Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.3, June 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.3.359

유한 체 기반의 개선된 가역 비밀이미지 공유 기법*

김 동 현,† 김 정 준, 유 기 영‡
경북대학교

An Improved Reversible Secret Image Sharing Scheme based on $GF(2^8)$*

Dong-hyun Kim,† Jung-joon Kim, Kee-young Yoo‡
Kyungpook University

요 약

2010년, Lin과 Chan은 가역 비밀이미지 공유(reversible secret image sharing) 기법을 최초로 제안했다. 이 기법의 장점은 쉐도우 이미지(shadow images)의 왜곡 비율(distortion ratio)이 작고, 비밀이미지의 삽입량(embedding capacity)이 기존의 기법들에 비해 높으며, 가역(reversible)이 가능하다. 그러나 그들의 기법은 몇 가지 문제점들이 존재한다. 첫째, 나머지 연산(modular operation)에 사용하는 소수 m에 의하여 전체 참가자들의 수가 제한된다. 둘째, 비밀 공유 과정 내 양자화 값(quantized value)과 다항식의 결과 값의 덧셈 연산에서 오버플로우(overflow)가 발생한다. 마지막으로, 다항식 최고차항의 계수가 0이 되어 $t-1$명의 참가자로도 비밀데이터 접근이 가능해지는 문제점을 가진다.

본 논문에서는 Lin과 Chan이 제안한 기법의 문제점을 해결하는 동시에 쉐도우 이미지의 왜곡 비율이 작고 비밀이미지의 삽입량을 향상시키는 기법을 제안한다. $GF(2^8)$상에서의 다항식 연산을 통해 전체 참가자 수의 제한과 오버플로우 문제를 해결하고, 다항식 최고차항의 계수 중 MSB 4-비트를 고정하는 방법을 적용하여 계수가 0이 될 수 있는 문제점을 해결한다. 실험결과에서는 Lin과 Chan의 기법에서 *PSNR*과 삽입량이 서로 반비례하지만 제안한 기법의 경우 삽입량이 증가하더라도 *PSNR*은 45dB 이상으로 유지됨을 알 수 있다.

ABSTRACT

Lin and Chan proposed a reversible secret image sharing scheme in 2010. The advantages of their scheme are as follows: the low distortion ratio, high embedding capacity of shadow images and usage of the reversible. However, their scheme has some problems. First, the number of participants is limited because of modulus prime number m. Second, the overflow can be occurred by additional operations (quantized value and the result value of polynomial) in the secret sharing procedure. Finally, if the coefficient of $(t-1)$th degree polynomial become zero, $(t-1)$ participants can access secret data.

In this paper, an improved reversible secret image sharing scheme which solves the problems of Lin and Chan's scheme while provides the low distortion ratio and high embedding capacity is proposed. The proposed scheme solves the problems that are a limit of a total number of participants, and occurrence of overflow by new polynomial operation over $GF(2^8)$. Also, it solve problem that the coefficient of (t−1)th degree polynomial become zero by fixed MSB 4-bit constant. In the experimental results, PSNR of their scheme is decreased with the increase of embedding capacity. However, even if the embedding capacity increase, PSNR value of about 45dB or more is maintained uniformly in the proposed scheme.

Keywords: Reversible Secret Image Sharing, Galois Field, Steganography, PSNR, Embedding Capacity

접수일(2013년 2월 26일), 수정일(2013년 5월 16일), 게재확정일(2013년 5월 21일)
* 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업입니다. (No. 2012-008348), 이 논문은 2012학년도 경북대학교 학술연구비에 의하여 연구되었음
† 주저자, pari001@infosec.knu.ac.kr
‡ 교신저자, yook@knu.ac.kr(Corresponding author)

I. 서 론

비밀 정보에 접근 가능한 비밀 키가 1개일 경우에는 소유자(owner)의 실수로 인한 분실 또는 사망하한다면 비밀 정보에 접근할 수 없는 문제가 발생하게 된다. 이러한 문제점을 해결하기 위해서 비밀 공유 기법이 제안되었다. 비밀 공유 기법은 비밀 정보에 접근할 수 있는 비밀 키가 단일이 아닌 다수의 인가된 참가자들의 키로 구성되어있다. 즉, n명의 참가자들에게 1개의 비밀 키를 조각으로 나누어 분배할 경우 적어도 t명 이상의 참가자가 소유한 키 조각들이 모이게 되면 원래의 비밀 키를 재구성할 수 있다. 반드시 n명의 참가자 모두가 모이지 않더라도 비밀 키를 복원할 수 있기 때문에 기존 단일 비밀 키의 문제점을 해결할 수 있다.

최초의 비밀 공유는 Blackey[1]와 Shamir[2]가 제안한 (t,n)-threshold 기법이고, 비밀 공유 과정은 다음과 같다. 기본 구성은 비밀정보 S를 참가자 n명에게 나누어 분배한다. 그리고 이 기법은 n명의 구성원 중 적어도 t명 이상의 구성원이 모여야만 비밀정보 S에 접근이 가능하다. (단, $t \leq n$)

2002년, Shamir의 (t,n)-threshold 기법을 이미지에 적용 시킨 Thien과 Lin[3]은 비밀이미지 공유 기법을 최초로 제안했다. 이들이 제안한 기법은 다음과 같다. 비밀이미지는 $1/t$의 크기를 가지는 n개의 쉐도우(shadow) 이미지를 생성시켜 분배자가 참가자에게 분배하는 쉐도우 이미지의 저장 공간을 줄이고, 쉐도우 이미지 전송 시 시간 단축의 성과를 얻었다. 하지만 이 기법은 의미 없는(meanless) 이미지의 생성으로 인하여 비밀이미지 공유에서는 효율적이지 못하였다. 하지만 그들은 2003년[4]에 의미 있는(meaningful) 이미지가 생성되도록 개선된 기법을 제안하였다.

Lin 등[12]은 커버(cover) 이미지 내에 비밀이미지를 삽입하기 위해 나머지 연산(modulo operation)을 이용한 비밀이미지 공유 기법을 제안하였다. 이 기법에서는 각 참가자들은 의미 있는 쉐도우 이미지를 분배하고, 이전 기법들에 비해서 왜곡이 작은 쉐도우 이미지를 얻었다.

최근 연구 동향은 의미 없는 이미지의 경우 공격자로부터 의심을 받거나 공격을 받을 수 있기 때문에 의미 있는 비밀이미지 공유 기법을 중심으로 활발한 연구가 진행 중이다[4-15]. 하지만 의미 있는 비밀이미지 공유 기법에만 제한되지 않고 가역 비밀이미지 공유 기법으로 병행되는 연구가 많이 진행 중에 있다[9,13-15].

