격자 기반의 가역적 데이터 은닉 기법

김영식* · 임대운**

1. 서 론

가역적 데이터 은닉은 원본 이미지에 영향을 주지 않은 채로 임의의 데이터를 숨기는 기술이다. 가역성은 군사용 영상이나 의료용 영상과 같은 특정한 응용에서는 매우 중요한 요소이다. 이런 응용에서는 원본 이미지를 기반으로 정확한 판정을 내려야 하기 때문에 원본 이미지를 손상시키지 않고 보존하는 것이 매우 중요하다. 현재까지 많은 가역적 데이터 은닉 기술이 제안되었다 [1]-[4]. 일반적으로 두 개의 연속적인 화소 사이의 차이를 사용해서 추가적인 은닉 정보를 주입하는 새로운 LSB 데이터를 생성하게 된다.

최근에 Zhang은 가역적인 데이터 은닉 기법을 제시하였다 [5]. 이 기법에서는 스트림 암호와 같은 호모몰픽 암호화 기법에 응용될 수 있다. 이 방식에서 데이터를 은닉하기 위해서 암호화된 이미지 픽셀이 s^2개의 화소로 구성된 여러 개의 그룹으로 나눠지게 된다. 데이터 은닉키를 사용해서 한 그룹의 화소들이 임의적으로 두 개의 집합 S_0과 S_1으로 나누어진다. Zhang이 제안한 방식에서는 S_0 또는 S_1에서의 화소의 마지막 세 LSB값이 각각 은닉 비트에 따라서 0에서 1 또는 1에서 0으로 변환이 된다.

원본 이미지에 은닉된 데이터를 추출하기 위해서 데이터 은닉 키를 가진 데이터 은닉자는 데이터가 은닉된 암호화된 이미지를 복호화한 후에 다시 한 번 s^2개의 화소로 구성된 두 개의 화소 집합 S_0와 S_1을 동일하게 구분해야 한다. 그런 후에 두 개의 가설 그룹 H_0와 H_1으로 구분한다. 이때 가설 그룹 H_0는 집합 S_0에 속한 모든 픽셀의 마지막 세 LSB 값을 0에서 1 또는 1에서 0으로 변환을 시키고 가설 그룹 H_1는 집합 S_1에 속한 모든 화소의 마지막 세 LSB 값에 대해 동일한 변환을 적용시킨다. 실제 은닉된 데이터가 0이냐 1이냐에 따라 H_0 또는 H_1 둘 중 하나가 원본 이미지와 동일한 화소 데이터를 갖게 된다. 이 때 판정은 H_0과 H_1의 각 화소의 공간 상관 특성을 계산해서 차이가 적은 가설 집합을 참인 가설로 판정하고 이를 기반으로 은닉된 데이터가 0인지 1인지를 알아내면서 동시에 원본 이미지를 복원하게 된다.

이 논문에서는 Zhang의 방식은 개선시킨 두 가지 새로운 가역적 데이터 은닉 기법을 제안한다. 제안된 방식에서는 두 개의 격자 패턴에 있는 화

※ 교신저자(Corresponding Author) : 임대운, 주소 : 서울특별시 중구 필동로 1길 30, 동국대학교 정보통신공학과, 신공학관 10110호, 전화: 02-2260-8923, FAX: 02-2285-3343, E-mail : daewoonlim@gmail.com
* 조선대학교 정보통신공학과
(E-mail : mypurist@gmail.com)
** 동국대학교 정보통신공학과
본 연구는 본 연구는 한국연구재단 중견연구자지원사업(과제번호 2012-0005196)과 일반연구자지원사업(과제번호 2010-0002355)의 지원을 받아 수행되었음.

소들만 값을 변환할 수 있도록 한다. 격자 상의 패턴들은 Zhang의 방식에서와 같이 두 개의 집합으로 데이터 은닉키에 따라 임의로 구분이 되고 두 개의 집합 중 하나의 집합에 속한 화소만이 값이 변환이 되도록 한다. 격자 상의 화소로 변환 대상을 한정함으로써 데이터 왜곡을 감소시킬 수가 있으며 동시에 검출 오류 확률을 줄일 수가 있다.

이 논문은 다음과 같이 구성된다. 2장에서는 Zhang의 방식을 자세히 설명한다. 그런 후에 3장에서는 새로 제안하는 방법을 설명할 것이다. 4장에서는 새로 제안한 방식의 특성을 분석한 후에 마지막으로 5장에서 결론을 맺을 것이다.

