Journal of Korea Multimedia Society Vol. 18, No. 11, November 2015(pp. 1332-1341)
http://dx.doi.org/10.9717/kmms.2015.18.11.1332

암호화된 이미지에서 대칭키 암호화 알고리듬을 이용한 가역 비밀이미지 공유 기법

전병현[†], 신상호[††], 정기현[†††], 이준호[††††], 유기영[†††††]

Reversible Secret Sharing Scheme Using Symmetric Key Encryption Algorithm in Encrypted Images

Byoung-Hyun Jeon[†], Sang-Ho Shin[††], Ki-Hyun Jung[†††],
Joon-Ho Lee[††††], Kee-Young Yoo[†††††]

ABSTRACT

This paper proposes a novel reversible secret sharing scheme using AES algorithm in encrypted images. In the proposed scheme, a role of the dealer is divided into an image provider and a data hider. The image provider encrypts the cover image with a shared secret key and sends it to the dealer. The dealer embeds the secret data into the encrypted image and transmits encrypted shadow images to the corresponding participants. We utilize Galois polynomial arithmetic operation over 2^8 and the coefficient of the higher-order term is fixed to one in order to prevent the overflow. In experimental results, we demonstrate that the PSNR is sustained close to 44dB and the embedding capacity is 524,288 bits.

Key words: Reversible Secret Image Sharing, Encrypted Images, Symmetric Key Encryption Algorithm, Information Hiding

1. 서 론

비밀 공유(secret sharing)는 기존의 암호화 방법과는 달리 비밀을 한 사람이 소유하는 것이 아니라 인증된 참가자 다수에게 비밀의 조각을 분배하고, 비밀을 복원하고자 하는 경우 일정한 수 이상의 참가자들로부터 비밀의 조각을 수집하여 본래의 비밀을 확인하는 것이다. 비밀 공유 기법은 한사람이 비밀을 소유할 수 없는 군사 로켓 발사 시스템이나 은행 거래 시스템의 접근 등과 같은 접근 제어(access control) 방법으로 활발하게 연구되어왔다[1-3].

비밀 공유 기법은 n명의 인증된 참가자 중 적어도 t명 이상이 모이면 비밀을 확인할 수 있다는 (t,n)-threshold의 개념을 사용했고, t명 보다 적은 인원이 모일 경우에는 비밀을 확인할 수 없으며, 참가자 개개인이 소유한 비밀의 정보를 통해 본래의 비밀을

※ Corresponding Author : Kee-Young Yoo, Address: (702-701) 80 Daehakro, Buk-gu, Daegu, Korea, TEL : +82-53-950-5553, FAX : +82-53-957-4846, E-mail : yook@knu.ac.kr
Receipt date : July 9, 2015, Revision date : Aug. 29, 2015
Approval date : Sep. 24, 2015
[†] Dept. of Computer Info & Communication, Yeungjin Cyber College (E-mail : bhjun64@hanmail.net)
[††] Realistic Media Result Product Promotion Group, Dongguk University Gyeongju Campus (E-mail : shshin.study@gmail.com)
[†††] Dept. of Cyber Security, Kyungil University (E-mail : kingjung@paran.com)
[††††] 6th R&D Institute, Agency for Defense Development (E-mail : joonho0522@gmail.com)
[†††††] School of Compuer Science and Engineering, Kyungpook National University (E-mail : yook@knu.ac.kr)
※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(No. 2015R1D1A1A01058019)

확인할 수 없다[4]. 비밀을 복원하는 과정에서는 Lagrange 보간법을 이용하여 본래의 다항식을 복원하여 비밀값을 확인하도록 하였으며, 이 후 Shamir의 비밀 공유 기법에 기반을 두어 다양한 분야에서 활용 가능한 방법들이 제안되었다[5-9]. 2002년에는 Thein과 Lin [10]에 의해 처음으로 그레이스케일(grayscale) 이미지를 이용한 비밀이미지 공유 기법이 제안되었다. 그러나 비밀이미지에 대한 손실이 발생하는 단점이 존재하여 이를 보안하기 위한 여러 기법들이 제안되었다[11-17]. 2010년에는 Lin과 Chan [18]에 의해 가역 비밀이미지 공유 기법이 제안되었고, 임계(threshold)값인 t에 따라 비밀이미지의 삽입 용량(embedding capacity)이 비례적으로 증가하는 장점이 존재했다. 그러나 $t-1$명 이하가 공모되더라도 비밀이미지를 복원할 수 있거나 삽입 용량이 증가할수록 공유 이미지(shadow image)의 왜곡 정도가 심해진다는 단점도 존재했다.

