

일반논문 (Regular Paper)

방송공학회논문지 제22권 제3호, 2017년 5월 (JBE Vol. 22, No. 3, May 2017)

<https://doi.org/10.5909/JBE.2017.22.3.350>

ISSN 2287-9137 (Online) ISSN 1226-7953 (Print)

지역적 삽입 비트를 고정시킨 PVD 영상 스테가노그래피

김재영^{a)}, 박한훈^{a)*}, 박종일^{b)}

PVD Image Steganography with Locally-fixed Number of Embedding Bits

Jaeyoung Kim^{a)}, Hanhoon Park^{a)*}, and Jong-Il Park^{b)}

요 약

스테가노그래피는 수신자와 송신자간에 비밀 정보를 제 3자가 알아차리지 못하게 통신하는 기법으로 수천 년 전부터 군사적, 외교적 또는 사업적인 정보들의 전달을 위해서 발달해 왔다. 현대에 이르러서는 디지털 미디어와 통신의 발달로 스테가노그래피의 기법이 더욱 발달하게 되었다. 이 중 영상을 활용하는 스테가노그래피의 기법들은 픽셀에 삽입 비트의 양을 고정하는 LSB, 이웃한 픽셀 쌍의 값 차이를 활용한 PVD 등이 있다. PVD 영상 스테가노그래피의 경우 이웃한 픽셀 쌍의 값의 차이와 설계한 range table에 따라서 삽입하는 비밀 정보량을 유동적으로 하여 많은 양의 정보를 삽입한다. 하지만 비밀 정보를 순서대로 삽입하기 때문에 특정 픽셀 쌍에서 삽입하는 정보량에 오류가 발생하면 그 이후의 정보들 모두 오류를 발생시킨다. 본 논문에서는 이러한 PVD의 특성이 갖는 오류나 외부 공격에 대한 취약점을 보완하고 비밀 정보를 추출 할 수 있는 방법을 제안한다. 실험의 방법은 다양한 잡음들을 스테고 영상에 삽입해서 삽입 된 비밀 정보를 비교하고 분석한다. 기존의 PVD는 잡음에 대해서 전혀 비밀 정보의 보존이 불가능하지만 제안된 지역적 삽입 비트 고정 PVD의 경우에는 스테고 영상의 부분적인 잡음에 대해서 비밀 정보를 강건하게 추출할 수 있음을 확인하였다.

Abstract

Steganography is a technique for secret data communication, which is not perceived by third person between a receiver and a transmitter. It has been developed for thousands of years for the transmission of military, diplomatic or business information. The development of digital media and communication has led to the development of steganography techniques in modern times. Technic of image steganography include the LSB, which fixes the number of embedded bits into a pixel, and PVD, which exploits the difference value in the neighboring pixel pairs. In the case of PVD image steganography, a large amount of information is embedded fluidly by difference value in neighboring pixel pairs and the designed range table. However, since the secret information in order is embedded, if an error of the number of embedded bits occurs in a certain pixel pair, all subsequent information will be destroyed. In this paper, we proposes the method, which improve the vulnerability of PVD property about external attack or various noise and extract secret information. Experimental process is comparison analysis about stego-image, which embedded various noise. PVD shows that it is not possible to preserve secret information at all about noise, but it was possible to robustly extract secret information for partial noise of stego-image in case of the proposed PVD image steganography with locally-fixed number of embedding bits.

Keyword : Image steganography, pixel-value differencing, locally-fixed bits, robust extraction

Copyright © 2017 Korean Institute of Broadcast and Media Engineers. All rights reserved.

“This is an Open-Access article distributed under the terms of the Creative Commons BY-NC-ND (<http://creativecommons.org/licenses/by-nc-nd/3.0>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited and not altered.”

I. 서론

비밀 정보를 제 3자가 알아차리지 못하도록 전송하는 방법인 스테가노그래피(steganography)는 수천 년 전부터 군사적이나 외교적 또는 사업적인 정보들을 은밀하게 전달하기 위해서 발달해왔다. 현대에 이르러서는 정보통신기술, 디지털 멀티미디어 그리고 인터넷의 발달로 인해서 스테가노그래피의 기법이 다양해졌고 과거와 같이 군사, 외교, 기술, 영업 뿐 아니라 의료, 저작권 등의 다양한 비밀 정보를 교환하거나 보호하기 위해서 활용된다^[1].

디지털미디어 중에서도 영상에 비밀 정보를 삽입하는 다양한 기법들이 연구 되었는데 공간 도메인에 삽입하는 기술 중에서 가장 대표적인 기법은 LSB(least significant bit)이다. LSB^[2]는 영상 픽셀의 하위 비트로 픽셀 단위로 삽입하고자 하는 정보의 양을 고정시켜서 모든 픽셀에 같은 정보량을 삽입하는 기법이다. PVD(pixel value difference)^[3]는 영상에서 이웃한 픽셀의 관계를 고려하는 기법으로 이웃한 두 픽셀인 픽셀 쌍의 값 차이가 크면 많은 정보를 삽입하고 이웃한 두 픽셀의 값 차이가 작으면 적은 정보를 삽입한다. PVD를 활용한 다양한 기법들이 존재하는데 대응하는 픽셀 쌍의 수를 늘려서 더 많은 정보를 삽입하는 TPVD^[4], OPVD^[5]등 이 있다. TPVD는 영상을 2×2 의 서브 블록으로 나누어 기준 픽셀에서 3방향으로 정보를 삽입하는 기법이며 OPVD는 영상을 3×3 의 서브 블록으로 나누어 중심 픽셀로부터 8방향으로 정보를 삽입하는 기법이다. 그리고 정보를 적층으로 쌓는 PVD 중첩 기법이 있다^[6]. PVD 중첩 기법은 layer단위로 중복되지 않는 서브 블록을 구성해서 PVD의 기법을 적용하게 된다. 이러한 PVD 기반의 스테가노그래피의 경우에 일반적으로 삽입용량적인 측면에서의 연구방식이며 인간의 시각적

인 인지의 능력에 의존하여 비밀 정보가 있다는 사실 자체를 제 3자로부터 숨겨 공격이나 추출의 시도를 사전에 차단하게 하는데 주안점을 둔다. 그렇기 때문에 외부로부터의 공격에 대한 강건함에 대해서는 전혀 고려하지 않는다^[3]. 또한 외부의 공격에 대해서 강건함을 보여주는 데이터 은닉 기법들은 주로 공간 도메인보다는 다른 도메인으로 변환하여 적용을 한다. 그러한 방법들은 주로 Fresnel 변환^[7], 웨이블릿 변환^[8-10], DCT 도메인^[11] 등 변환을 통한 다른 도메인을 활용하는 방법들이다. 그래서 PVD 알고리즘의 경우 공간도메인에 비밀 정보를 삽입한다는 점 때문에 외부로부터의 공격이 발생하게 될 경우에 삽입한 비밀 정보의 보존이 굉장히 어렵다. 특히나 PVD의 알고리즘의 경우에 픽셀 쌍의 픽셀 값 차이에 따라서 삽입하는 정보량을 유동적으로 선택하기 때문에 삽입 비트수의 오류가 발생하게 되면 해당 픽셀 쌍 이후의 모든 정보가 오류를 유발한다. 이러한 문제를 개선하기 위해서 전체 영상의 삽입 비트 수를 고정시키게 되면 삽입 용량의 측면에서 손실이 크게 되며 마치 LSB와 같은 기능을 하게 된다. 본 논문에서는 PVD가 갖는 약점인 외부의 공격이나 오류가 발생 시 정확한 비밀 정보가 추출이 되지 않는다는 점을 보완하기 위한 지역적 삽입 비트 고정 PVD 영상 스테가노그래피를 제안한다. 지역적 삽입 비트 고정 PVD는 초기 픽셀 쌍 또는 서브 블록에서 오류가 발생하더라도 전체적인 삽입 정보가 최대한 온전하게 추출 될 수 있도록 해준다. 2장에서는 논문의 기반이 되는 PVD의 기법에 대해서 간단하게 소개하며 3장에서 지역적 삽입 비트 고정 PVD의 삽입과 추출 방법에 대해서 구체적으로 제안하고 4장에서는 실험, 최종으로 5장에서 결론을 도출한다.