2010년, Lin과 Chan[13]은 n명의 참가자들 중 선택된 t명의 참가자들로부터 획득한 쉐도우 이미지를 이용해 비밀이미지를 복원하는 동시에 커버 이미지를 완벽하게 복원하는 가역 비밀이미지 공유 기법을 제안하였다. 이 기법은 기존의 비밀이미지 공유 기법에 비해 쉐도우 이미지의 왜곡이 작고, 삽입량이 많은 장점을 가진다. 하지만 이 기법에는 오버플로우가 발생하고, 다항식의 최고차 항의 계수가 0이 되는 문제점과 이미지의 심한 왜곡문제로 전체 참가자 수의 증가가 제한되는 문제점을 가진다.

최근 2011년에는 Lin과 Wang[14]은 기존의 Lin과 Chan에서 나머지 연산에서 2^{α}를 이용하여 커버 이미지 정보를 상수항에 삽입하는 기법을 제안하였다. 이 기법에서는 오버플로우 문제를 해결하는 동시에 이미지 왜곡을 4dB정도 감소시킨다. 하지만 이 기법 역시 참가자의 수가 증가하면 이미지의 왜곡이 심해져서 참가자의 수가 제한되는 문제점이 있다.

이들의 기법에서 발생하는 문제들을 해결하는 동시에 쉐도우 이미지의 왜곡 비율이 작으며, 이미지에 삽입량을 향상시키는 기법을 제안한다. $GF(2^8)$를 기반으로 한 새로운 다항식을 구성하여 참가자 수의 제한 및 오버플로우가 발생하는 문제점을 해결한다. 그리고 다항식 최고차 항의 계수가 0이 되는 문제점을 MSB 4-비트로 고정함으로써 해결한다. 실험 결과에서는 Lin과 Chan의 기법에서 비밀 정보 삽입량이 증가할수록 *PSNR*은 감소하지만 제안한 기법의 경우 비밀 정보 삽입량이 증가하더라도 쉐도우 이미지의 *PSNR*은 45dB 정도를 유지한다.

본 논문의 구성은 다음과 같다. 2장에서는 유한 체와 Lagrange 보간법(interpolation), 그리고 Lin과 Chan의 가역 비밀이미지 공유 기법에 대해서 간략히 살펴보고, 3장에서는 제안하는 기법의 비밀 공유 과정과 비밀 복원 과정에 대해서 자세히 살펴본다. 4장에서는 두 기법에 대한 실험 결과를 분석하고, 5장에서는 결론을 도출한다.

II. 관련연구

2.1 유한 체(Galois Field)

일반적으로 컴퓨터 내에서 사용되는 비트 연산(bit operation)을 수학적으로 표현하기 위해 유한 체를

사용하고, 특히 곱셈(multiplication)과 나머지(modulus) 연산에 대해 매우 효율적이다. 이러한 유한 체는 암호학의 발전과 함께 여러 분야에서 널리 사용되어왔다.[16,17]

체(field) 내의 모든 원소에 대한 개수가 유한(finite)일 경우 유한 체(finite field) 또는 Galois 체(Galois field)로 정의하고, F_{p^n} 또는 $GF(p^n)$으로 표기한다. 만약, $n=1$이라면 유한 체는 $GF(p)$로 표현이 가능하다. 다음의 식 (1)은 Z_p 상의 n차 다항식을 보여준다.

$$f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_0 \pmod p \quad (1)$$

단, $(a_0,a_1,\cdots,a_n \in Z_p)$이고, $a_n \neq 0$이다.

한편, $n>1$이라면 p와 n은 각각 소수와 비트의 수를 의미하고, $GF(p^n)$상에서 표현할 수 있는 정수의 범위는 $[0,p^n-1]$이다. 본 논문에서는 유한 체의 표기 형식을 $GF(p^n)$으로 한다.

만약 소수 $p=2$라면, $GF(2^n)$를 생성한다. 다음의 식 (2)는 $GF(2^n)$상에서의 $(n-1)$차 다항식을 보여준다.

$$f(x)=a_{n-1}x^{n-1}+\cdots+a_0 \pmod{m(x)} \quad (2)$$

단, $(a_0,a_1,\cdots,a_n \in GF(2^n))$ 이고 $a_n \neq 0$.

식 (2)는 n개 이진 계수 $(a_{n-1},a_{n-2},\cdots,a_0)$의 연속적으로 고유하게 표현될 수 있다. 그러므로 $GF(2^n)$ 내 모든 다항식은 n개의 비트열(bit stream) (즉, $a_{n-1},a_{n-2},\cdots,a_0$)로 표현된다. 식 (2)에서 $m(x)$는 기약 다항식 (irreducible polynomial)이다. 예를 들어, $f(x)=x^2+x+1$와 $g(x)=x+1$, $m(x)=x^3+x+1$가 주어졌다면 $f(x)+g(x)=x^2$ (즉, $111 \oplus 011=100$) 이고 $f(x)\times g(x)=x$ (즉, $(x^2+x+1)\times(x+1)=x^3+1=1001$) 이다.

본 논문에서는 $GF(2^8)$상에서 수행되기 때문에 기약 다항식 $m(x)=x^8+x^4+x^3+x+1$을 사용한다.

2.2 Lagrange 보간법(Interpolation)

일반적으로 보간법이란 연속적인 함수에 대한 전체적인 함수 형태를 알지 못하고 특정한 시점에서의 함수 값만 알고 있을 때 알지 못하는 나머지 지점에서의 함수 값을 추정하는 방법으로 선형(linear), 지수(exponential), 로그-선형(log-linear) 보간법 등이 존재한다. 본 논문에서는 선형 보간법의 하나인 Lagrange 보간법을 이용하여 비밀 정보를 복원한다.

Lagrange 보간법[18,19]은 다항식 $L(x)$상의 x_i에 해당하는 좌표 값 y_i를 k개 알고 있을 경우 다른 좌표 값 한 쌍을 알 수 있는 것으로, 구체적인 방법은 다음과 같다.

임의의 다항식 $L(x)$상의 점들에 대한 좌표 값 k개가 식 (3)과 같이 주어져 있다면, 식 (4)를 이용해 계산을 수행 후 $L(x)$를 복원하여 다른 좌표 값을 알 수 있게 된다.

$$(x_0,y_0),(x_1,y_1),\cdots,(x_k,y_k) \quad (3)$$

$$L(x):=\sum_{j=0}^{k}\left(y_j \prod_{\substack{0\le m\le k\\ m\neq j}} \frac{x-x_m}{x_j-x_m}\right) \quad (4)$$

제안하는 기법 내에서 Lagrange 보간법은 쉐도우 이미지로부터 비밀 정보를 추출하는 과정에 사용되고 추출에 사용되는 것은 다음의 식 (5)와 같다.

$$F(x)=\sum_{j=1}^{t}\left(y_j \prod_{\substack{1\le k\le t\\ k\neq j}} \frac{x-x_k}{x_j-x_k}\right) \bmod m(x) \quad (5)$$