2. Zhang의 가역적 데이터 은닉 기술

이 장에서는 Zhang이 제안한 데이터 은닉 기법에 대해서 자세히 설명할 것이다. Zhang의 기법에서는 두 명의 사용자가 존재한다. 한 명의 사용자는 원본 이미지를 소유한 자로서 암호화를 위한 비밀키를 사용해서 이미지를 암호화시킨다. 이때 암호화 방식은 호모몰픽 성질을 만족하는 암호화여야 하고 대표적으로 동기적 스트림 암호가 이에 해당된다. 동기적 스트림 암호는 주어진 평문과 비밀키로부터 생성된 랜덤 비트 사이에 XOR 연산을 통해서 암호화를 수행한다.

암호화된 이미지가 주어지면 또 다른 사용자인 데이터 은닉자는 데이터 은닉을 위한 키를 가지고서 암호화된 이미지에 은닉을 시도한다. 이 때 암호화 방식 자체가 갖고 있는 호모몰픽 성질로 인해서 암호화 이후에 은닉을 수행하더라도 복호 후에 은닉된 정보를 추출하는 것이 가능해 진다. 은닉을 위해서 먼저 이미지 화소가 s^2개의 화소로 구성된 그룹들로 나누어지고 각 그룹에는 한 비트의 은닉 정보가 숨겨지게 된다. 각 그룹들은 다시 은닉키를 이용해서 임의의 두 개의 집합 S_0과 S_1로 나눠진다. 이 때 은닉 비트가 0이면 S_0집합의 화소만을 변환시키고 은닉 비트가 1이면 S_1집합의 화소만을 변환시킨다. 변환은 각 화소의 마지막 세 개의 LSB에 대해서 일어나고, 변환이 일어날 때 세 개의 LSB 각 비트는 0은 1로 1은 0으로 Inversion 변환을 하게 된다.

데이터 추출을 위해서는 암호화된 이미지를 먼저 복호화해야 한다. 이미지를 암호화했던 사용자가 데이터가 은닉된 암호화된 이미지를 복구하게 되면, 데이터 은닉자는 숨겨진 정보를 다시 추출하는 것이 가능하다. 이 때 복호화된 이미지를 다시 s^2 개의 화소로 구성된 그룹으로 동일하게 구분되고, 각 그룹은 동일한 데이터 은닉키를 사용해서 다시 임의의 S_0과 S_1로 동일하게 나누어진다. 이 때 은닉된 데이터가 0이냐 1이냐에 따라 두 개의 가설 그룹 H_0과 H_1을 생성한다. H_i $(i=0,1)$는 각 그룹의 화소 중에서 S_i에 속한 화소만을 마지막 세 개의 LSB 각 비트에 대한 Inversion 변환을 다시 수행하게 된다. 만일 실제로 은닉된 데이터가 i라면, S_i에 속한 화소가 은닉을 위해 Inversion 변환이 적용되었을 것이므로, 다시 한 번 Inversion 변환을 수행함으로써 본래의 화소 데이터로 복원이 된다. 그러나 S_{1-i}에 속한 화소들은 데이터 은닉 시에 변환되지 않았으므로 결국 가설집합 H_{1-i}에 속한 모든 화소들은 모두 마지막 세 개의 LSB 비트가 Inversion 변환이 적용이 된 상태가 된다. 다시 말해 정확한 가설 집합 H_i는 왜곡이 최소화되어 본래의 영상으로 회복되고 반면에 틀린 가설 집합 H_{1-i}는 왜곡이 최대화된다. 이러한 왜곡은 이미지 자체의 공간 상관 특성을 통해서 측정할 수 있다. 일반적으로

영상 이미지는 주변 화소와 연속성을 갖고 유사한 영상 값을 갖게 되는데, 왜곡이 일어나게 되면 주변 화소 사이의 값의 변화가 커진다. 이를 측정함으로써 왜곡의 없는 가설 집합과 왜곡이 최대화된 가설 집합을 다음과 같이 측정할 수 있다.

$$f_i = \sum_{u=2v=2}^{s-1\,s-1} \left| p_{u,v} - \frac{p_{u-1,v} + p_{u,v-1} + p_{u+1,v} + p_{u,v+1}}{4} \right| \quad (1)$$

이 때 (1)에서의 값은 중심 값과 주변 네 개의 화소의 평균 값 가의 차이를 누적시킨다. 왜곡이 없는 영상은 이 차이가 최소화될 것이고 왜곡이 최대화된 영상은 이 차이가 최대화될 것으로 가정된다. 따라서 두 개의 가설 집합에 대한 측정 값 f_0과 f_1의 크기를 비교해서 만일 $f_0 < f_1$이면 H_0가 참인 가설 집합으로 판정되고 그 반대이면 H_1이 참인 가설 집합으로 판정된다. 따라서 참인 가설 집합을 앎으로써 은닉된 데이터 값을 알게 되고 본래의 영상 이미지 데이터도 복구할 수가 있다.