II. PVD(pixel-value differencing) 기법

[3]에서 제안한 PVD기법은 이웃한 두 픽셀의 픽셀 값의 차이에 따라서 1개의 픽셀 쌍마다 삽입하는 비트의 수를 조절한다. 비밀 정보를 삽입하기 전에 영상을 1×2 크기의 중복되지 않는 서브 블록으로 나누고 서브 블록 내부의 이웃한 두 픽셀을 p_0 와 p_1 이라고 할 때 픽셀 값의 차 d 를 $d = p_1 - p_0$ 이라고 한다. 8비트, 1채널의 그레이 영상에서 픽셀 값이 0~255의 값을 갖기 때문에 d 값의 범위는 -

a) 부경대학교 전자공학과(Pukyong National University, Department of Electronic Engineering)

b) 한양대학교 컴퓨터소프트웨어학과(Hanyang University, Department of Computer and Software)

‡ Corresponding Author : 박한훈 (Hanhoon Park)

E-mail: hanhoon_park@pknu.ac.kr

Tel: +82-51-629-6225

ORCID: <http://orcid.org/0000-0002-6968-4565>

* 이 연구는 방위사업청 및 국방과학연구소의 재원에 의해 설립된 신호 정보 특화연구센터 사업의 지원을 받아 수행되었음.

Manuscript received November 8, 2016; Revised May 27 2017; Accepted April 27, 2017.

255~255가 된다. 영상의 특성상 $|d|$ 의 값이 큰 부분은 영상의 edge에 해당하는 부분이라고 볼 수 있으며 $|d|$ 의 값이 작은 부분은 평탄한 부분이라고 볼 수 있다. PVD기법은 edge에 해당하는 부분에서 더 많은 정보를 삽입 할 수 있다. 실질적으로 픽셀 쌍에 정보를 삽입하기 위해서는 range table을 설계해야 한다. [3]에서 사용한 range table은 표 1의 (a)와 (b)이며 range table (a)를 사용할 경우에 (b)를 사용하는 것 보다 더 많은 삽입 양을 갖게 된다^[3]. range table의 l_k 와 u_k 는 $|d|$ 값 즉 픽셀 쌍의 값 차이가 가질 수 있는 하한값과 상한 값이다. 픽셀 값 차이 $|d|$ 는 항상 사용한 range table의 $l_k \leq |d| \leq u_k$ 의 관계를 만족해야 하며 이를 만족하는 픽셀 쌍은 range table에서 해당하는 삽입 비트 수 n 값을 갖게 된다. 예를 들어 하나의 픽셀 쌍 (p_0, p_1) 이 (127,30) 이라면 이 픽셀 쌍에 삽입 가능한 비트수를 결정하기 위해서 우선 d 값을 계산하게 되며 그 값은 $|d| = |30 - 127| = 97$ 이므로 표 1의 range table (a)와 (b)에서 비교해보면 각 삽입 비트 수 n 은 6비트와 5비트가 된다.

표 1. 픽셀 쌍의 픽셀 값 차이에 대한 삽입 비트 수 range table (a) 와 (b) [3]
Table 1. Range table (a) and (b), the number of embedded bits about differences of pixel values of the pixel pair [3]

(a)

l_k	u_k	n
0	7	3
8	15	3
16	31	4
32	63	5
64	127	6
128	255	7

(b)

l_k	u_k	n
0	1	1
2	3	1
4	7	2
8	11	2
12	15	2
16	23	3
24	31	3
32	47	4
48	63	4
64	95	5
96	127	5
128	191	6
192	255	6

PVD를 적용하기 위한 range table의 설계와 삽입하고자 하는 비밀정보의 bit stream(그림 1 참조)이 구성이 되었다면 정보의 삽입과 추출이 가능하다. 다음의 과정을 통해서 높이 H , 가로 W 인 $H \times W$ 크기의 커버 영상에 비밀 정보를 삽입하고 추출하는 과정을 보여준다.



그림 1. 문자열 "ABC"의 bitstream
Fig. 1. Bitstream of a string "ABC"

삽입 과정은 다음과 같다.

- step 1 : 커버 영상은 $(H \times W)/2$ 개의 서브 블록으로 구성되므로 첫 번째 픽셀을 p_0 라고 하고 첫 번째 서브 블록을 SB_0 이라고 하면 $0 \leq n < (H \times W)/2$ 이다. n 번째 서브 블록의 픽셀은 p_{2n} 과 p_{2n+1} 이며 $d_n = p_{2n+1} - p_{2n}$ 이다.
- step 2 : 설계한 range table을 통해서 $l_k \leq d_n \leq u_k$ 를 만족하는 삽입 비트 수 t_n 을 구한다.
- step 3 : 삽입 할 bit stream으로부터 t_n 만큼 가져와서 십진수 T_n 으로 변환한다.
- step 4 : 새로운 d'_n 은 d_n 이 '0' 또는 양수이면 $d'_n = l_k + T_n$, 음수이면 $d'_n = -(l_k + T_n)$ 이다.
- step 5 : 최종 삽입을 위한 $m_n = d'_n - d_n$ 이며 d_n 이 홀수이면

$$p'_{2n} = p_{2n} - \text{ceiling}(m_n/2),$$

$$p'_{2n+1} = p_{2n+1} + \text{floor}(m_n/2)$$

d_n 이 짝수이면

$$p'_{2n} = p_{2n} - \text{floor}(m_n/2),$$

$$p'_{2n+1} = p_{2n+1} + \text{ceiling}(m_n/2).$$

- step 6 : 비밀 정보 bit stream의 삽입이 끝날 때 까지 step 1~5를 반복한다.

추출 과정은 다음과 같다.

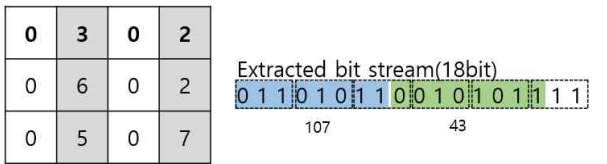
- step 1 : 생성된 스테고 영상을 서브 블록으로 나누고 n

번째 서브 블록의 픽셀을 각 p_{2n}, p_{2n+1} 이라고 하면 $d_n = p_{2n+1} - p_{2n}$ 이다.

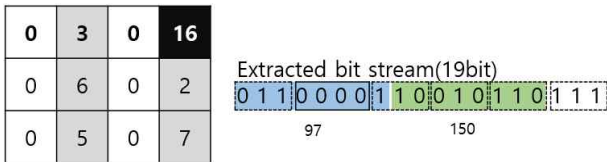
- step 2 : 삽입 시 사용한 range table과 조건 $l_k \leq |d_n| \leq u_k$ 을 만족하는 삽입 비트 수 t_n 과 l_k 를 구한다.
- step 3 : $|d_n| - l_k$ 를 2진수로 변환하고 bit stream에 추가한다.
- step 4 : 비밀 정보량을 만족할 때 까지 step 1~3을 반복한다.

III. 제안 방법

PVD는 비밀 정보의 추출이 삽입 순서에 따라서 bit stream에도 차례로 삽입되기 때문에 생성된 스테고 영상에 공격이나 오류가 발생하고 그로인해 서브 블록에서 추출 비트의 수에 오류가 발생하면 그 이후의 bit stream을 원래 포맷으로 변환하는 과정에서 문제가 발생한다(그림 2 참조). 그래서 이러한 오류에 대해서 좀 더 강건한 추출을 위해서 다음의 지역적 삽입 비트 고정 알고리즘을 제안한다.