2.3 Lin과 Chan이 제안한 방법

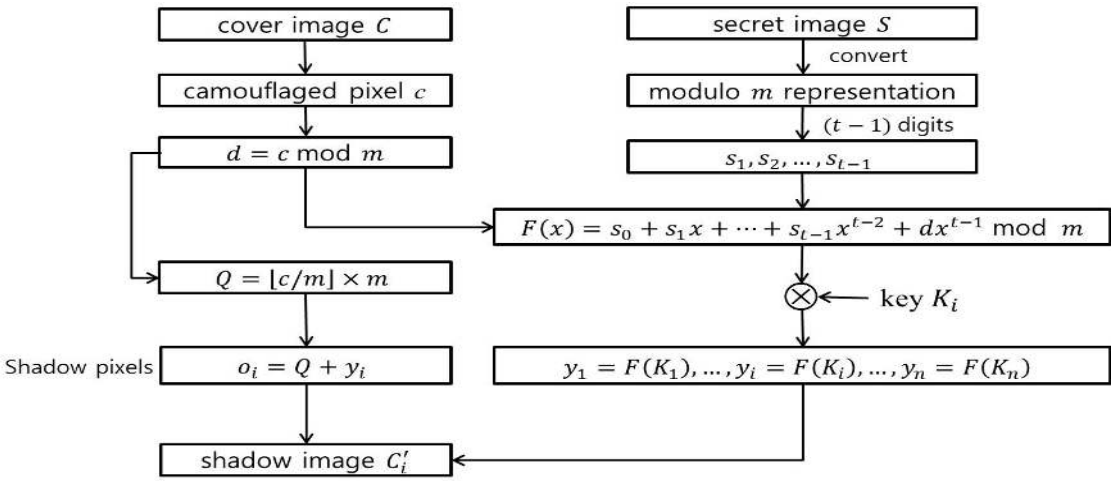
2010년에 Lin과 Chan은 가역 비밀이미지 공유 기법을 처음으로 제안했다. 이 기법은 쉐도우 이미지의 높은 품질과 비밀 정보 삽입량의 결과가 다른 기존 기법들에 비해 높다. 게다가 그들의 기법은 비밀데이터와 커버 이미지를 손실 없이(lossless) 복구할 수 있는 가역 기법을 제안했다. 본 절에서는 이들이 제안한 기법에 대해 살펴보고, 문제점을 제시한다.

Lin과 Chan의 기법에서 사전 과정으로 분배자(dealer)는 소수 m과 각 참가자들에게 분배할 유일키 $K_i(i=1,2,\cdots,n)$를 m범위 내에서 선택한다. 다항식의 계수들 $s_1,s_2,\cdots,s_{t-1}$은 비밀이미지 S를 m진법으로 표현된 각 픽셀로부터 연속적으로 결정된다.

2.3.1 비밀 공유 과정

c는 커버 이미지 C의 픽셀 값이다. 분배자는 나머지 값 d를 다음의 식 (6)에 의해 먼저 계산한다.

$$d=c \bmod m \quad (6)$$



〔그림 1〕 Lin과 Chan의 기법의 비밀 공유 과정

다음으로 $(t-1)$차 다항식은 다음의 식 (7)과 같이 생성된다.

$$F(x) = (s_0 + s_1 x + \cdots + s_{t-1}x^{t-2} + dx^{t-1}) \bmod m \quad (7)$$

식 (7)에서 함수 $F(x)$와 비밀 키 K_i는 다음과 같이 계산된다.

$$y_1 = F(K_1), \cdots, y_i = F(K_i), \cdots, y_n = F(K_n) \quad (8)$$

Lin과 Chan은 가역성의 특성을 만족하기 위해 양자화 연산(quantization operation)을 사용하며 원본 커버 픽셀 값 c의 복원이 가능하다. 양자화 연산은 다른 뜻으로 위장 픽셀 Q을 만드는 과정이다. 그들은 Q와 y_i를 합하여 쉐도우 이미지의 픽셀 값 o_i를 생성한다. 다음의 식 (9)은 양자화 값을 만드는 과정이다.

$$Q = \lfloor c/m \rfloor \times m \quad (9)$$

쉐도우 이미지의 픽셀 값 o_i는 Q가 c의 양자화 값일 때 생성된다. 그리고 o_i는 i번째 위장 픽셀로 표현된다. 쉐도우 이미지는 o_i를 사용하여 만든다. 분배자는 참가자들에게 의미 있는 쉐도우 이미지 C_i'와 키 K_i를 분배한다.

〔그림 1〕은 Lin과 Chan의 가역 비밀 공유 과정을 보여준다.

2.3.2 비밀 복원 과정

n명의 참가자들에 대한 쉐도우 이미지 C_n' 중 적어도 t개 이상의 쉐도우 이미지와 키 K가 주어졌을 때, 비밀이미지 S와 커버 이미지 C는 손실 없이 복구가 이루어진다. 커버 이미지의 각 픽셀은 선택된 t개의 쉐도우 이미지 각 픽셀과 동일한 위치의 픽셀을 가져오기 위해서 재구성 된다. 비밀데이터 $s_0, s_1, \cdots s_{t-1}$와 원본 커버 이미지 픽셀 c를 추출하기 위하여 인가된 t명의 참가자들은 c_j'로부터 식 (7)과 같은 다항식 $F(x)$를 얻어야 한다. t명의 참가자들은 쉐도우 y_j'를 얻기 위해 나머지 연산을 사용한다. y_j'는 다음의 식 (10)에 의해 계산된다.

$$y_j' = c_j' \bmod m \quad (10)$$

식 (10)에서 계산된 y_j'와 키 K_j의 쌍을 이용하면 상수와 계수들은 Lagrange 보간법을 이용하여 계산된다. 즉, 인가된 참가자들은 다항식 내 최고차 항의 계수 d와 비밀데이터 $s_0, s_1, ..., s_{t-1}$을 얻을 수 있다.

원본 커버 픽셀 c를 복원하기 위해 참가자들은 양자화 값 Q를 다음의 식 (11)와 같이 계산한다.

$$Q = \lfloor c_j'/m \rfloor \times m \quad (11)$$

또한 커버 픽셀 c는 식 (12)과 같이 계산된다.

$$c = Q + d \quad (12)$$

이들 과정을 반복한다면 t명의 참가자들은 전체의 커버 이미지 C와 비밀데이터를 복원할 수 있다. 마지막으로 t명의 참가자들은 추출된 비밀데이터로부터 비밀이미지 S를 복원한다.

2.3.3 Lin과 Chan의 기법의 문제점

첫째, 오버플로우(overflow)가 발생한다. 만약 양자화 값 Q가 다음의 식 (13)에 해당할 경우에 오버플로우가 발생한다.

$$Q \geq \lfloor 255/m \rfloor \times m \quad (13)$$

예를 들면, Q의 값이 252이고 y_j의 값이 4이상일 경우에 쉐도우 이미지의 픽셀 값 o_i의 값은 256으로 오버플로가 발생하게 된다. 쉐도우 이미지의 픽셀 값이 오버플로우가 발생한다면, 올바른 비밀 정보를 찾아낼 수 없는 문제점이 발생한다.

