 2007년 경북대학교 대학원 컴퓨터공학과 박사수료.
- 2009년 현재 영진전문대학 컴퓨터정보계열 조교수

<주관심분야 : 정보보호, 영상처리, 데이터베이스, Steganography, 네트워크보안>

정 기 현(정회원)



- 1995년 경북대학교 컴퓨터공학과 졸업(공학사).
- 1997년 경북대학교 대학원 컴퓨터공학과 석사졸업(공학석사).
- 2007년 경북대학교 대학원 컴퓨터공학과 박사졸업(공학박사).
- 2009년 현재 영진전문대학 컴퓨터정보계열 조교수

<주관심분야 : Information Hiding, Watermarking, Cryptography, Network Security, Game & Mobile Programming, Virtual Reality>

유 기 영(정회원)



- 1976년 경북대학교 수학교육과 졸업(이학사).
- 1978년 한국과학기술원 컴퓨터공학과 석사졸업(공학석사).
- 1987년 - 1992년 : Rensselaer Polytechnic Institute.Computer Science 박사과정 졸업(공학박사).
- 2009년 현재 경북대학교 컴퓨터공학과 교수

<주관심분야 : 정보보호, Wireless Mesh Networks, RFID, DRM>