Stego image



Be attacked

그림 2. 추출 비트 수 오류
 Fig. 2. Error in the number of extracted bits

1. 지역적 삽입 비트 고정

지역적 삽입 비트 고정에 앞서서 서브 블록의 구성을 한다. PVD 삽입과 이웃한 픽셀들의 지역적인 픽셀 값 유사성

을 활용하기 위해서 1×2 의 정수 배를 하여 $m \times m$ 크기의 서브 블록으로 구성한다. 서브 블록은 픽셀 값의 지역적 유사성을 보존할 수 있도록 정사각형의 형태로 구성한다. $m \times m$ 크기의 서브 블록에는 $(m \times m)/2$ 개의 PVD 서브 블록이 있고 서브 블록 내의 고정 삽입 비트는 다음과 같이 구할 수 있다(그림 3. 참조).

$$t_{avg} = \left\lfloor \frac{\sum_{n=0}^{(m \times m)/2 - 1} t_n}{(m \times m)/2} \right\rfloor \quad (1)$$

①		⑤	
②		⑥	
③		⑦	
④		⑧	

Number of embedding bits about each pixel pair = t_n

$$t_{avg} = (\sum_{n=0}^7 t_n) / 8$$

그림 3. 4×4 서브 블록 삽입 비트 수 고정
 Fig. 3. Fixed number of embedding bits in the 4×4 sub-block

2. 삽입 알고리즘

$H \times W$ 크기의 커버 영상을 $m \times m$ 서브 블록으로 분할하면 $(H \times W)/m^2$ 개의 서브 블록으로 구성된다. 서브 블록의 내부는 $(m \times m)/2$ 개의 픽셀 쌍으로 구성되어 되며 이 때 첫 번째 서브 블록을 SB_0 x 번째 서브 블록을 SB_x 라고 하며 x 번째 서브 블록의 첫 번째 픽셀 쌍은 $p_{x,0}$ 와 $p_{x,1}$ 그리고 SB_x 서브 블록의 n 번째 픽셀 쌍은 $p_{x,2n}$ 과 $p_{x,2n+1}$ 이다. 서브 블록의 픽셀 쌍의 수는 $m \times m/2$ 가 된다.

$m \times m$ 서브 블록에 따라서 삽입 비트 수 t_{avg} 를 고정하기 때문에 다음과 같은 3가지의 경우가 존재한다. case 1 $t_{avg} = t_n$ 와 case 2의 $t_{avg} < t_n$ 의 경우에는 기존의 PVD와 동일한 방법으로 적용한다. case 3 $t_{avg} > t_n$ 의 경우는 다음과

같은 순서로 삽입을 한다.

step 1 : $t_{avg} > t_n$ 을 만족하는 x 번째 서브 블록의 n 번째 픽셀 쌍의 픽셀이 각 $p_{x, 2n}$ 과 $p_{x, 2n+1}$ 일 때 $d_{x, n} = p_{x, 2n+1} - p_{x, 2n}$ 이다.

step 2 : range table을 통해서 $l_k \leq d_{x, n} \leq u_k$ 를 만족하는 l_k 값을 구한다.

step 3 : 삽입 할 bit stream으로부터 t_{avg} 만큼 가져와서 십진수 T_{avg} 으로 변환한다.

step 4 : 새로운 $d'_{x, n}$ 을 계산하며 다음과 같다.

$$d_{x, n} \geq 0 \text{ 이면 } d'_{x, n} = l_k + T_{avg}$$

$$d_{x, n} < 0 \text{ 이면 } d'_{x, n} = -(l_k + T_{avg}) \text{ 이다.}$$

step 5 : $m_{x, n} = d'_{x, n} - d_{x, n}$ 이며 비밀 정보가 삽입된 이후 픽셀 값은

$$p'_{x, 2n} = p_{x, 2n} - ceiling(m_{x, n}/2) ,$$

$$p'_{x, 2n+1} = p_{x, 2n+1} + floor(m_{x, n}/2) \text{ 이다.}$$

step 6 : 비밀 정보 bit stream의 삽입이 끝날 때 까지 step 1~5를 반복한다.

결론적으로는 $t_{avg} \leq t_n$ 의 경우는 같다고 볼 수 있으며 $t_{avg} < t_n$ 의 경우는 기존의 PVD와 비교해서 최대용량을 삽입하지 못하는 경우이다.

3. 추출 알고리즘

3. 2절과 동일한 조건하에서 추출 알고리즘을 설명한다. 동일하게 3가지의 경우가 존재한다. case 1의 $t_{avg} = t_n$ 경우는 기존의 PVD와 같으며 case 2 $t_{avg} < t_n$ 의 경우는 다음과 같다.

step 1 : $t_{avg} < t_n$ 을 만족하는 x 번째 서브 블록의 n 번째 픽셀 쌍의 픽셀이 각 $p_{x, 2n}$, $p_{x, 2n+1}$ 이라고 하면 $d_{x, n} = p_{x, 2n+1} - p_{x, 2n}$ 이다.

step 2 : Range table과 조건 $l_k \leq |d_{x, n}| \leq u_k$ 을 만족하는 l_k 를 구한다.

step 3 : $|d_{x, n}| - l_k$ 값을 2진수로 변환하고 t_{avg} 보다 큰 비트는 제외하고 bit stream에 추가한다.

step 4 : 비밀 정보량을 만족할 때 까지 step 1~3을 반복한다.

case 3 $t_{avg} > t_n$ 의 경우는 다음과 같다.

step 1 : $t_{avg} > t_n$ 을 만족하는 x 번째 서브 블록의 n 번째 픽셀 쌍의 픽셀이 각 $p_{x, 2n}$, $p_{x, 2n+1}$ 이라고 하면 $d_{x, n} = p_{x, 2n+1} - p_{x, 2n}$ 이다.

step 2 : Range table과 조건 $l_k \leq |d_{x, n}| \leq u_k$ 을 만족하는 l_k 를 구한다.

step 3 : $|d_{x, n}| - l_k$ 를 2진수로 변환하고 t_n 다음 번째의 $t_{avg} - t_n$ 개의 MSB(most significant bit)는 '0' 으로 복원하고 bit stream에 추가한다.

step 4 : 비밀 정보량을 만족할 때 까지 step 1~3을 반복한다.

4. 비밀 정보 오차 발생

외부의 잡음이나 오류가 없더라도 오차가 발생하게 된다. 그 오차는 다음과 같은 경우 발생할 수 있다. 우선 case 2의 $t_{avg} < t_n$ 인 경우에는 손실 없이 정보의 추출이 가능하지만 case 3의 $t_{avg} > t_n$ 경우에는 다음 그림 4와 같은 오차가 발생한다. 즉 t_n 보다 큰 순서의 비트에 대해서는 보존되지 않을 수 있다.

그림 4와 같이 삽입 비트 수 t_{avg} 를 결정 한 후의 삽입 알고리즘은 기존의 경우와 같이 PVD와 같이 서브 블록 전체의 픽셀 쌍에 적용하는데 다음과 같이 삽입과 추출이 진행된다. $t_{avg} = 4$, $P(8,8)$, $t_n = 3$, bit stream 1111, range table은 8, 8, 16, 32, 64, 128에 secret data를 삽입하는 과정은 다음과 같다.

step 1 : if ($t_{avg} > t_n$) $d = 8 - 8 = 0$.

step 2 : $l_k = 0$, $data = 15$, $d' = 0 + 15 = 15$.

step 3 : $m = d' - d = 15$.

step 4 : $P'(0,15)$.