비밀이미지 공유 기법은 커버이미지 내에 비밀 정보를 은닉(hiding)하는 스테가노그래피(steganography)와 밀접한 관계를 형성한다. 특히, 스테가노그래피에서 연구 중인 다양한 비밀 정보 삽입 기법들이 비밀이미지 공유에도 적용 중인 사례가 존재하고 [10-18,21,22], 최근에는 암호화된 이미지(encrypted image) 내에 비밀 정보를 숨기는 방법들도 활발히 제안되고 있다[19,20]. 이는 기존의 커버이미지 공급과 비밀 정보의 은닉을 한 사람에 의해 수행된 것과 달리 이미지의 정보를 이미지 제공자(image provider)와 데이터 수신자(data receiver)만이 확인이 가능해야 하는 경우 비밀 정보를 커버이미지에 숨기는 사람을 알 수 없어야 하고, 이를 막기 위해 이미지 제공자가 자신의 커버이미지를 암호화 과정을 통해 암호화된 이미지로 변경한 후 이를 비밀 정보를 숨기는 자에게 전송해야 한다. 이를 통해 커버이미지의 노출이나 기타 저작권과 관련된 문제 혹은 커버이미지를 임의로 사용할 수 없는 장점이 존재한다.

본 논문에서는 AES 표준 암호 알고리듬를 사용하여 암호화된 이미지를 생성하고, 암호화된 이미지에 비밀이미지의 정보를 은닉하여 참가자들에게 공유하는 새로운 형태의 비밀 공유 기법을 제안한다. 제안하는 기법에서는 기존의 딜러의 역할을 이미지 제공자와 비밀을 조각으로 분리하여 암호화된 이미지 내에 삽입하는 데이터 은닉자(data hider)로 분리한다. 이미지 제공자는 자신의 커버이미지를 모든 참가자들과 공유한 비밀키와 AES 표준 암호 알고리듬을 이용하여 암호화된 이미지를 생성한 후 데이터 은닉자에게 전송한다. 데이터 은닉자는 비밀을 조각으로 분리하여 암호화된 이미지 내에 삽입한 후 공유 이미지를 생성하고, 이를 해당 참가자에게 분배한다. 본래의 비밀을 복원하고자 하는 경우 적어도 t명 이상의 참가자들이 모여 자신이 소유한 공유 이미지를 제출하여 본래의 비밀을 확인한 후 각 참가자는 이미지 제공자와 공유한 비밀키를 이용하여 복호화 과정을 수행한 후 커버이미지를 확인한다. 또한, 효율적인 비밀이미지 공유와 오버플로우(overflow)를 방지하기 위해 유한체($GF(2^8)$)상에서 다항식 연산을 수행한다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문의 배경 이론이 되는 암호화된 이미지를 이용한 정보은닉 기법과 Shamir의 비밀 공유 기법을 소개한 다음, 3장에서 제안하는 기법의 세 가지 알고리듬을 설명한다. 여기에서는 제안한 알고리듬의 전체적인 개요와 암호화된 이미지의 생성, 공유 이미지 생성, 비밀이미지와 커버이미지 복원 알고리듬을 각각 서술한다. 제안한 기법에 대한 실험 및 결과 분석을 4장에서 다루고, 5장에서 결론을 맺는다.

2. 관련연구

2.1 암호화된 이미지에 기반을 둔 가역 정보은닉 기법

암호화된 이미지에 기반을 둔 가역 정보은닉 기법은 3명의 사용자들로 구성된다. 이미지 제공자(image provider), 데이터 은닉자(data hider) 그리고 데이터 수신자(data receiver)이고, 각각의 역할은 Fig. 1과 같다. 이미지 제공자는 데이터 수신자와 공유된 비밀키를 이용해 자신의 커버이미지(cover image)를 암호화한 후 데이터 은닉자에게 암호화된 이미지를 전송한다. 암호화된 이미지를 수신 받은 데이터 은닉자는 데이터 수신자와 미리 공유된 데이터 은닉키를 이용하여 자신이 숨기고자 하는 데이터를 암호화된 이미지 내에 삽입한 후 이를 데이터 수신자에게 전송한다. 이를 수신 받은 데이터 수신자는 데이터 은닉키를 이용하여 암호화된 이미지 내에 삽입된 정보를 추출하고, 이미지 제공자와 공유된 비밀키를 이용하여 암호화된 이미지를 복원한 후 본래의 이미지를