둘째, 전체 참가자의 수 n은 m에 의해 제한된다. (즉, $n \leq m$) 만약 $n > m$이면 다항식의 결과 값 y_j는 동일한 값이 반복적으로 생성하게 되며 그 결과 동일한 픽셀 값이 분배된다. 예를 들면, $m = 3$이고 $n = 4$라면 다항식의 결과 값 y_1과 y_4의 값이 같아지게 되며 o_i의 값 역시 같은 값을 가진다. 즉, 첫 번째 참가자와 네 번째 참가자 둘 다 같은 쉐도우 이미지의 픽셀을 얻는다. 그러므로 네 번째 참가자의 비밀 공유는 의미가 없어진다.

셋째, 다항식의 최고차 항 계수가 0이 될 수 있는 문제점을 가진다. 예를 들면, 커버 이미지의 픽셀 값 c가 161이고 $m = 7$이라면 나머지 값 $d = 0$이 되므로 최고차 항의 계수가 0이 된다. 만약 최고차 항의 계수가 0이 된다면 t명의 참가자가 모여야 비밀 정보에 접근이 가능하지만 t명보다 작은 인원으로도 비밀 정보에 접근이 가능한 문제점이 발생한다. 이는 비밀 공유 기법에 위배되는 문제점이다.

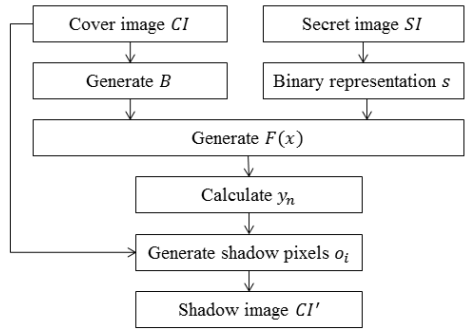
이러한 문제점들을 본 논문에서 $GF(2^8)$상의 새로운 다항식을 사용해 해결한다. 자세한 설명은 다음 장에서 언급할 것이다.

III. 제안한 방법

제안하는 방법은 Lin과 Chan의 문제점들을 해결하기 위해 새로운 다항식 기법을 적용하여 높은 품질의 쉐도우 이미지와 많은 비밀 정보 삽입을 목적으로 한다. Lin과 Chan의 기법에서 발생하는 문제점들을 해결하기 위해 다항식 내 최고차 항의 계수 중 MSB 4-비트를 고정하는 기법을 적용한 $GF(2^8)$상의 다항식을 구성한다.

3.1 비밀 공유 과정

본 절에서는 제안한 기법의 비밀 공유 과정에 대해서 설명한다. [그림 2]는 제안한 기법 내 비밀 공유 과정을 보여주고 있다.



[그림 2] 제안한 기법 내의 비밀 공유 과정

입력(Input): $M \times M$ 픽셀의 커버 이미지 CI와 $N \times N$ 픽셀의 비밀이미지 SI

출력(Output): $M \times M$ 픽셀의 쉐도우 이미지들 $C_1', C_2', \cdots, C_n'$

Step 1: 커버 이미지 CI로부터 연속적인 4픽 셀의 최하위(LSB) 두 비트를 연결하여 식 (14)와 같이 다항식의 상수 $B^{(i)}$를 구성한다.

$$B^{(i)} = b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0 \quad (14)$$

단, $0 \leq i \leq (M \times M)/4 - 1$이다. $B^{(i)}$는 커버 이미지의 정보를 가지고 있으며 가역 기법을 위해 사용된다. [그림 3] 내의 $C_{(x,y)}$는 전체 커버 이미지 x번째 행과 y번째 열의 픽셀 위치를 나타낸다 $(0 \leq x \leq M-1,\ 0 \leq y \leq M-1)$.

예를 들면, [그림 4]와 같이 (2,3)-threshold 기법 내에 적용한다면 연속적인 4픽셀을 비트로 변형하여 $164 = (10100100)_2$, $168 = (10101000)_2$, $175 = (10101111)_2$, $154 = (10011010)_2$이라 가정한다면 각 픽셀의 LSB 2-비트를 결합하면 $(00001110)_2$이 되고

$C_{(x,y)}$	$C_{(x,y+1)}$	$C_{(x,y+2)}$	$C_{(x,y+3)}$
$x_7x_6x_5x_4x_3x_2b_7b_6$	$x_7x_6x_5x_4x_3x_2b_5b_4$	$x_7x_6x_5x_4x_3x_2b_3b_2$	$x_7x_6x_5x_4x_3x_2b_1b_0$

[그림 3] 커버 이미지 C_i의 네 픽셀 값

이 값은 다항식의 상수항으로 사용된다.

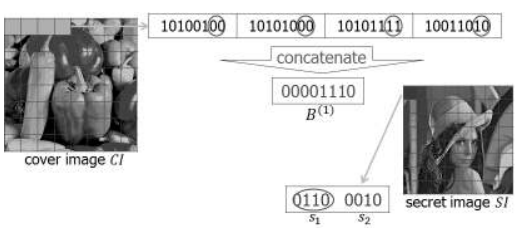
Step 2: 다항식의 계수로 사용하기 위하여 비밀이미지 SI로부터 비밀데이터 S를 구성한다.

$$SI_{(x,y)} = s_j \| s_{j+1} \tag{15}$$

이때, s_j와 s_{j+1}은 각각 4-비트로 구성된다. 4-비트로 구성하는 목적은 거의 대부분의 계수에는 8-비트의 비밀데이터가 삽입되는 반면 다항식 최고차 항의 계수에는 MSB 4-비트가 고정되고 LSB 4-비트에만 비밀데이터가 삽입되기 때문에 모든 비밀데이터 S의 구성은 4-비트로 한다. 그러므로 비밀데이터 S는 식 (16)과 같이 나타낸다.

$$S = (s_1, s_2, \cdots, s_{N\times N}) \tag{16}$$

예를 들면, 〔그림 4〕와 같이 비밀이미지 SI 내의 임의의 픽셀 값 98을 비트로 변형하면 $(01100010)_2$이 된다. 이 비트의 MSB 4-비트(0110)는 s_1이 되고 LSB 4-비트(0010)는 s_2가 된다. 이러한 방법으로 비밀이미지의 전체 픽셀까지 순차적으로 반복할 경우 S는 각 4-비트로 구성된 비트열이 만들어진다.



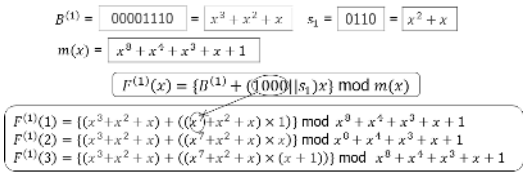
〔그림 4〕 비밀 공유 과정 내 Step 1과 Step 2의 예시

Step 3: 비밀 공유를 하기 위해 식 (17)과 같이 다항식을 구성한다.

$$F^{(i)}(x) = (B^{(i)} + (s_1 \| s_2)x + (s_3 \| s_4)x^2 + \cdots + (l \| s_{(t-1)\times 2-1})x^{t-1}) \bmod m(x) \tag{17}$$

이때, l은 4-비트 고정 상수(즉, 1000)이고 다항식 최고차 항 계수의 LSB 4-비트에 비밀데이터가 삽입된다. 단, i의 범위는 $0 \le i \le (M\times M)/4-1$이다.