3. 개선된 가역적 데이터 은닉 기법

이 장에서는 Zhang이 제안한 방식을 분석한 후에 두 개의 개선된 기법을 제안한다. 새로 제안된 방식은 더 높은 PSNR을 가지며 Zhang의 방식보다 은닉된 비트를 추출할 때 오류 확률이 더 작다는 것을 보일 것이다.

우선 Zhang이 제안한 방식에서는 두 가지 문제가 존재한다. 첫 째는 암호화된 이미지에서 절반의 화소가 은닉 데이터에 따라서 왜곡이 일어나게 된다. 이러한 왜곡은 결국 은닉된 데이터를 추출하고 나면 완전히 제거될 수 있지만, 왜곡이 커지면 은닉된 데이터를 발견할 확률이 더 커지게 된다. 두 번째는 은닉된 데이터를 복구할 때 두 개의 가설 집합 H_0과 H_1사이의 공간 상관 특성 사이에서의 차이 값이 랜덤한 선택으로 인해서 최대화되지 못하게 된다. 그 결과 오류의 확률이 결코 작지 않게 되는 문제가 있다.

3.1 개선된 데이터 은닉 기법

그림 1에서 나타낸 제안된 데이터 은닉 기법은 그림 2와 같은 격자 패턴에 기반을 둔다.

제안된 가역적 데이터 은닉 방식에서는 홀수 $s = 2n+1$ 를 사용하고, 원본 이미지는 s^2 개의 화소를 갖는 여러 개의 그룹으로 나눠진다. 각 그룹에서의 $s \times s$ 화소 중에서, 가장 외각에 있는 화소들은 변환되지 않는다. 각 그룹에서의 화소를 x축의 경우 $0 \le i \le s-1$ 로 y축의 경우 $0 \le j \le s-1$로 인덱스를 부여한다고 가정하자. 그러면 격자 1에 대해서 $i = 2k+1$ ($0 \le k \le (s-3)/2$)과 $j = 2l+1$ ($0 \le l \le (s-3)/2$)에 있는 화소만 선택된다. 이 경우에 변환될 수 있는 화소는 n^2가 된다. 격자 2의 경우에 격자 1에서 선택된 화소에

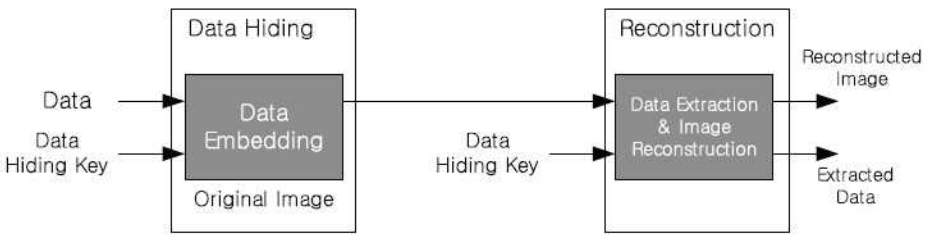

그림 1. 제안된 데이터 은닉 방식

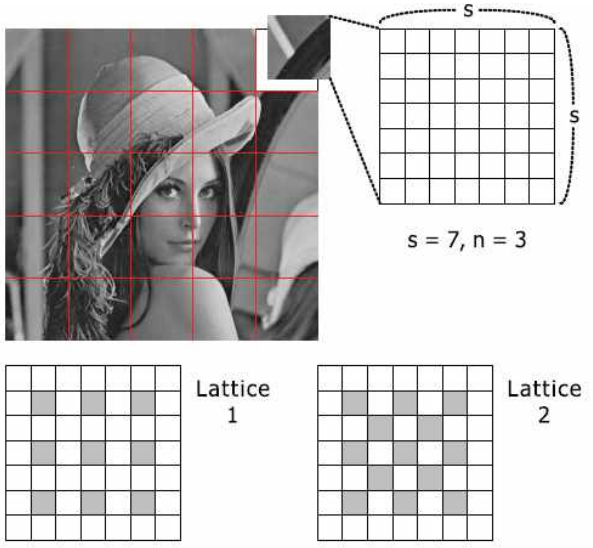

그림 2. 개선된 방식에서 사용하는 격자 패턴. 이 때 그룹의 크기는 $s=2n+1$로 홀수 값을 갖는다.