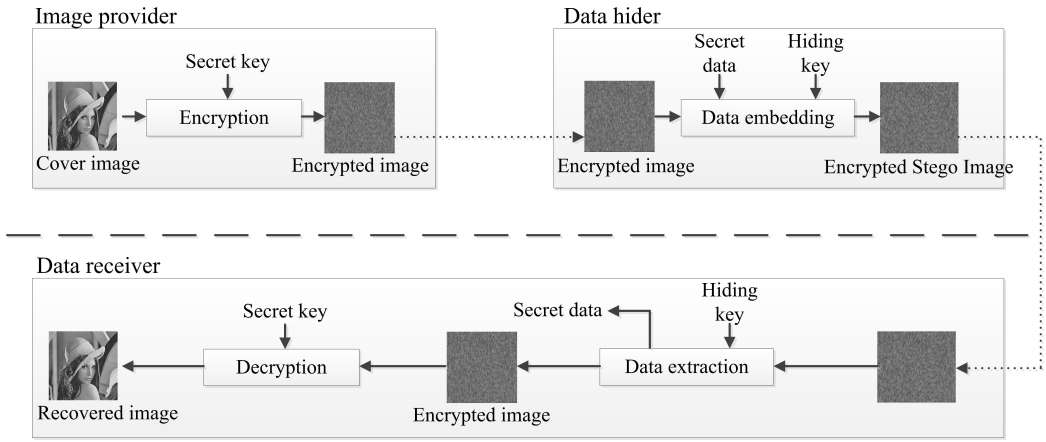

Fig. 1. Flowchart of Zhang's encrypted image-based reversible data hiding scheme.

확인한다[19].

이러한 기법은 Zhang[19]에 의해 처음으로 제안된 것으로 커버이미지 내에 임의의 픽셀 블록을 의사난수와의 XOR 불대수 연산을 수행하여 암호화된 이미지를 생성했다. 픽셀의 블록 크기가 작을수록 보안 위협에 쉽게 노출되기 때문에 이러한 문제점을 해결하고자 Hong 등[20]은 보안 강도에 따라 적응적인 블록 사이즈 선택 기법을 제안했다.

2.2 Shamir의 비밀 공유 기법

Shamir는 (t,n)-threshold 개념과 다항식(polynomial) 연산 및 Lagrange의 보간법(interpolation)에 기반을 두어 비밀 공유 기법을 제안했다[4]. 초기화 과정, 공유값 분배과정, 그리고 비밀 복원과정으로 모든 과정에서 하나의 비밀로부터 공유값을 생성, 분배, 그리고 복원하는 역할은 딜러가 수행한다. 딜러는 합법적으로 인증된 자로 가정한다[1-4].

초기화 과정에서 딜러는 소수 p에 대하여 Z_p상의 0이 아닌 서로 다른 원소 n개를 선택($p \geq n+1$)하고, 이를 x_i로 표기한다. 단, i는 참가자들의 순번을 의미하고, 범위는 $1 \leq i \leq n$을 만족한다. 임의의 i에 대해서, 딜러는 고유값 x_i를 i번째 참가자 P_i에 대응시켜 준다.

공유값 분배과정에서는 먼저, 딜러가 공유하려는 비밀(S)을 Z_p상의 원소로 가정한다. 딜러는 Z_p상에서 $t-1$개의 원소들을 비밀스럽게 선택하고, 이를 $a_1, a_2, ..., a_{t-1}$로 각각 표기한다. 임의의 i에 대해, 딜러는 식 (1)을 이용해 공유값 $y_i = f(x_i)$값을 생성한다. 딜러는 해당 참가자 공유값(y_i)을 분배한다.

$$f(x) = S + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \pmod{p} \quad (1)$$

비밀 복원과정에서는 딜러에 의해 n명의 참가자 중 적어도 t명 이상의 인원으로 부터 참가자 P_i가 소유한 공유값 y_i를 수집한다. 수집한 (i, y_i)쌍들과 Lagrange 보간법을 이용하여 공유값 분배과정에서 사용했던 식 (1)을 식 (2)에 의해 복원한다. 딜러에 의해 복원된 식 (2)를 통해 비밀(S)를 계산한 후, 비밀의 복원을 완료한다.

$$f(x) = \sum_{j=1}^{t} \left(y_j \prod_{1 \leq o \leq t, o \neq j} \frac{x - x_o}{x_j - x_o} \right) \bmod p \quad (2)$$

단, x_j와 x_o는 순번이 j번과 o번째인 참가자의 고유값을 각각 의미하고, y_j는 $f(x_j)$에 대응되는 값이며, p는 소수이다.

3. 암호화된 이미지에서 대칭키 암호 알고리듬을 이용한 가역 비밀이미지 공유 기법

본 절에서는 제안하는 암호화된 이미지에서 대칭키 암호 알고리듬을 이용한 가역 비밀이미지 공유 기법의 전체적인 개요를 설명하고, 암호화된 이미지의 생성 과정, 비밀이미지의 공유 과정과 복원 과정을 각각 알고리듬으로 기술한다.