예를 들면, 〔그림 5〕와 같이 $B^{(i)} = (00001110)_2 = x^3+x^2+x$로 표현이 가능하고 $s_1 = (0110)_2 = x^2+x$로 표현이 가능하다. 또한 $GF(2^8)$상에 $m(x) = x^8+x^4+x^3+x+1$이므로 다항식 $F^{(1)}(x)$에 대입하여 계산한다. 단, MSB 4-비트(1000)은 다항식 내 x^7으로 간주된다.



〔그림 5〕 비밀 공유 과정 내 Step 3의 예시

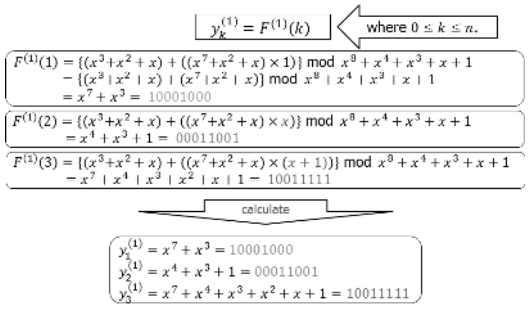
Step 4: 식 (17)로부터 생성되는 n개 다항식은 다음의 식 (18)에 의해 $y_1^{(i)}, y_2^{(i)}, \cdots, y_n^{(i)}$ 로 계산된다.

$$y_k^{(i)} = F^{(i)}(k) \tag{18}$$

이때, k는 분배자가 참가자에서 나누어주는 키 값이며 범위는 $0 \le k \le n$이다. 그리고 i는 1씩 증가한다. 만약 i가 $(M\times M)/4$와 같다면 다음 Step 5로 진행하고 반대일 경우는 Step 3으로 돌아가 다시 실행함으로써 커버 이미지 전체 픽셀만큼 수행한다.

예를 들면, 〔그림 6〕과 같이 다항식 $F^{(1)}(x)$로부터 계산된 세 다항식의 결과 값들은 다음과 같이 나타난다.

$(y_1^{(1)} = x^7+x^3 = (10001000)_2,$
$y_2^{(1)} = x^4+x^3+1 = (00011001)_2,$
$y_3^{(1)} = x^7+x^4+x^3+x^2+x+1 = (10011111)_2)$



〔그림 6〕 비밀 공유 과정 내 Step 4의 예시

Step 5: 커버 이미지 C와 $y_1^{(i)}, y_2^{(i)}, \ldots, y_n^{(M\times M/4)-1}$를 이용하여 n개의 쉐도우 이미지$(C_1', C_2', \ldots, C_n')$를 생성한다. 이때, $y_1^{(i)}, y_2^{(i)}, \cdots, y_n^{(M\times M/4)-1}$은 8비트로 식 (19)과 같이 구성된다.

$$y_j^{(i)} = b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0 \tag{19}$$

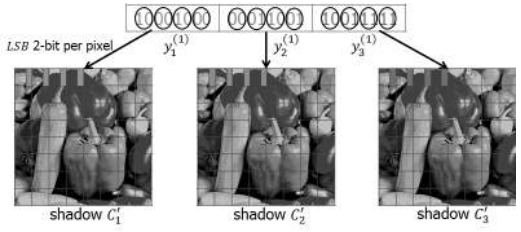
생성된 8-비트의 값은 〔그림 4〕과 같이 2-비트씩

나누어서 커버 이미지의 LSB 2-비트로 삽입된다.

$C'_{(x,y)}$	$C'_{(x,y+1)}$	$C'_{(x,y+2)}$	$C'_{(x,y+3)}$
$X_7x_6x_5x_4x_3x_2b_7b_6$	$x_7x_6x_5x_4x_3x_2b_5b_4$	$x_7x_6x_5x_4x_3x_2b_3b_2$	$x_7x_6x_5x_4x_3x_2b_1b_0$

〔그림 7〕 쉐도우 이미지 C'의 4픽셀에 대한 삽입과정

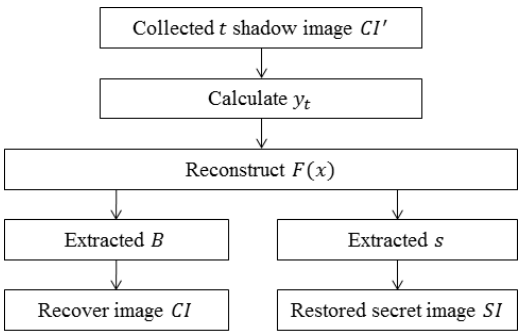
예를 들면, 〔그림 8〕과 같이 $y_1^{(1)}=(10001000)_2$에서 2비트로 나눈 10,00,10,00은 원본 커버 이미지 내에 4픽셀의 LSB 2-비트로 삽입되어 반복을 통해 쉐도우 이미지 C_1'을 생성한다.



〔그림 8〕 비밀 공유 과정 내 Step 5의 예시

3.2 비밀 복원 과정

본 절에서는 제안한 기법의 비밀 복원 과정에 대해서 설명한다. 〔그림 9〕는 제안한 기법 내 비밀 복원 과정을 보여준다.



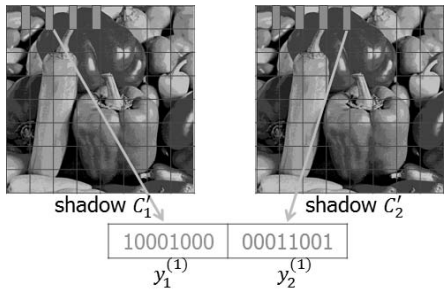
〔그림 9〕 제안한 기법 내 비밀 복원 과정

입력(Input): $M\times M$ 픽셀의 선택된 t 쉐도우 이미지들 $C_1', C_2', \cdots, C_t'$

출력(Output): $M\times M$ 픽셀의 복원된 커버 이미지 CI와 $N\times N$ 픽셀의 복원된 비밀이미지 SI

Step 1: 선택된 t개의 커버 이미지 $C_1', C_2', \cdots, C_t'$로부터 $y_k^{'(i)}$를 추출한다. 단, $0\le i\le (M\times M)/4-1$, $1\le k<t$.

예를 들면, (2,3)-threshold 기법에서 〔그림 10〕과 같이 쉐도우 이미지 C_1'과 C_2'를 선택할 경우 각각 연속적인 4픽셀의 LSB 2-비트씩을 추출해 결합을 하면 $y_1^{(1)}=(10001000)_2$, $y_2^{(1)}=(00011001)_2$를 생성할 수 있다.