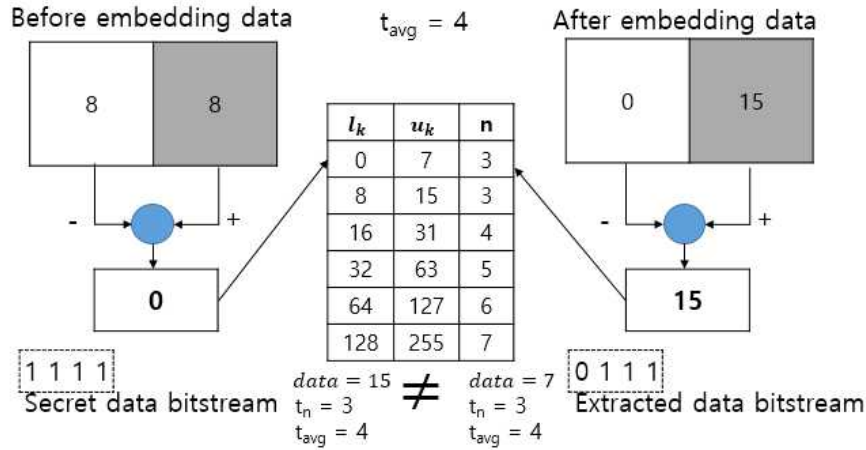


그림 4. $t_{avg} > t_n$ 의 경우 추출 오차
 Fig 4. Extraction error in the $t_{avg} > t_n$ case

P 의 삽입 비트 수는 3이지만 t_{avg} 가 4이기 때문에 4비트의 $data$ 를 삽입하게 된다. 삽입 한 후의 P' 에 대해서 추출해보면 다음과 같다.

step 1 : $P'(0,15)$, $d = 15 - 0 = 15$, $l_k = 8$,
 $t_n = 4$.

step 2 : $data = d - l_k = 7 = 0111_2$ 이고 t_{avg} 는 4이므로 최종 추출 $data = 0111_2$ 이다.

추출 과정에서 위의 경우에 삽입 비트가 3이고 t_{avg} 가 4였기 때문에 이 차이로 삽입 값은 1111_2 이나 추출 값은 0111_2 로 4번째 비트가 오차를 보인다. 즉 $t_{avg} > t_n$ 이 발생하면 추출 시점에서 $t_{avg} - t_n$ 비트 수 만큼의 MSB를 임의로 복원을 해야 하는 경우가 발생하기 때문에 오차가 발생한다. 하지만 일반적으로 비밀 정보의 원 형태는 byte단위로 사용하기 때문에 크게 문제가 되지 않으며 비밀 정보가 영상의 경우이므로 단지 1pixel만큼의 오차만을 나타내므로 전체적인 bit stream에는 거의 영향을 주지 않는다.

IV. 실험 및 결과

실험은 영상 스테가노그래피의 중요한 요소인 삽입 용량

과 커버 영상과 비밀 정보가 삽입 된 스테고 영상이 얼마나 유사한지를 나타내기 위한 수치인 PSNR(peak signal to noise ratio)의 관계와 의사 난수 발생(pseudo-random numbers)을 통해서 임의의 위치에 임의의 값을 갖는 잡음을 추가하여 잡음이 더해진 스테고 영상에서도 비밀 정보가 온전하게 추출이 가능한지에 대해서 살펴본다.

1. 삽입 용량과 은닉성 비교

PVD와 지역적 삽입 비트 고정 PVD가 용량과 PSNR의 성능이 어떻게 차이를 보이는지 확인하기 위해서 512×512 크기의 8비트, 1채널 커버 영상 7개(lena.bmp, baboon.bmp, jet.bmp, goldhill.bmp, pepper.bmp, barbara.bmp, boat.bmp)에 271×180 크기의 puppy.bmp를 비밀 정보로 삽입한다. 지역적 삽입 비트 고정 PVD의 서브 블록 크기는 6×6 을 사용한다.

표 2에서 PVD와 지역적 삽입 비트 고정 PVD를 비교하였다. 지역적 삽입 비트 고정 PVD의 경우에 용량적인 측면에서는 약간의 성능 저하가 발생하지만 PSNR의 측면에서는 더 낫다는 것을 보여 주었다. PVD의 경우에는 그림 6(a)와 같이 동일한 비밀 정보가 추출이 되었지만 지역적 삽입 비트 고정 PVD의 삽입한 비밀 정보와 추출한 비밀 정보의 비교에서 12개의 pixel이 값의 차이를 보였다(표 2 참조). 하지만 그림 6 (b), (c), (d), (e), (f), (g), (h)에서 확인

할 수 있는 것처럼 비밀 정보가 영상의 경우에는 인지하
는데 전혀 문제가 없다. 또한 전체적인 정보를 분석하는데

문제가 없었기 때문에 정보의 보존의 측면에서는 문제가
없다고 할 수 있다.



(a)



(b)

그림 5. 스테고 영상. (a) PVD 적용, (b) 지역적 삽입 비트 고정 PVD 적용

Fig 5. Stego-image. (a) Using PVD and (b) using PVD with locally-fixed number of embedding bits

표 2. PVD와 6×6크기 서브 블록을 사용한 지역적 삽입 비트 고정 PVD 용량 및 PSNR비교

Table 2. Capacity and PSNR comparison between PVDs with and without locally-fixed number of embedding bits

method	cover image	secret(bit)	capacity(bit)	PSNR (dB)	error pixels
PVD	lena	puppy (390,240)	410,394	41.6066	0
proposed method			393,300	42.3895	12
PVD	baboon		457,105	38.0646	0
proposed method			410,040	38.9864	12
PVD	jet		409,845	41.1636	0
proposed method			393,714	41.7001	12
PVD	goldhill		411896	41.559	0
proposed method			392886	42.5912	12
PVD	pepper		404449	41.4452	0
proposed method			392094	42.1204	12
PVD	barbara		464314	35.6523	0
proposed method			429786	37.441	12
PVD	boat		451083	39.3212	0
proposed method			397458	40.4689	12

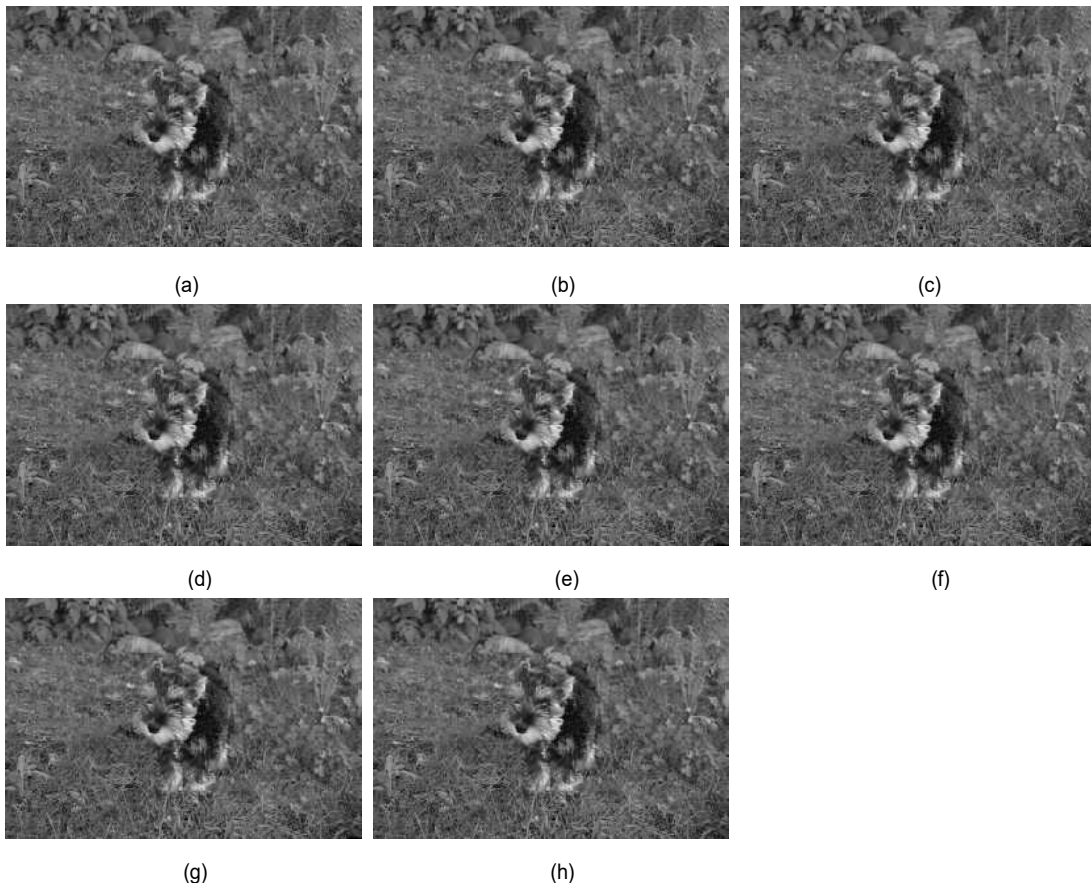


그림 6. 삽입 비밀 정보와 추출 정보. (a)삽입 비밀 정보, (b), (c), (d), (e), (f), (g), (h) 그림 5(b)의 스테고 영상으로부터 추출된 정보
 Fig. 6. Embedded secret data and extracted data. (a) embedded secret data and (b), (c), (d), (e), (f), (g) and (h) extracted data from the stego images in Fig. 5(b)