3.1 용어 정의와 제안하는 기법의 개요

본 논문에서는 제안하는 기법은 Shamir의 (t,n)-threshold 기법에 기반을 두고, 그레이스케일(gray-

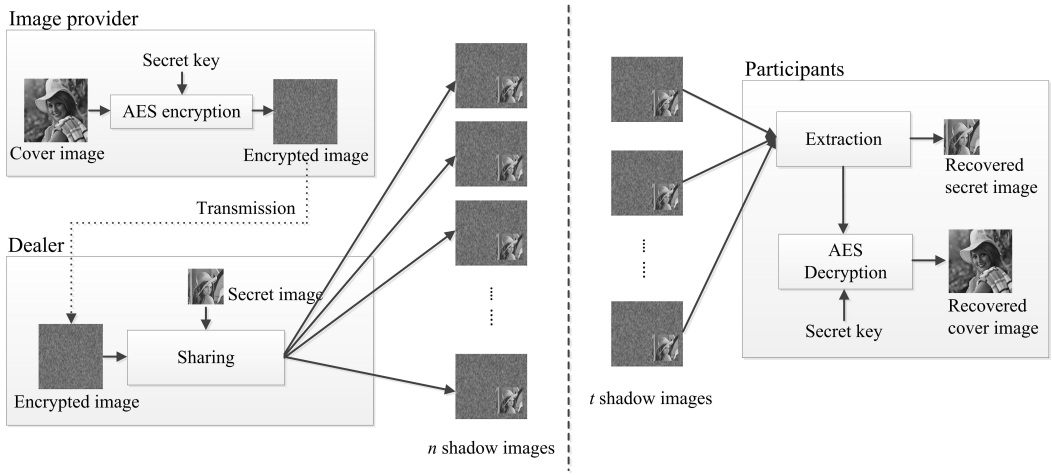

Fig. 2. Flowchart of the proposed scheme.

scale) 이미지의 정보 손실을 방지하기 위해 유한 체 상에서의 다항식 연산을 수행한다. 제안하는 기법의 개요는 Fig. 2와 같고, 각각의 사용자가 수행하는 역할은 다음과 같다.

이미지 제공자는 자신이 소유한 커버이미지를 대칭키 암호 알고리듬을 이용하여 암호화된 이미지를 생성한다. 암호화된 이미지를 전송받은 딜러는 자신이 은닉하고자 하는 비밀이미지를 새로운 비밀이미지 공유 방법을 이용하여 암호화된 이미지 내에 숨긴 후 n명의 참가자에 대한 공유 이미지를 생성하여 참가자에게 각각 분배한다. 한편, 임의의 참가자들이 본래의 비밀이미지를 복원하기 원한다면, 적어도 t명 이상의 참가자들로부터 공유 이미지를 수집한 후 본래의 비밀 데이터를 Lagrange 보간법을 이용하여 본래의 다항식을 복원한 후 비밀이미지를 복원하고, 본래의 암호화된 이미지를 얻게 된다. 이를 참가자 자신이 소유한 비밀키를 이용하여 복호화 과정을 수행하면 본래의 커버이미지를 확인하게 된다. 이를 통해 딜러는 이미지 제공자로부터 전달받은 이미지를 확인할 수 없기 때문에 이미지 제공자와 참가자 간의 안전한 저작권이 보장되는 동시에 이미지 제공자와 참가자 또는 딜러와 참가자들 간의 이중 인증을 수행할 수 있는 장점이 존재하게 된다. 제안하는 기법의 알고리듬을 설명하기 위해 사용되는 용어는 Table 1과 같다. 커버이미지, 비밀이미지, 참가자 P_i의 공유 이미지를 각각 CI, SI, SHI_{P_i}로 표기한다. M과 L은 각각 CI와 SHI_{P_i} 및 SI의 행(row)과 열(column) 크기를 지칭하고, 각 이미지 내에 존재하는 C_l, S_l, SH_l은 8비트 단위의 픽셀 값으로 나타내며, 다항식 $f(x)$의 최고차항의 차수(degree)는 임계값 t에 의해 결정된다.

3.2 암호화된 이미지 생성 과정

본 과정에서는 이미지 제공자에 의해 자신이 소유한 커버이미지로부터 암호화된 이미지를 생성한다.