〔그림 10〕 비밀 복원 과정 내 Step 1의 예시

Step 2: 유한 체 상에서 쉐도우 이미지의 픽셀 값 $y_k^{'(i)}$와 비밀 키 k와 함께 Lagrange 보간법을 이용하여 식 (20)과 같이 다항식 $F^{'(i)}(x)$를 재구성한다.

$$F^{'(i)}(x)=B^{'(i)}+(s_1\|s_2)x+(s_3\|s_4)x^2+\cdots+(l\|s_{(t-1)\times 2-1})x^{t-1} \bmod m(x) \quad (20)$$

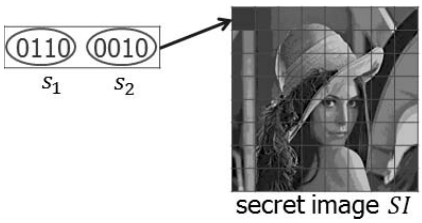
Lagrange 보간법을 이용하면 재구성된 다항식으로부터 상수항 $B^{'(i)}$과 각 차수의 계수들 $s_1\|s_2, \cdots, s_{(t-1)\times 2-1}$을 계산할 수 있다. 또한, 다항식 최고차 항의 계수 중 MSB의 4-비트를 알고 있다면 나머지 LSB의 4-비트도 계산된다. 그리고 i는 1씩 증가한다. 만약 i가 $(M\times M)/4$와 같다면 다음 Step 3로 진행하고 반대일 경우는 Step 1으로 돌아가 다시 실행함으로써 커버 이미지 전체 픽셀만큼

수행한다.

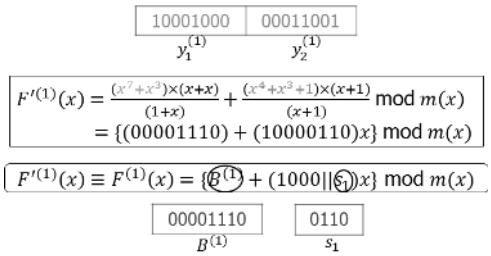
Step 3: Step 2의 결과로부터 비밀데이터 S를 추출한다. 그리고 S를 다시 SI로 변환한다.

예를 들면, 〔그림 12〕와 같이 추출된 $(0110)=s_1$, $(0010)=s_2$로부터 S로 변환하여 비밀 이미지의 픽셀 값이 복원된다.

Step 4: 복원된 $B^{'(i)}$는 8-비트의 값으로 구성되



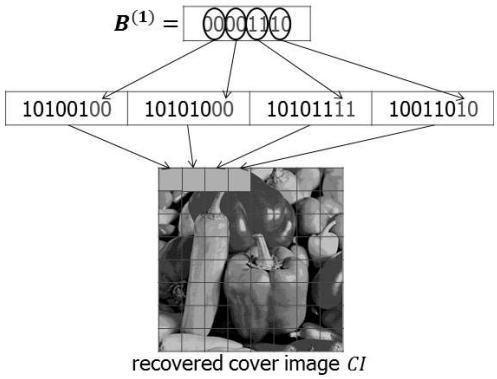
〔그림 11〕 비밀 복원 과정 내 Step 3의 예시



〔그림 12〕 비밀 복원 과정 내 Step 2의 예시

어 있으며 2-비트씩 나누어서 커버 이미지의 LSB 2-비트로 삽입함으로써 커버 이미지를 복원한다.

예를 들면, 〔그림 13〕과 같이 추출된 $B^{(1)}=(00001110)_2$에서 00, 00, 11, 10으로 2-비트씩 나누어서 연속적인 4픽셀의 LSB 2-비트로 삽입하게 되면 $(10100100)_2=164$, $(10101000)_2=168$, $(10101111)_2=175$, $(10011010)_2=154$과 같이 원본 커버 이미지의 픽셀 값이 복원된다.



〔그림 13〕 비밀 복원 과정 내 Step 3의 예시

IV. 실험 결과

본 장에서는 제안한 기법과 Lin과 Chan의 기법에 대해 이미지 품질과 비밀 정보 삽입량에 대해 비교하고, 이를 통해 제안한 기법의 우수성을 검증한다. 4.1절에서는 두 기법을 실험하기 위한 도구 및 평가 기준에 대하여 설명하고 4.2절에서는 *PSNR*의 실험 결과 및 분석을 보여준다. 마지막으로, 4.3절에서는 삽입량의 실험 결과 및 분석을 보여준다.

4.1 실험 도구 및 평가 기준

일반적으로 비밀이미지 공유 기법들의 성능 평가를 위해 크게 두 가지의 측정 기준을 사용한다. 첫 번째는 비밀 정보 삽입량(capacity)으로 커버 이미지 내에 비밀데이터를 얼마나 많이 삽입할 수 있는가를 측정하는 것이다. 비밀이미지 공유 기법에서는 보통 커버 이미지 내에 삽입된 비밀데이터의 양을 측정하며 그 단위는 bpp(bit per pixel)나 전체 이미지 내에 삽입된 비밀데이터의 용량(bit)을 사용한다. 제안하는 방법에서 비밀 정보 삽입량은 커버 이미지와 t의 크기에 따라 결정된다. 두 번째는 생성된 쉐도우와 커버 이미지 간의 이미지 왜곡(distortion)을 측정하는 것으로 공격자에게 커버 이미지 내 비밀 정보 삽입의 유무를 알 수 없게 하는 기법인 스테가노그래피 관점에서 매우 중요한 요소이다. 이러한 왜곡을 측정하기 위해 *PSNR*을 사용하는데 다음의 식 (21)와 같이 계산한다.

$$PSNR=\left(10\log_{10}\left(\frac{255^2}{MSE}\right)\right) \tag{21}$$

단, *MSE*는 에러평균의 제곱(mean squared error)값으로 다음의 식 (22)와 같이 계산한다.

$$MSE=\left(\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(I_{(i,j)}-I'_{(i,j)})^2\right) \tag{22}$$

단, $I_{(i,j)}$와 $I'_{(i,j)}$는 $H\times W$ 크기의 쉐도우 이미지와 커버 이미지의 픽셀 값이고, *PSNR* 값이 클수록 높은 이미지의 왜곡이 없어진다. 만약 *PSNR*이 35dB보다 크다면 사람의 육안(human visible system)으로 구별하기 어렵다.

실험에 사용된 커버 이미지는 〔그림 14〕와 같이 일반적으로 사용하는 그레이 스케일 이미지 8개를 사용하였고, 각 이미지의 크기는 512×512이다. 〔그림 15〕는 실험에 사용한 비밀이미지이며 256×256 크기의 Pepper 이미지를 사용한다.

4.2 PSNR의 실험 결과 및 분석

본 절에서는 Lin과 Chan의 기법과 제안한 기법의 *PSNR*의 실험 결과를 비교한다.