더하여서 $i=2k$ $(i \le k \le (s-3)/2)$와 $j=2l$ $(1 \le l \le (s-3)/2$ $)$에 위치한 화소 역시 선택된다. 따라서 $n^2+(n-1)^2$ 개의 화소가 변환될 수 있다. 그림 2에서는 격자 1과 격자 2의 예를 $s=7$과 $n=3$ 을 사용해서 보여주고 있다. 두 개의 격자 모두 데이터 은닉은 각각의 중앙 화소에서만 수행이 된다. 변환되는 화소는 언제나 고정된 화소로 불러 쌓여 있게 된다. 따라서 주변 값의 평균은 언제나 원본 이미지를 기반으로 한 평균값과 동일하게 된다.

실제로 변환되는 화소를 선택하기 위해서 다시 격자상의 n^2 또는 $n^2+(n-1)^2$ 개의 원소를 두 개의 집합 S_0과 S_1로 데이터 은닉키를 사용해서 임의적으로 구분하게 된다. 한 비트의 데이터를 은닉하기 위해서 S_0 또는 S_1 상의 화소에 대해서만 변환이 일어난다. 이 때 선택된 집합 S_i 상의 화소들에 대해서 격자상에 있는 중앙 화소는 격자 상에 있지 않은 상하좌우 화소의 값에 기반을 해서 변환이 된다. 다시 말해 격자 상의 화소 $p_{i,j}$의 상하좌우 화소의 합 $c_{i,j}=p_{i-1,j}+p_{i+1,j}+p_{i,j-1}+p_{i,j+1}$를 사용해서 이 값이 정해진 임계값 T와 비교해서 다음과 같이 강도(intensity) I 만큼의 변환이 일어난다.

$$p'_{i,j}=\begin{cases} p_{i,j}-I, & \text{if } c_{i,j}>T \\ p_{i,j}+I, & \text{otherwise} \end{cases}$$

이 때 적절한 임계값 T는 데이터 은닉자가 화소의 클리핑을 막도록 실험을 통해서 선택할 수 있다.

3.2 은닉된 데이터의 복원

은닉된 데이터를 복원하기 위해서 사용자는 동일한 데이터키를 사용해서 S_0와 S_1를 다시 생성하게 되고 다시 두 개의 가설 집합 H_0와 H_1를 격자를 고려해서 동일하게 생성하게 된다. 그리고 각 가설 집합 H_0와 H_1에 대해서 다음과 같은 값을 계산하여 은닉된 데이터를 판정하게 된다. 먼저 격자 1의 경우 다음과 같은 값을 각 가설 집합에 대해서 구하게 된다.

$$f=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}|p_{2i+1,2j+1}-m_{i,j}|$$

여기에서 $m_{i,j}=(p_{2i,2j+1}+p_{2i+2,2j+1}+p_{2i+1,2j}+p_{2i+1,2j+2})/4$ 이다. 그리고 격자 2의 경우 다음과 같은 값을 각 가설 집합에 대해서 구하게 된다.

$$f=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}|p_{2i+1,2j+1}-m_{i,j}|+\sum_{i=1}^{n-1}\sum_{j=1}^{n-1}|p_{2i,2j}-l_{i,j}|$$

여기에서 $m_{i,j}$는 격자 1에서와 동일하고 $l_{i,j}=(p_{2i-1,2j}+p_{2i+1,2j}+p_{2i,2j-1}+p_{2i,2j+1})/4$이다. 만일 $f_i<f_{1-i}$ 인 경우에는 i가 바로 은닉된 데이터로 간주된다.