2. 잡음에 대한 비밀 정보 추출 비교

이 절에서는 첫 번째로 4장 1절에서 생성한 스테고 영상에 5%의 잡음을 추가하여 삽입한 정보의 추출이 온전히 이루어지는지 알아보고 두 번째로 텍스트 영상을 사용하여 잡음의 양을 조절해가며 비밀 정보를 추출하여 텍스트 영상이 얼마나 보존되는지 알아본다. 마지막으로 가우시안 잡음에 대해서 비밀 정보 추출이 어떻게 되는지 알아본다.

2.1. 5%의 잡음 삽입에 대한 PVD와 제안된 방법의 추출 정보 비교

4장 1절에서 생성한 스테고 영상을 사용하여 외부의 오류나 공격에 대해서 강건함을 확인하기 위해서 총 픽셀 쌍수의 5%에 해당하는 $6553(0.05 \times (H \times W)/2)$ 개의 픽셀에 의사 난수 발생(pseudo-random numbers)을 사용해서 잡음을 추가하였다(그림 7 참조). 5%의 오류에 대한 추출된 비밀 정보는 다음의 그림 8과 같다. 5%의 정보를 추가한

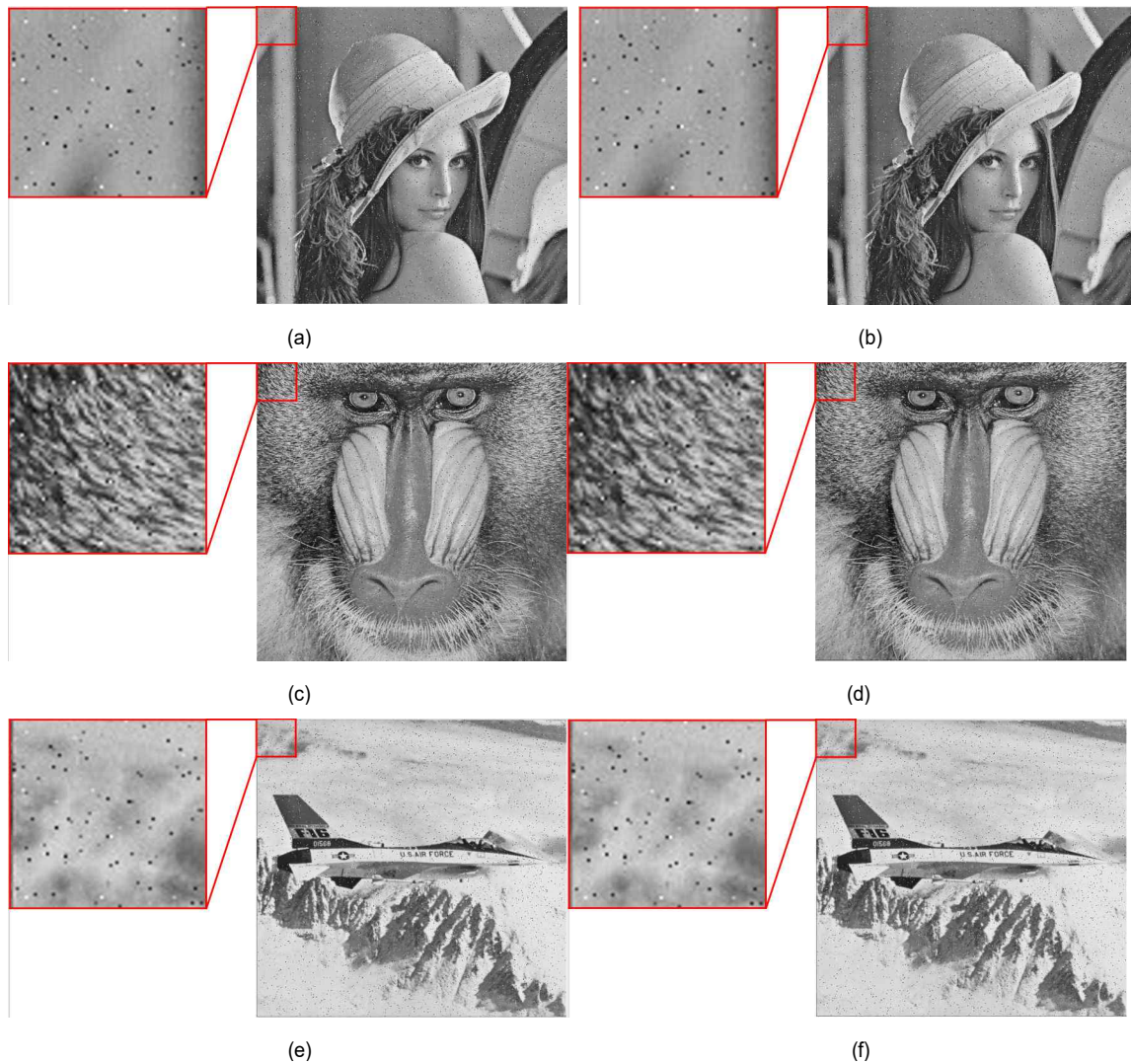


그림 7. 잡음 5% 삽입 스테고 영상 PVD(a, c, e)와 지역적 삽입 비트 고정 PVD(b, d, f) (각 lena stego.bmp, baboon stego.bmp, jet stego.bmp)
 Fig 7. Stego-image with 5% noise (a, c, e)(using PVD) and (b, d, f)(using locally-fixed number of embedding bits) (each lena stego.bmp, baboon stego.bmp and jet stego.bmp)

스테고 영상은 표 3에서 처럼 PSNR이 약 24~25dB정도를 보였고 이는 커버 영상이 많이 훼손되었음을 알려준다. 이렇게 잡음을 추가한 PVD 스테고 영상으로부터 추출한 비

밀 정보 그림 8 (a), (c), (e)는 비밀 정보로 사용하기에는 너무 훼손의 정도가 심한 것을 볼 수 있다. 반면에 지역적 삽입 비트 고정 PVD의 경우에는 그림 8 (b), (d), (f)에서

표 3. 5% 잡음에 대한 PVD와 지역적 삽입 비트 고정 PVD 추출 정보 비교

Table 3. Comparison between extraction results of conventional PVD and PVD with locally-fixed number of embedding bits at 5% random noise

method	cover image	embedded noise(%)	PSNR (dB)	error pixels	error-ratio (error pixels / total pixels)(%)
PVD	lena	6553(5)	25.2146	48556	99.3575
proposed method	stego		25.2305	5937	12.2271
PVD	baboon		25.3686	48562	99.3698
proposed method	stego		25.4119	5868	12.0074
PVD	jet		24.0446	48566	99.3779
proposed method	stego		24.0540	5895	12.0626
PVD	goldhill		24.9828	48543	99.3309
proposed method	stego		25.0025	5860	12.0131
PVD	pepper		24.9636	48559	99.3636
proposed method	steog		24.9774	5833	11.9578
PVD	boat		25.2242	48553	99.3513
proposed method	stego		25.2632	5935	12.1669
PVD	barbara		24.8547	48560	99.3657
proposed method	stego		24.975	5908	12.1115