Lin과 Chan의 기법에 대한 *PSNR*의 결과는 m 값이 커질수록 변동되는 비트의 수가 많아지기 때문에 *PSNR* 역시 낮아진다. 〔표 1〕은 Lin과 Chan의 방법 내 비밀데이터 삽입량과 *PSNR*의 비율이 가장 좋은 $m(\leq t)=7$일 때와 제안한 방법에서는 t에 따른 실험 결과 비교를 보여준다. 그들의 방법 내 두 번째 문제점에 따라 (7,8)-threshold 방법에서 $m=7$이기 때문에 7명 이상 비밀 공유가 불가능하다. 하지만 제안한 방법에선 t의 증가에 따라*PSNR*은 약 45dB 정도로 유지된다. 또한 분배자는 전체 참가자를 256명으로 정할 수 있으며, 높은 품질의 쉐도우 이미지를 얻을 수 있다.〔표 2〕는 Lin과 Chan의 방법의 m에 따른 커버 이미지별 왜곡 정도를 보여준다. 〔표 2〕에서와 같이 만약 m이 11보다 더 큰 값을 사용한다면 *PSNR*은 35dB보다 작아지므로 스테가노그래피 기법의 기능을 상실하게 된다. 그러므로, 이들 기법은 참가자들의 수에 따라 삽입량과 *PSNR* 사이에 이율 배반성을 가진다. 즉, 전체 참가자들의 수가 11명으로 제한되는 문제점을 가지게 된다. 〔표 3〕은 제안한 방법의 t에 따른 커버 이미지별 왜곡 정도를 보여준다. 제안한 기법은 삽입량과 *PSNR* 사이에 이율 배반성을 가지지 않는다. 즉, 전체 참가자의 수가 증가하면 할수록 비밀 정보 삽입량은 증가하면서 *PSNR* 역시 45dB로 유지할 수 있는 장점을 가지고 스테가노그래피 기법의 기능 역시 문제없이 적용된다.

〔그림 14〕 사용한 9개의 커버 이미지

〔그림 15〕 사용한 비밀 이미지와 복원된 비밀 이미지

〔표 1〕 Lin과 Chan의 기법과 제안한 기법의 비밀 정보를 숨길 수 있는 양과 이미지의 왜곡정도 비교 ((7,8)-threshold)

t	Lin&Chan's 기법		제안한 기법	
	삽입량 (bit)	PSNR (dB)	삽입량 (bit)	PSNR (dB)
2	786,432	47.02	262,144	45.62
3	1,572,864	46.87	786,432	45.57
4	2,359,296	42.31	1,310,720	45.86
5	3,145,728	42.26	1,835,008	45.61
6	3,932,160	39.52	2,359,296	45.81
7	4,718,592	39.39	2,883,584	45.74
8	N/A	N/A	3,407,872	45.93
9	N/A	N/A	3,932,160	45.79
10	N/A	N/A	4,456,448	45.54
11	N/A	N/A	4,980,736	45.66
12	N/A	N/A	5,505,024	45.81
13	N/A	N/A	6,029,312	45.76
14	N/A	N/A	6,553,600	45.68
15	N/A	N/A	7,077,888	45.89
⋮	⋮	⋮	⋮	⋮

〔표 2〕 Lin과 Chan의 기법의 m에 따른 커버 이미지별 왜곡 정도

Cover image	PSNR (dB)				
	$m=3$	$m=5$	$m=7$	$m=11$	$m=13$
Airplane	46.62	42.16	39.32	36.48	34.78
Airport	47.02	42.38	39.49	36.72	34.80
Boat	46.98	42.28	39.44	36.24	34.45
Couple	46.87	42.24	39.14	36.65	34.58
Goldhill	46.81	42.21	39.65	36.44	34.34
Lena	46.92	42.26	39.43	36.58	34.86
Mandrill	47.01	42.35	39.58	36.77	34.28
Toy	46.82	42.26	39.26	36.80	34.85
City	46.77	42.18	39.20	36.54	34.94
Average	46.87	42.26	39.39	36.58	34.65

〔표 3〕 제안한 기법의 t에 따른 커버 이미지별 왜곡 정도

Cover image	PSNR (dB)						
	$t=3$	$t=5$	$t=7$	$t=11$	$t=13$	…	$t=256$
Airplane	45.38	45.42	45.35	45.48	45.68	…	45.53
Airport	45.42	45.45	45.40	45.32	45.54	…	45.48
Boat	45.65	45.62	45.86	45.72	45.84	…	45.80
Couple	45.37	45.54	45.76	45.68	45.62	…	45.65
Goldhill	45.69	45.65	45.91	45.83	45.76	…	45.72
Lena	45.73	45.69	45.84	45.74	45.85	…	45.83
Mandrill	45.75	45.77	45.79	45.61	45.87	…	45.78
Toy	45.48	45.62	45.87	45.72	45.71	…	45.72
City	45.65	45.72	45.92	45.80	45.93	…	45.88
Average	45.57	45.61	45.74	45.66	45.76	…	45.71

4.3 삽입량의 실험 결과 및 분석

본 절에서는 Lin과 Chan의 기법과 제안한 기법의 비밀 정보 삽입량의 실험 결과를 비교한다.

Lin과 Chan의 기법의 삽입량은 threshold 값 t, m 그리고 커버 이미지의 크기와 관련있다. 첫째, t가 증가하면 할수록 삽입량은 증가한다. 그 이유는 t가 증가하면 다항식에서 더 많은 계수에 비밀데이터를 삽입할 수 있기 때문이다. 둘째, m값이 커지면 커질수록 삽입량 역시 증가한다. 그 이유는 비밀이미지의 픽셀 값을 m진법으로 표현할 때 나오는 자릿수의 개수가 적어지므로 더 많은 양의 삽입이 가능하다. 마지막으로 커버 이미지의 크기가 클수록 비밀데이터를 삽입할 수 있는 공간이 늘어남으로써 삽입량은 증가한다.

Lin과 Chan의 방법에서 비밀 정보 삽입량과 *PSNR*의 비율이 가장 좋은 m이 7일 경우 삽입량은 $((t-1)\times M\times M)/3$ (pixel)을 나타낸다. 그러므로, 한 픽셀당 삽입할 수 있는 비트의 수는 $(t-1)/3$ (bpp)가 된다. 하지만 이들 기법에는 삽입량이 증가할수록 *PSNR*이 감소하게 된다.

반면, 제안한 기법의 삽입량 역시 t에 따라서 증가하게 되고 커버 이미지의 크기가 커질수록 삽입량 역시 증가하는 성질은 그들의 방법과 같다.

제안한 방법 내 삽입량은 $((8t-12)\times M\times M)/4$ (pixel)을 나타내며 Lin과 Chan의 기법 내 m과 같은 다른 요인에 저항 없이 t가 증가함에 따라 일정하게 증가한다. 그러므로, 한 픽셀당 삽입할 수 있는 비트의 수는 $(2t-3)$ (bpp)가 된다. 결론적으로, 이미지 전체에 대한 삽입량은 그들의 기법이 제안한 기법보다 더 많은 삽입량을 가진다. 하지만 전체 참가자의 수를 크게 한다면 제안한 기법이 더 많은 삽입량을 가진다.