Table 1. The definition of terminology

Terms	Description
$CI=\{C_0, C_1, ..., C_{L^2-1}\}$	A set of pixels in a cover image (CI) with $L\times L$
$EI=\{E_0, E_1, ..., E_{L^2-1}\}$	A set of pixels in an encrypted image (EI) with $L\times L$
$SI=\{S_0, S_1, ..., S_{M^2-1}\}$	A set of pixels in a secret image (SI) with $M\times M$
P_i	i-th participant
$SHI_{P_i}=\{SH_0, SH_1, ..., SH_{L^2-1}\}$	A set of pixels in a shadow image (SHI) for i-th participant with $L\times L$
$f_j(x)$	j-th polynomial of $(t-1)$-degree for secret image sharing

본 절에서는 제안하는 기법의 암호화된 이미지 생성 과정을 단계별로 상세하게 기술한다.

입력(input) : 커버이미지
출력(output) : 암호화된 이미지와 공유된 비밀키

step 1 : 이미지 제공자는 커버이미지의 암호와 복호를 수행하기 위해 참가자들과 공유할 비밀키(K)를 선택한다. 선택된 비밀키의 크기는 AES 표준 알고리듬의 권고 사항에 따라 128비트, 192비트, 256비트 중 하나로 선택할 수 있다.

step 2 : 선택된 비밀키(K)의 크기에 따라 AES 표준 알고리듬 내의 수행할 라운드 횟수를 결정하고, 커버이미지의 픽셀 값을 비트로 표현하여 128비트씩 나누어 순차적으로 AES 표준 알고리듬을 식 (3)과 같이 수행하여 임시의 암호화된 이미지(TI)를 생성한다.

$$TI=\{AES(T_0),AES(T_0),...,AES(T_{(L^2-1)/16})\}, \quad (3)$$

단 T_m $\left(0\le m\le \frac{L^2}{16}-1\right)$은 16개의 커버이미지 내의 픽셀들을 연결한 값으로 $T_m=C_{16m}\|C_{16m+1}\|\cdots\|C_{16m+15}$와 같이 표현할 수 있다.

step 3 : 생성된 임시의 암호화된 이미지를 블록 암호 연산(block cipher operation) 기법 중 하나인 카운터 모드(counter mode: CTR)을 이용하여 선택하여 암호화된 이미지(EI)를 식 (4)와 같이 생성한다.

$$EI=\{CTR(AES(T_0))\|CTR(AES(T_1))\|...\| CTR(AES(T_{(L^2-1)/16}))\}, \quad (4)$$

단 '||'은 $CTR(AES(T_m))$간의 연결(concatenation)을 의미한다.

step 4 : 생성된 암호화된 이미지(EI)를 딜러에게 개방된 네트워크를 통해 전송하고, 비밀키(K)는 모든 참가자들에게 안전한 네트워크를 통해 분배한다.

3.3 공유 이미지 생성 및 분배 알고리듬

본 과정은 이미지 제공자로부터 전달받은 암호화된 이미지 내에 비밀이미지를 딜러에 의해 삽입한 후 생성된 공유 이미지를 해당 참가자에게 분배한다. 이를 위해 암호화된 이미지의 픽셀 값과 비밀이미지의 픽셀 값을 이용하여 다항식을 생성한 후 해당 참가자의 인덱스 값을 이용해 함수 값을 생성한 후 각각의 암호화된 이미지 내에 삽입하게 된다.

입력(input) : 암호화된 이미지, 비밀이미지
출력(output) : n개의 공유 이미지

step 1 : j번째 암호화된 이미지 블록(B_j)를 EI로부터 식(5)와 같이 생성한다. B_j는 8비트로 구성되고, B_j의 개수는 EI의 크기에 의해 결정된다. 마지막 B_j가 8비트로 구성되지 못할 경우 알려진 패딩 방법을 이용해 8비트를 구성한다.

$$B_j=LSBe_2(E_{4j})\|LSBe_2(E_{4j+1})\|LSBe_2(E_{4j+2})\| LSBe_2(E_{4j+3}), \quad (5)$$

단 $LSBe_2$는 2비트 LSB 추출(extraction)을 의미하고, j의 범위는 $0\le j\le \frac{L^2}{4}-1$이다.

step 2 : B_j를 이용하여 다항식 $f_j(x)$를 식(6)과 같이 생성한다.

$$f_j(x)=B_j+S_0x+\cdots+S_{t-3}x^{t-2}+x^{t-1}\ (\mathrm{mod}\ m(x)), \quad (6)$$

단 $m(x)$는 유한 체(GF(2^8))상에서의 기약다항식(irreducible polynomial)을 의미하고, $0\le j\le \frac{L^2}{4}-1$이며, S_t의 개수는 임계값이 t일 경우 $t-2$개가 다항식의 계수로 삽입된다.