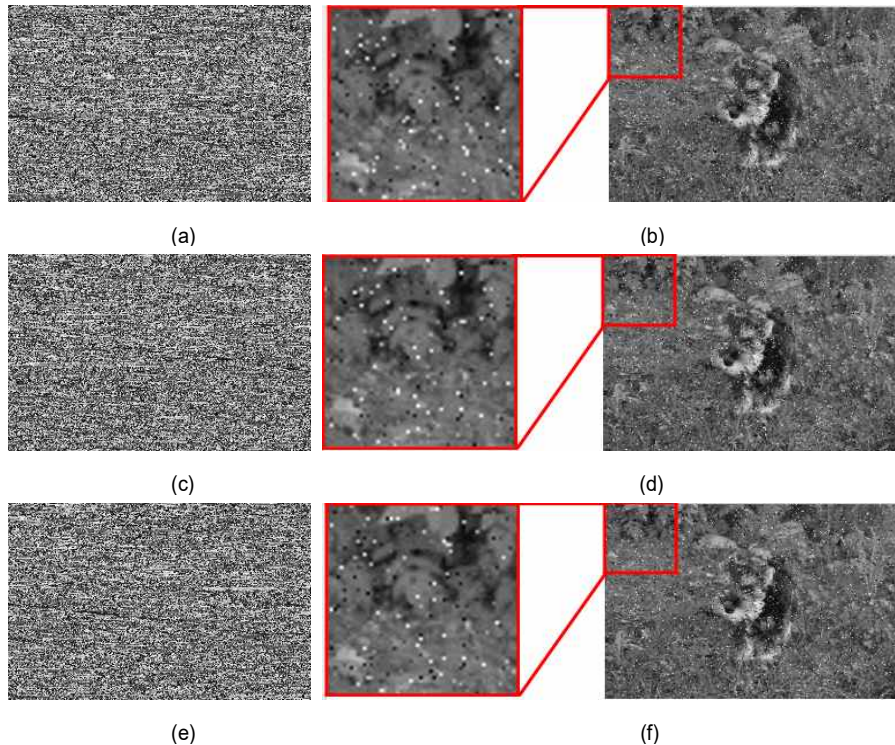


그림 8. 그림 7의 스테고 영상에 대해 기존 PVD에 의한 추출 정보 (a, c, e)와 지역적 삽입 비트 고정 PVD에 의한 추출 정보(b, d, f)
 Fig 8. Extracted data from the stego-images in Fig. 7 (a, c, e) using conventional PVD and (b, d, f) using PVD with locally-fixed number of embedding bits

볼 수 있는 것처럼 전체적인 비밀 정보의 내용은 유지가 되는 것을 볼 수 있다. 표 3의 오류 픽셀/비밀 정보의 수치를 보면 원 정보와 실제 정보의 오차정도를 보여준다. PVD의 경우에는 대략 99%이상 훼손이 되었음을 볼 수 있으며 지역적 삽입 비트 고정 PVD의 경우에는 12%정도의 훼손을 보였고 나머지는 온전하게 추출이 되었다(세부사항은 표 3 참조).

2.2 잡음량의 변화에 따른 제안된 방법의 추출 비밀 정보 비교

블록 크기를 8×8 로 하고 잡음을 0.1%, 1%, 10%, 20%, 30%, 40%, 50%, 60%, 70%로 점차 증가시켜가며 비밀 정보를 추출하였다. 좀 더 의미 있는 결과를 유도하기 위해서 삽입 정보를 텍스트 영상으로 하였고 실험에 사용한 커버 영상은 다음 그림 9 (a)와 같고 세부 사항은 표 4와 같다.

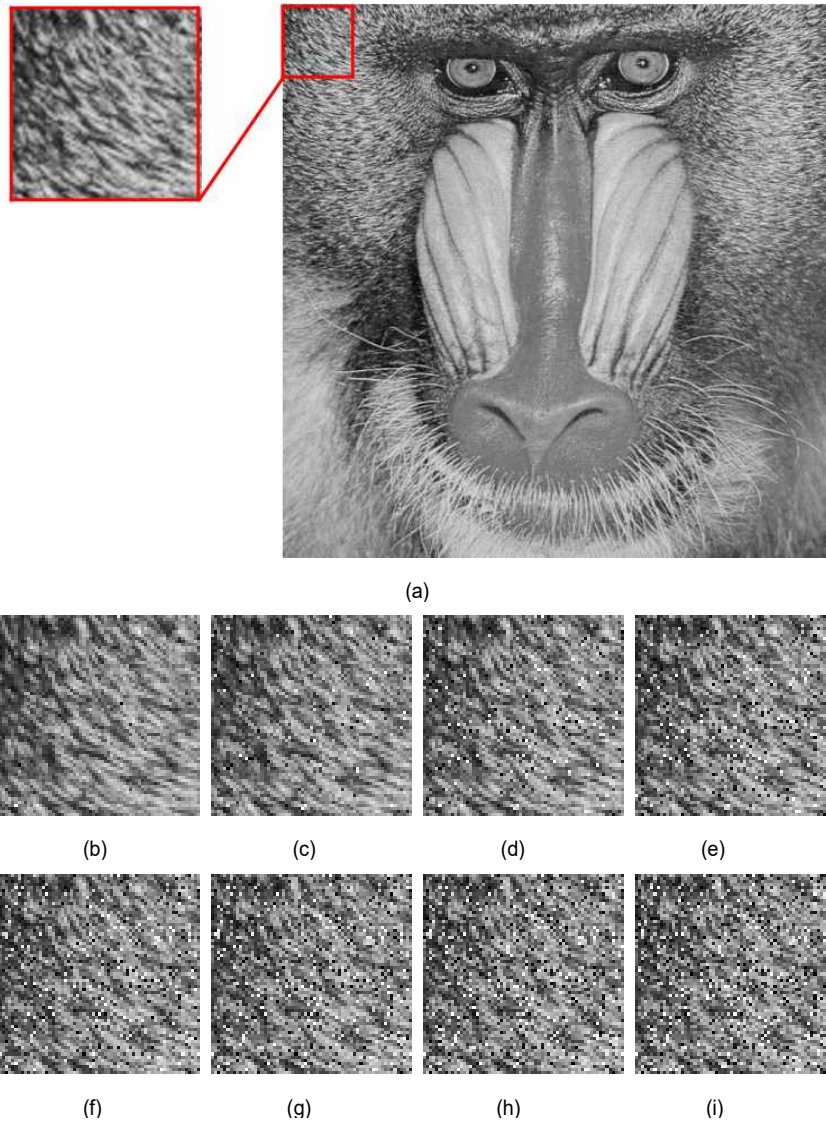


그림 9. "text.bmp" 영상을 삽입한 스테고 영상 (a), 0.1%, 1%, 10%, 20%, 30%, 40%, 50%, 60%, 70% 잡음을 추가한 부분 스테고 영상 (b), (c), (d), (e), (f), (g), (h), (i)

Fig. 9. Stego-image (a) embedding "text.bmp" image, a part of stego-image (b), (c), (d), (e), (f), (g), (h) and (i) with 0.1%, 1%, 10%, 20%, 30%, 40%, 50%, 60% and 70% noise

그림 9 (a)에 잡음 량을 변경시켜가며 비밀 정보를 추출한 결과는 그림 10과 같다. 잡음 량이 증가하여 세부 내용의 식별이 제한이 되더라도 추출 된 정보가 텍스트 영상라고 파악 할 수는 있을 정도로 완전한 정보의 훼손으로부터는 강건함이 보장된다.