V. 결 론

본 논문은 유한 체 기반의 개선된 가역 비밀이미지 공유 기법을 제안하였다. $GF(2^8)$상에서 다항식 연산을 수행함으로써 Lin과 Chan의 기법보다 많은 참가

자에게 비밀 공유가 가능해졌고, 오버플로우도 발생하지 않는다. 다항식($F^{(i)}(x)$) 내 최고차 항의 계수를 MSB-4비트(즉, 1000)를 고정 함으로써 최고차 항의 계수가 0이 되는 문제점도 해결하였다. 결과적으로, Lin과 Chan의 기법에서 발생하는 모든 문제점을 새로운 다항식 방법을 이용하여 해결하였다.

실험 결과에서는 t가 증가함에 따라 Lin과 Chan의 기법과 제안한 기법 모두 비밀 정보 삽입량이 증가하였다. 그들의 기법은 제안한 기법보다 비밀 정보 삽입량이 더 많다. 하지만 그들의 기법은 t와 n의 값이 11로 제한되므로 비밀 정보 삽입량이 제한되는 반면 제안한 기법은 t가 256까지 증가함에 따라 삽입량도 계속 증가하였다. *PSNR*은 그들의 기법보다 제안한 기법이 더 좋다. 그들의 기법 내 *PSNR*은 비밀 정보 삽입량 증가에 따라 감소하게 되는 이율 배반성의 특성을 가진다. 만약 $m > 11$ 라면, *PSNR*은 35dB보다 작아지므로 스테가노그래피 특성이 상실된다. 하지만 제안한 기법은 비밀 정보 삽입량이 증가하더라도 *PSNR*은 45dB이상 유지된다.

향후에는 $GF(2^8)$에 의한 256명으로 제한된 전체 참가자의 수를 확장하여 자유롭게 할 수 있는 기법에 대하여 연구 중이다.

참고문헌

〔1〕 G. R. Blackley, "Safeguarding cryptographic keys," Managing Requirements Knowledge, International Workshop on, pp.313-317, June, 1979.

〔2〕 A. Shamir, "How to share a secret," Commun. ACM, vol. 22, pp. 612-613, November, 1979.

〔3〕 J.-C. L. Chih-Ching Thien, "Secret image sharing," Computers & Graphics, vol. 26, No. 5, pp. 765-770, October, 2002.

〔4〕 J.-C. L. Chih-Ching Thien, "An image sharing method with user-friendly shadow images," IEEE Trans. Cir. and Sys. for Video Technol, vol. 13, No. 12, pp. 1161-1169, December, 2003.

〔5〕 W.-H. T. Chang-Chou Lin, "Secret image sharing scheme with steganography and authentication," J. Syst. Softw., vol. 73, No, 10, pp. 405-414, December, 2004.

〔6〕 K.-H. Y. C.-C. W. Ching-Nung Yang, Tae-Shih Chen, "Improvements of image sharing with steganography and authentication," Journal of System & Software, vol. 80, No. 7, pp. 1070-1076, July, 2007.

〔7〕 S.-J. S. Rang-Zan Wang, "Scalable secret image sharing," Signal processing: Image communication, vol. 22, pp. 363-373, April, 2007.

〔8〕 S.-M. H. Ching-Nung Yang, "Constructions and properties of k out of n scalable secret image sharing," Optics Communications, vol. 283, No. 9, pp. 1750-1762, May, 2010.

〔9〕 Y.-Y. C. Ching-Nung Yang, "A general (k, n) scalable secret image sharing scheme with the smooth scalability," The Journal of Systems and Software, vol. 84, No. 10, pp. 1726-1733, October, 2011.

〔10〕 T. Tassa, "Hierarchical threshold secret sharing," Journal of cryptology, vol. 20, No. 2, pp. 237-264, February, 2007.

〔11〕 C. Q. Cheng Guo, Chin-Chen Chang, "A hierarchical threshold secret image sharing," Pattern Recognition Letters, vol. 33, No. 1, pp. 83-91, January, 2012.

〔12〕 C.-C. C. Pei-Yu Lin, Jung-San Lee, "Distortion-free secret image sharing mechanism using modulus operator," Pattern Recognition Letters, vol. 42, pp. 886-895, May, 2009.

〔13〕 C.-S. C. Pei-Yu Lin, "Invertible secret image sharing with steganography," Pattern Recognition Letters, vol. 31, No. 13, pp. 1887-1893, October, 2010.

〔14〕 Y.-Y. L. R.-Z. W, "Improved Invertible Secret Image Sharing with Steganography,"2011 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 93-96, October, 2011.

〔15〕 D.-H. K, G.-J. L, M.-H. P, K.-Y. Y, "A Reversible Secret Sharing Scheme based

on $GF(2^8)$," The 9th International Conference on Infomation Technology: New Generation, ITNG 2012, pp. 425-430, April, 2012.

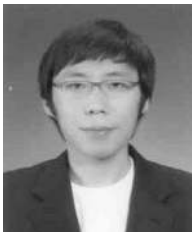
〔16〕 안준언, 유기영, "고속 RSA 암호 시스템을 위한 몽고메리 알고리즘의 구현 및 분석," 통신정보보호학회논문지, vol. 9, No. 2, pp. 61-71, 1999년 6월.

〔17〕 유기영, 김정준, "유한 필드 GF(2^m)상의 시스톨릭 곱셈기/제곱기 설계," 정보과학회논문지: 시스템 및 이론, 제28권, 제6호, pp. 289-300, 2001년 6월.

〔18〕 W. Stallings, Cryptography and network security: principles and practices, 4th Ed., Prentice Hall, Nov. 2005.

〔19〕 D. R. Stinson, Ceyptography Theory and Practice. Chapman & Hall / CRC Press, 3rd Edition, pp. 481-515, 2006.

〈저자소개〉



김 동 현 (Dong-hyun Kim) 학생회원
2011년 2월: 대구대학교 전산통계학과 졸업
2013년 2월: 경북대학교 전자전기컴퓨터학부 석사졸업
〈관심분야〉 정보보호, 암호학, 비밀공유, 스테가노그래피

김 정 준 (Jung-Joon Kim) 정회원
1981년 2월: 경북대학교 전자공학과 졸업
1983년 2월: 한국과학기술원 전자공학과 석사졸업
1997년 7월: 미국 루이지애나 주립대 전자 및 컴퓨터공학과 박사졸업
1984년~2011년: ㈜ KT 상무
2012년 3월~현재: 경북대학교 IT대학 전자공학부 부교수
〈관심분야〉 정보보호, 신호처리, 임베디드 단말, 유무선통합, ICT 컨버전스

유 기 영 (Kee-young Yoo) 종신회원
1976년 2월: 경북대학교 수학교육학과 졸업
1978년 2월: 한국과학기술원 전산학과 석사졸업
1992년 3월: 미국 Rensselaer Polytechnic Institute 전산학과 박사졸업
1978년 3월~현재: 경북대학교 IT대학 컴퓨터학부 교수
〈관심분야〉 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그래피, 인증프로토콜, 양자보안