step 3 : i번째 참가자(P_i)의 함수 값 $y_j^{P_i}$를 식 (7)과 같이 계산한다.

$$y_j^{P_i}=f_j(x_{P_i})=b_7b_6b_5b_4b_3b_2b_1b_0, \quad (7)$$

단 x_{P_i}는 i번째 참가자의 고유값을 의미하고, $0\le P_i\le n$이다.

step 4 : 생성된 $y_j^{P_i}$를 i번째 참가자의 공유 이미지 SHI_{P_i}를 구성한다. SHI_{P_i}를 구성은 Fig. 3과 같이 EI의 연속된 4개의 픽셀에 대해 $y_j^{P_i}$를 2비트씩 나누어 각 픽셀 내에 2비트 LSB 대체 방법을 이용하여 삽입한다. 다른 참가자에 대한 공유 이미지도 위와 같은 과정을 반복하여 구성한다.

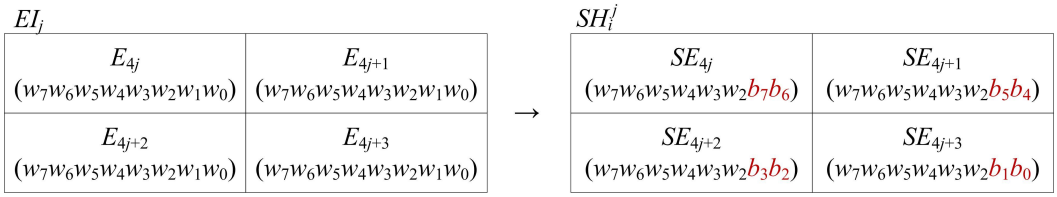

Fig. 3. Example of generating the i-th shadow image.

***step* 5 :** 생성된 공유 이미지 SHI_{P_i}를 i번째 $(1 \le i \le n)$ 참가자에게 개방된 네트워크를 통해 분배한다.

3.4 비밀이미지와 커버이미지 복원 과정

본 과정은 비밀이미지와 암호화된 이미지를 Lagrange 보간법에 의해 복원을 수행한다. 비밀이미지 복원 후 각 참가자는 이미지 제공자로부터 전송받은 비밀키(K)를 이용하여 복원된 암호화된 이미지를 복호화 과정을 통해 본래의 커버이미지를 확인한다.

***입력(input)* :** t개의 공유 이미지, 비밀키
***출력(output)* :** 복원된 비밀이미지, 복원된 커버이미지

***step* 1 :** i번째 참가자의 공유 이미지 SHI_{P_i}내의 연속되는 4개의 픽셀로부터 2비트 LSB를 추출하여 $y'^{P_i}_j$를 식 (8)과 같이 구성한다.

$$\begin{aligned} y'^{P_i}_j &= b_7'b_6'b_5'b_4'b_3'b_2'b_1'b_0' \\ &= LSBe_2(SH_{4j}) \| LSBe_2(SH_{4j+1}) \| LSBe_2(SH_{4j+2}) \| \\ &\quad LSBe_2(SH_{4j+3}) \end{aligned} \tag{8}$$

***step* 2 :** 식(9)와 같은 Lagrange 보간법을 이용하여 다항식 $f'_j(x)$를 식(10)과 같이 복원한다.

$$f'_j(x) = \sum_{l=1}^{t}\left(y'^{P_i}_j \times \prod_{1 \le k \le t, k \ne l} \frac{x - x_{P_k}}{x_{P_l} - x_{P_k}} \right) \bmod m(x), \tag{9}$$

$$f'_j(x) = B'_j + S_0 x + \cdots + S_{t-3}x^{t-2} + x^{t-1} (\bmod\ m(x)), \tag{10}$$

단 $m(x)$는 유한 체(GF(2^8))상에서의 기약다항식(irreducible polynomial)을 의미하고, $0 \le j \le \frac{L^2}{4} - 1$이다.

***step* 3 :** $f'_j(x)$의 일반항의 계수들로부터 비밀이미지의 픽셀들$\{S_0, S_1, \ldots, S_{M^2-1}\}$을 수집한 후 본래의 비밀이미지를 복원한다.

***step* 4 :** 각 참가자는 $f'_j(x)$의 상수항으로부터 암호화된 이미지 블록 B'_j를 이용하여 본래의 암호화된 이미지 EI'를 복원한다.

***step* 5 :** 각 참가자는 복원된 암호화된 이미지 EI'를 비밀키(K)와 AES 표준 알고리듬을 이용하여 복호화과정을 수행한 후 본래의 커버이미지를 확인한다.

4. 실험 및 결과 분석

본 절에서는 실험을 통하여 제안한 기법과 다른 기법들 [13-15] 간의 삽입용량(embedding capacity)과 PSNR(Peak Signal to Noise Ratio)을 비교 분석한다. 이를 통하여 본 논문에서 제안한 기법의 우수성을 검증한다.