2.3 가우시안 잡음에 대한 제안된 방법의 추출 비밀 정보 비교
 평균이 0이고 표준 편차가 1이며 최대 픽셀 값(255)의

5%에 해당하는 값을 가중치로 갖는 가우시안 잡음을 jet.bmp의 커버 영상에 271×180크기의 puppy.bmp를 삽입한 스테고 영상(그림 11참조)으로 삽입하여 비밀 정보가 어떻게 추출되는지에 대해서 실험해 보았다. 사용한 스테고 영상은 블록 크기를 64로 적용한 삽입 비트 고정 PVD이다. 실험 결과 가우시안 잡음의 경우에는 영상의 전체 픽셀에 대해서 적용이 되기 때문에 그림 11 (d)에서 확인 할 수 있는 것처럼 삽입 된 비밀 정보가 심하게 훼손이 된 것을 확인 할 수 있었다.

표 4. 잡음 별 PSNR과 error-ratio
 Table 4. PSNR and error-ratio for noise level

cover image	embedded noise(%)	block size	PSNR (dB)	error pixels	error-ratio (error pixels / total pixels)(%)
baboon.bmp (512×512)	0	8×8	38.8423	0	0
	131(0.1)		37.2684	724	1.4842
	1310(1)		31.4718	1824	3.73924
	13107(10)		22.4759	11788	24.1656
	26214(20)		19.6461	20279	41.5724
	39321(30)		18.0151	26782	54.9036
	52428(40)		16.8854	31796	65.1825
	65536(50)		16.0306	35595	72.9705
	78643(60)		15.3518	38561	79.0508
	91750(70)		14.8037	40821	83.6839

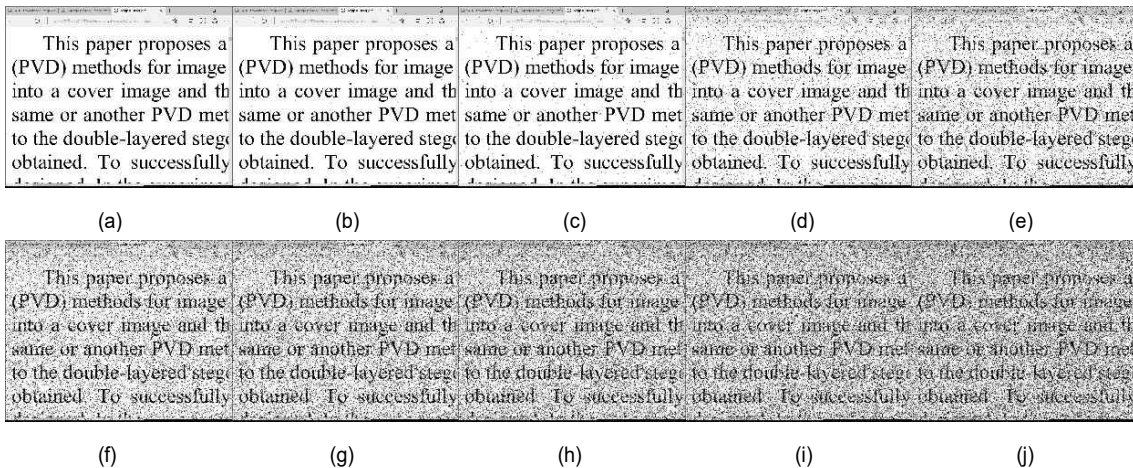


그림 10. 원본 “text.bmp” 영상 (a), 0.1%, 1%, 10%, 20%, 30%, 40%, 50%, 60%, 70% 잡음을 삽입한 스테고 영상에서 추출한 영상 (b), (c), (d), (e), (f), (g), (h), (i), (j)
 Fig. 10. The original “text.bmp” image (a), stego-image (b), (c), (d), (e), (f), (g), (h), (i) and (j) with 0.1%, 1%, 10%, 20%, 30%, 40%, 50%, 60% and 70% noise

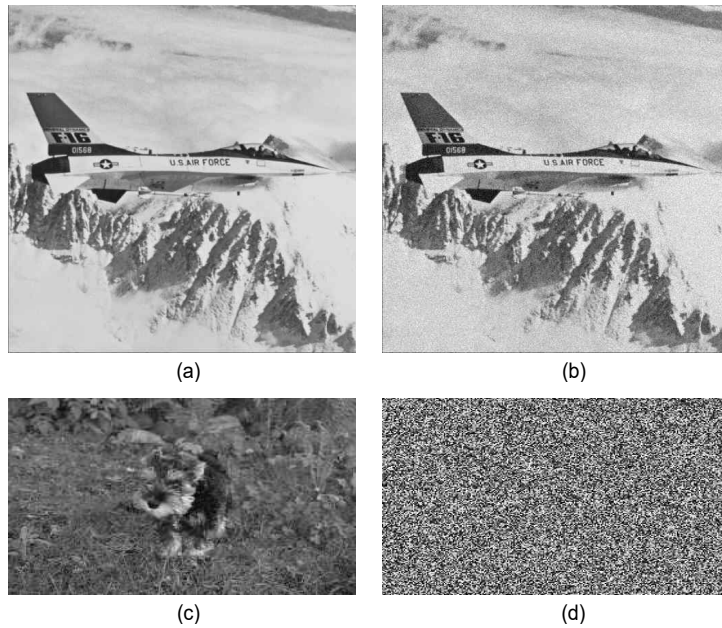


그림 11. 잡음을 삽입하기 전 스테고 영상 (a)와 추출 비밀 정보 (c), 5% 가우시안 잡음을 삽입한 스테고 영상 (b)와 추출 비밀 정보 (d)
 Fig 11. Stego-image (a) before embedding gaussian noise, extracted secret information (c), stego-image (b) after embedding 5% gaussian noise and extracted secret information (d)

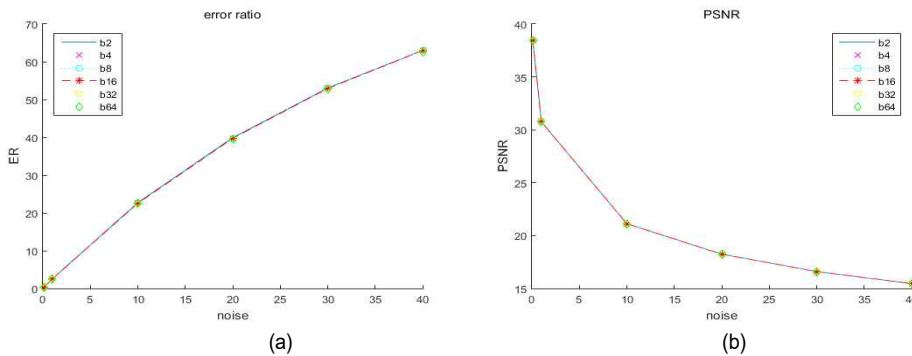


그림 12 . 블록사이즈별 잡음에 대한 error-ratio (a)와 PSNR (b)
 Fig 12. Error-ratio(a) and PSNR(b) of different block sizes for noise

3. 블록 크기별 잡음에 대한 PSNR과 비밀정보 에러 비율 비교

3절에서는 블록 크기와 잡음 량을 바꾸어 가며 에러 비율과 PSNR에 대해서 비교를 하며 실험에는 jet.bmp의 커버 영상에 271×180크기의 puppy.bmp를 삽입한 스테고 영상을 사용한다. 삽입한 비밀 정보의 크기를 $H_s \times W_s$ 라고 하고 삽입한 정보와 추출한 정보가 일치하지 않는 픽셀 수

를 e_p 라고 할 때 에러 비율은 다음의 식 2와 같다. 그림 12의 (a)와 (b)는 블록 크기별로 삽입한 잡음의 량에 대한 에러 비율과 PSNR을 보여주는데 블록 크기가 변하더라도 에러 비율과 PSNR이 크게 차이가 나지 않는 것을 볼 수 있다(세부 사항은 표 5 참조).