4. 제안된 가역적 데이터 은닉 기법의 성능 분석

4.1 제안된 가역적 데이터 은닉 기법의 PSNR

먼저 새로 제안한 방식의 PSNR을 계산해 보도록 하자. 변화가 될 화소들은 강도 I에 의해서 영향을 받게 된다. 따라서 평균 에러의 에너지는 다음과 같이 계산될 수 있다.

$$E = I^2$$

격자 1을 사용하는 방식에서는 $s^2=(2n+1)^2$ 개의 화소 중에서 $n^2/2$ 개의 화소만이 변화가 일어나게 된다. 따라서 PSNR을 다음과 같이 주어지게 된다.

$$PSNR = 10\log_{10}\frac{2\times 255^2(2n+1)^2}{En^2} = 51.44\text{dB} + 20\log_{10}\left[\frac{1}{I^2}\left(2+\frac{1}{n}\right)\right]$$

만일 $I<9$라면 (5)에서의 두 번째 항은 -13.06dB보다 더 크다. 따라서 격자 1에 기반을 둔 제안된 방식은 PSNR이 Zhang의 것 보다 더 크게 된다. 격자 2를 사용하는 경우에는 $s^2=(2n+1)^2$ 개의 화소 중에서 $(n^2+(n-1)^2)/2$ 개의 화소만이 변화를 하게 된다. 그래서 PSNR은 다음과 같이 계산할 수 있다.

$$PSNR = 10\log_{10}\frac{2\times 255^2(2n+1)^2}{E(n^2+(n-1)^2)} = 51.14\text{dB} + 10\log_{10}\left[\frac{1}{I^2}\left(2+\frac{8n-1}{2n^2-2n+1}\right)\right]$$

따라서 $I\le 6$이면 두 번째 항은 -12.55 dB보다 더 크게 되고 따라서 제안된 방식의 PSNR은 Zhang의 것 보다 더 크게 된다.

4.2 제안된 가역적 데이터 은닉 기법의 BER 성능

제안된 방식에서의 데이터 추출시의 BER은 그림 3와 그림 4에서 Zhang의 것과 비교하여 도시하였다. 이 때 각각의 원본 이미지는 흑백의 Lena와 Baboon을 각각 사용하였다. 제안된 방식의 BER은 강도 I와 임계값 T 그리고 데이터 은닉키에 의존하게 된다. 그림 3과 그림 4에서의 결과들은 20개의 서로 다른 데이터 은닉키로부터 얻은

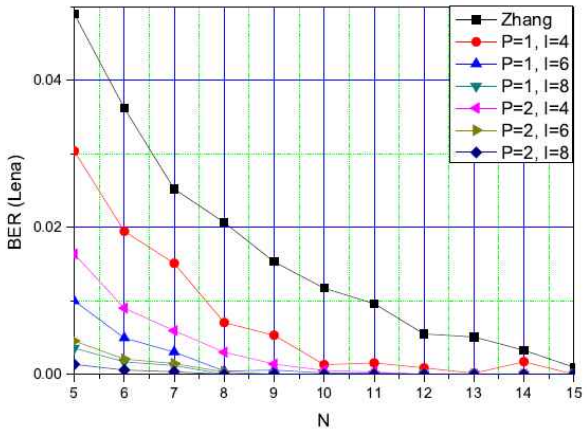

그림 3. Lena를 사용했을 경우에 제안된 방식과 Zhang의 방식의 BER 특성 비교. 여기서 $P=1$은 격자 1을 의미하고 $P=2$는 격자 2를 의미한다. 그리고 강도 I는 4, 6, 8의 값에 대해 시뮬레이션 하였다.

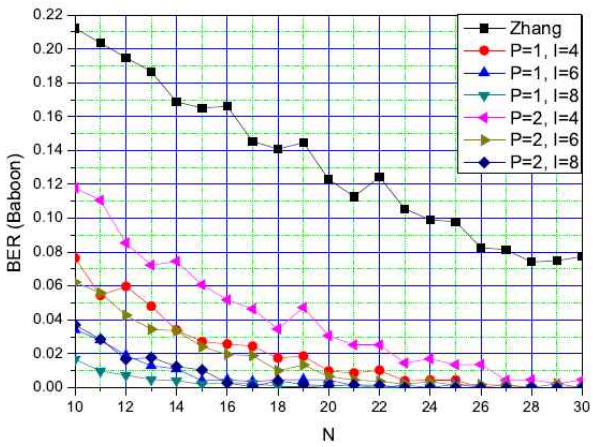

그림 4. Baboon를 사용했을 경우에 제안된 방식과 Zhang의 방식의 BER 특성 비교. 여기서 $P=1$은 격자 1을 의미하고 $P=2$는 격자 2를 의미한다. 그리고 강도 I는 4, 6, 8의 값에 대해 시뮬레이션 하였다.