4.1 실험 도구와 평가 기준

대부분의 비밀이미지 공유 기법들에 대한 성능 평가는 크게 두 가지 측정 기준이 사용된다. 첫 번째는 삽입용량으로서 커버이미지 내에 비밀 이미지를 숨겨 공유 이미지를 생성하는 경우 공유 이미지 내에 얼마나 많은 비밀 데이터가 삽입되었는지를 측정하는 것이다.

다른 측정 기준은 커버와 공유 이미지 간의 이미지 왜곡(distortion)이다. 비밀이미지 공유 기법의 목적은 공격자에게 커버이미지 내에 비밀 데이터를 은닉했는지를 알 수 없게 하는 것이므로, 커버와 공유 이미지 간의 왜곡은 매우 중요하다. 왜곡을 측정하기 위해서는 PSNR을 사용하고, 이것은 식 (11)과 같이 표현된다.

$$PSNR = 10 \times \log\left(\frac{MAX^2}{MSE} \right), \tag{11}$$

단 MSE는 에러(error) 평균의 제곱(mean squared error)값으로 식 (12)와 같이 표현되고, MAX는 한 픽

셀이 표현할 수 있는 최댓값(maximum value)을 의미하는 것으로 본 논문의 실험에서는 그레이스케일 이미지를 사용하므로 255를 사용한다.

$$MSE = \frac{1}{4M^2} \sum_{i=0}^{4M^2-1} [E_i - SH_i]^2, \quad (12)$$

단 E_i와 SH_i는 본 논문에서 사용하는 암호화된 이미지와 공유 이미지의 i번째 픽셀 값을 각각 의미한다. $PSNR$ 수치는 높으면 높을수록 두 이미지 간의 왜곡이 거의 없는 것(최대값: ∞)이고, 낮으면 낮을수록 두 이미지 간의 왜곡은 매우 많아져(최소값: 0), 사람의 시각으로 인지할 수 있게 된다. 일반적으로 사람이 인지할 수 없는 왜곡의 PSNR 값은 $30dB$로서 이 값보다 적을 경우 왜곡 확인이 가능하다.

실험에 사용된 커버이미지는 Fig. 4와 같이 비밀이미지 공유 기법들의 실험에서 일반적으로 사용하는 그레이스케일 이미지 8개를 사용했고, 각 이미지의 크기는 512×512로 고정하였다.

본 실험에서는 $(2,3)$-threshold과 $(4,4)$-threshold (Wang & Shyu[20] 기법에 해당)인 경우에 대해 실험을 수행했다. 비밀이미지는 난수를 발생하는 C++ 라이브러리를 이용하여 비트열(bitstream)을 생성한 후 이를 8비트 단위로 나누어 하나의 픽셀로 사용하였다.

Table 2. The comparison of the embedding capacity (unit: bit)

Test images	Lin & Tsai [13]	Wang & Shyu [14]	Chang et al. [15]	Proposed
Lena	524,288	131,072	786,432	524,288
Baboon	524,288	131,072	786,432	524,288
Airplane	524,288	131,072	786,432	524,288
Peppers	524,288	131,072	786,432	524,288
Boat	524,288	131,072	786,432	524,288
Man	524,288	131,072	786,432	524,288
Elaine	524,288	131,072	786,432	524,288
Woman	524,288	131,072	786,432	524,288

4.2 삽입 용량의 실험 결과 및 분석

본 논문의 실험에서는 공유된 이미지 내에 삽입된 비밀 데이터의 용량을 측정하는 것으로 기준을 정하여 다른 기법들[13-15]과 비교를 수행했다. Table 2는 삽입 용량에 대한 다른 기법들과 제안한 기법의 결과를 보여주고 있다. Table 2에서 8개의 테스트 이미지들에 대해 각 기법마다 모두 동일한 값이 나타난 이유는 공간 영역(spatial domain) 내에서의 LSB 대체 방법을 사용했기 때문이다. Wang과 Shyu[14]의 기법은 일반적인 비밀이미지 공유 기법들과 달리 비밀이미지를 분할하여 공유된 이미지로 생성하고, n명의 참가자 중 n명 모두 참가해야 완벽하게 비밀이