$$e_p / ((H_s \times W_s) / 2) \times 100 \quad (2)$$

표 5. 블록 크기별 error-ratio와 PSNR 비교
 Table 5. Comparison of error-ratio and PSNR of different block sizes

cover image	embedded noise(%)	block size	capacity (byte)	PSNR (dB)	error pixel	error-ratio (error pixels / total pixels)(%)
jet (512×512)	52428(40)	2×2	405,470	15.462	30727	62.991
	39321(30)			16.6007	25872	53.0381
	26214(20)			18.2469	19464	39.9016
	13107(10)			21.1203	11075	22.704
	1310(1)			30.7503	1250	2.5625
	131(0.1)			38.4551	129	0.2645
	52428(40)	4×4	399,712	15.4619	30708	62.952
	39321(30)			16.6006	25785	52.8598
	26214(20)			18.2469	19356	39.6802
	13107(10)			21.1203	10977	22.5031
	1310(1)			30.7497	1236	2.5338
	131(0.1)			38.4511	125	0.2563
	52428(40)	8×8	394,816	15.462	30736	63.0094
	39321(30)			16.6007	25849	52.991
	26214(20)			18.247	19349	39.6658
	13107(10)			21.1205	11016	22.583
	1310(1)			30.7515	1246	2.5543
	131(0.1)			38.4617	132	0.2706
	52428(40)	16×16	393,856	15.4619	30711	62.9582
	39321(30)			16.6006	25806	52.9028
	26214(20)			18.2468	19385	39.7396
	13107(10)			21.1201	10992	22.5338
	1310(1)			30.7483	1245	2.5523
	131(0.1)			38.4431	135	0.2768
52428(40)	32×32	393,216	15.4619	30589	62.7081	
39321(30)			16.6006	25690	52.665	
26214(20)			18.2468	19227	39.4157	
13107(10)			21.1201	10902	22.3493	
1310(1)			30.7481	1230	2.5215	
131(0.1)			38.4417	129	0.2645	
52428(40)	64×64	393,216	15.4619	30521	62.5687	
39321(30)			16.6005	25734	52.7552	
26214(20)			18.2467	19285	39.5346	
13107(10)			21.1199	11019	22.5892	
1310(1)			30.7459	1260	2.58303	
131(0.1)			38.4291	136	0.2788	

V. 결 론

PVD는 미세한 잡음이나 오류가 발생하는 경우에도 삽입된 비밀 정보가 정상적인 추출이 불가능하지만 삽입 비트 고정 PVD의 경우에는 미세한 잡음이나 오류의 경우 삽입된 잡음의 정도만이 훼손되고 나머지 정보는 정상적으로 추출 되는 것으로 보아 커버 영상의 일부분에 대해서는 오류의 정도에 관계없이 삽입된 비밀 정보가 정상적으로 보존이 되는 것을 확인할 수 있었다. 때문에 PVD에 비해서 삽입 비트 고정 PVD의 경우가 더 강건하다는 사실을 확인할 수 있었다. 하지만 가우시안 잡음과 같이 잡음의 정도는 미미하더라도 영상의 전반적인 부분에 잡음이 발생하게 되면 삽입 비트 고정 PVD의 경우에도 정상적인 비밀 정보의 추출이 불가능 했다. 또한 블록 크기와 잡음 량에 대해서 에러 비율과 PSNR이 독립적이기 때문에 삽입 용량 측면에서 볼 때 블록 크기가 작을수록 좋다는 것을 알 수 있다. 하지만 서브 블록의 삽입 비트수가 식 (1)에 의해서 정의되어 삽입 비트 수에서 손실이 발생하며 기존의 PVD의 삽입 비트 수보다 삽입 비트 고정 PVD의 경우에 삽입 용량이 감소한다. 그래서 추후 연구로 삽입 비트 고정 PVD의 삽입 용량이 PVD, TPVD, 그리고 OPVD같은 기법들에 비해서 적기 때문에 PVD 삽입 양을 늘리기 위한 연구가 병행되어야 할 것이며 PVD 중첩 스테가노그래피가 좋은 방안이 될 것으로 판단이 된다. 그리고 압축이나 변환 등에 대한 오류에 대해서도 좀 더 강건한 추출이 될 수 있는 방안을 연구해야 할 것이다.

참 고 문 헌 (References)

- [1] H. Kim, "Theoretical Background and Detection Technique of Steganography," *Journal of the Korea Information Security*, Vol. 12, No. 1, pp. 34-47, 2002.
- [2] S. Ji, "A Study of Optimal Image Steganography Based on LSB Techniques," *Journal of the Korea Industrial Information Systems Research*, Vol. 20, No. 3, pp. 29-36, 2015.
- [3] D. C. Wu and W. H. T, "A Steganographic Method for Images by Pixel-Value Differencing," *Pattern Recognition Letters*, Vol. 24, pp. 1613-1626, 2003.
- [4] K. C. Chang, C. P. Chang, P. S. Huang, and T. M. Tu, "A Novel Image Steganographic Method using Tri-way Pixel-Value Differencing," *Journal of Multimedia*, Vol. 3, No. 2, pp. 37-44, 2008.
- [5] C. Balasubramanian, S. Selvakumar, and S. Geetha, "High Payload image Steganography with Reduced Distortion using Octonary Pixel Pairing Scheme," *Multimed Tools Appl*, Vol. 73, pp. 2223-2245, 2014.
- [6] J. Kim and H. Park, "Image Steganography using Layered Pixel-Value Differencing," *Proc. of SPIE*, Tokyo, Japan, 2016.
- [7] Y. Lee, Y. Seo and D. Kim, "Hologram Watermarking using Fresnel Diffraction Model," *Proc. of the Korea Society of Broadcast Engineers Conference*, Vol 19, No. 5, pp. 606-615, 2014.
- [8] W. Sohn, and L. N. T. dung, "A Blind Watermarking Scheme using Singular Vector based on DWT/RDWT/SVD," *Journal of Broadcast Engineering*, Vol 21, No 2, 2016.
- [9] Y. Lee, Y. Seo, and D. Kim, "A Robust Blind Watermarking for Digital Image using DWT according to its Resolution," *Journal of Broadcasting Engineering*, Vol 20, No 6, pp 888-900, 2015.
- [10] S. Youssef, A. A. Elfarag, and R. Raouf, "A Robust Steganography Model using Wavelet-based Block-Partition Modification," *International Journal of Computer Science & Information Technology*, Vol 3, No 4, pp. 15-28, 2011.
- [11] S. Singh, and T. J. Siddiqui, "A Security Enhanced Robust Steganography Algorithm for Data Hiding," *International Journal of Computer Science Issues*, Vol 9, No 1, 2012.

저 자 소 개



김 재 영

- 2012년 : 부경대학교 전자컴퓨터정보통신공학부 공학사
- 2016년 ~ 현재 : 부경대학교 일반대학원 석사과정
- ORCID : <http://orcid.org/0000-0003-2348-3626>
- 주관심분야 : 스테가노그래피



박 한 훈

- 2000년 : 한양대학교 전자통신전파공학과 공학사
- 2002년 : 한양대학교 대학원 전자통신전파공학과 공학석사
- 2007년 : 한양대학교 대학원 전자통신전파공학과 공학박사
- 2008년 ~ 2011년 : NHK방송기술연구소 박사후연구원
- 2012년 ~ 현재 : 부경대학교 전자공학과 부교수
- ORCID : <http://orcid.org/0000-0002-6968-4565>
- 주관심분야 : 증강현실, 인간컴퓨터상호작용, 3차원 영상처리/비전 등



박 종 일

- 1987년 : 서울대학교 전자공학과 공학사
- 1989년 : 서울대학교 전자공학과 공학석사
- 1995년 : 서울대학교 전자공학과 공학박사
- 1992년 ~ 1994년 : 일본 NHK방송기술연구소 객원연구원
- 1995년 ~ 1996년 : 한국방송개발원 선임연구원
- 1996년 ~ 1999년 : 일본 ATR지능영상통신연구소 연구원
- 1999년 ~ 현재 : 한양대학교 공과대학 컴퓨터공학부 교수
- ORCID : <http://orcid.org/0000-0003-1000-4067>
- 주관심분야 : 증강현실, 계산사진학, 3차원 컴퓨터비전, 인간컴퓨터상호작용