BER값의 평균을 도시한 것이다. 임계값의 영향은 그리 크지 않지만 강도 I와 비교해 너무 큰 값을 사용하는 경우에 클리핑 등으로 인해 BER 특성이 열화된다. 반면에 PSNR은 I가 커질수록 더 작아지게 된다. BER은 s가 커질수록 더 작아져 0으로 수렴하지만 s가 커지게 되면 은닉되는 데이터의 양이 줄어들게 된다.

4.3 제안된 가역적 데이터 은닉 기법의 보안 특성

제안된 방식에서 왜곡이 일어나는 비트의 수는 Zhang의 것에서 왜곡이 일어나는 비트 수에 비교하여 격자에 따라 각각 $n^2/(2n+1)^2$ 또는 $(n^2+(n-1)^2)/(2n+1)^2$ 배 더 작게 된다. 따라서 특정 I 범위 내에서 Zhang의 것보다 PSNR이 더 크게 되고 따라서 은닉 데이터의 존재가 검출될 가능성이 Zhang의 것보다 더 작다.

여기에 더하여 s가 알려져 있다면 공격자가 정확히 동일한 S_0와 S_1을 은닉키 없이 만들어낼 확률은 격자에 따라 각각 $1/\binom{n^2}{n^2/2}$ 또는 $1/\binom{n^2+(n-1)^2}{(n^2+(n-1)^2)/2}$ 가 되어, 충분히 큰 n에 대해서 매우 작은 확률을 갖게 된다. 예를 들어 $n=5$인 경우 격자 1의 경우 정확히 S_0과 S_1을 나눌 확률이 1/5,200,300이 되고 격자 2의 경우는 $1/2{,}69\times10^{11}$ 이 된다. 따라서 데이터 은닉을 알아낸다고 하더라도 은닉키를 알지 못하면 정확한 은닉 데이터를 알아낼 확률이 매우 작음을 알 수 잇다.

5. 결 론

이 논문에서는 격자에 기반을 둔 새로운 가역적 데이터 은닉 기법을 제안하였다. 새로 제안한 방식은 기존의 방식과 비교해서 PSNR도 더 크고 오류 확률도 더 작음을 알 수 있다. 제안된 방식에서 원본 이미지는 은닉 데이터를 성공적으로 추출한 후에는 어떠한 왜곡도 없이 얻을 수가 있다. 더 나아가 은닉 데이터의 존재를 검출하는 것 역시 기존의 방식에 비교했을 때 더 작음을 알 수 있다.

참 고 문 헌

[1] J. Tian, “Reversible data embedding using a difference expansion,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890 - 896, Aug. 2003.

[2] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless generalized-LSB data embedding,” *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253 - 266, Feb. 2005.

[3] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” *IEEE Trans. Circuits Syst., Video Technol.*, vol. 16, no. 3, pp. 354 - 362, 2006.

[4] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, “Reversible image watermarking using interpolation technique,” *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 1, pp. 187 - 193, 2010.

[5] X. Zhang, “Reversible data hiding in encrypted image,” *IEEE. Signal. Processing Lett.*, vol. 18, no. 4, pp. 255 - 258, Apr. 2011. B. von Solms and D. Naccache, "On blind signatures and perfect crimes", Computers and Security, Vol. 11, No. 6, pp581-583, 1992.

김 영 식

• 2001년 2월 서울대학교 전기공학부 공학사
• 2003년 2월 서울대학교 전기·컴퓨터공학부 석사
• 2007년 2월 서울대학교 전기·컴퓨터공학부 박사
• 2007년 3월~2010년 8월 삼성전자 책임연구원
• 2010년 9월~현재 조선대학교 정보통신공학과, 조교수
• 관심분야 : 암호학, 정보보호, 오류정정부호, 정보이론

임 대 운

• 1994년 2월 한국과학기술원 전기및전자공학과 학사
• 1997년 2월 한국과학기술원 전기및전자공학과 석사
• 2006년 8월 서울대학교 전기·컴퓨터공학부 박사
• 1995년 9월~2002년 8월 LS산전(주) 중앙 연구소 선임 연구원
• 2006년 9월~현재 동국대학교 컴퓨터정보통신공학부 조교수
• 관심분야 : OFDM, 부호 이론, 시공간 부호