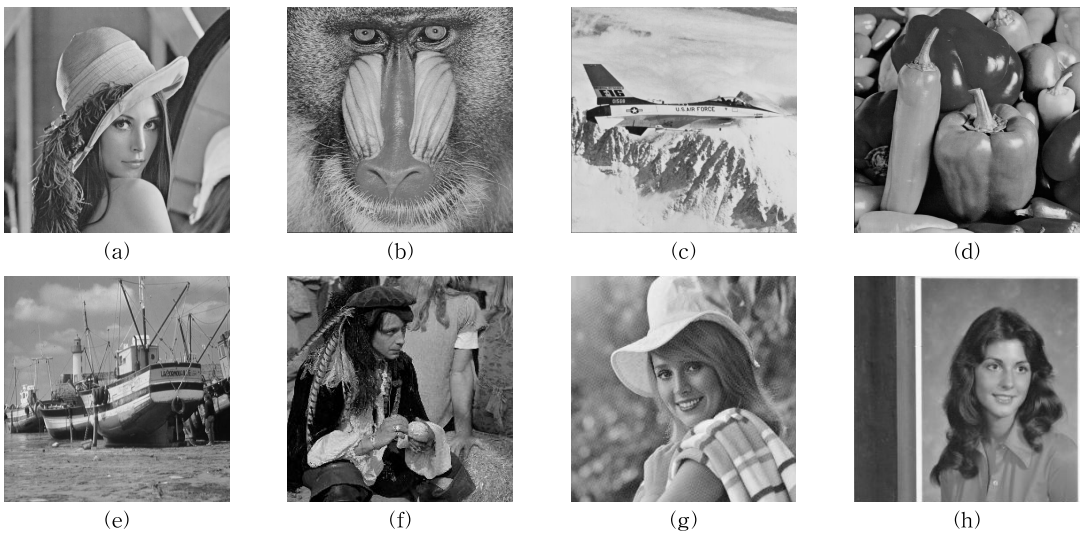

Fig. 4. Eight grayscale test images: (a) Lena, (b) Baboon, (c) Airplane, (d) Peppers, (e) Boat, (f) Man, (g) Elaine and (h) Woman.

미지가 복원된다는 특징이 있기 때문에 본 실험에서는 그들이 제안한 기법의 모드 중 가장 우수한 결과를 보여주는 'progressive' 모드와 (4, 4)-threshold 일 경우에 대해 수행했고, 다른 기법들의 경우 2비트 또는 3비트 LSB 대체 방법을 사용하였기 때문에 이를 기준으로 실험을 수행했다. 제안한 기법은 암호화된 이미지 내의 픽셀에 대해 2비트 LSB 대체 방법을 사용했기 때문에 524,288비트의 삽입 용량을 나타냈고, Lin과 Tsai[13]의 기법 내에서 사용된 방법인 4개 픽셀을 하나의 블록으로 매핑(mapping)하여 비밀이미지의 한 픽셀을 삽입하는 과정은 동일하지만 블록 내의 첫 번째 픽셀에는 삽입하지 않고, 두 번째 픽셀부터 연속적으로 3비트씩 총 9비트를 삽입한다. 이중 1비트는 오류 수정을 위한 비트의 역할을 수행하기 때문에 삽입용량 측정에선 제외했다. 그러므로 Lin과 Tsai[18] 또한 524,288비트를 삽입했다. 한편, Chang 등[15]의 기법은 인증 기능을 추가한 것이기 때문에 3비트 LSB 대체 방법을 사용하여 커버이미지 내의 모든 픽셀에 대해 비밀 데이터 2비트와 1비트의 인증을 각각 삽입했다. 이로 인해 다른 기법들에 비해 삽입 용량이 커졌고, 그 결과 786,432비트를 삽입했다.

4.3 PSNR의 실험 결과 및 분석

Table 3은 8개의 그레이스케일 이미지들에 대한 PSNR의 실험 결과를 나타낸다. Wang과 Shyu[14]의 기법은 공유 이미지가 의미 없는 것으로 생성되기 때문에 실험에서 제외했다. Lin과 Tsai[13]가 제안한 것과 본 논문에서 제안한 기법의 삽입 용량은 동일했지만 제안하는 기법의 PSNR의 결과가 더 우수했다. Chang 등[15]의 기법은 커버이미지의 모든 픽셀에 대해 3비트 LSB 대체 방법을 사용했고, Lin과 Tsai[13]의 기법은 커버이미지의 한 블록 당 3개의 픽셀에 대해 3비트 LSB 대체 방법을 사용했기 때문에 일반적으로는 Lin과 Tsai[13]가 제안한 기법의 PSNR에 대한 결과가 더 우수해야 한다. 그러나 Chang 등[15]은 이러한 단점을 극복하기 위해 1비트의 인증을 해당 픽셀 값과 유사하게 생성해 삽입하므로 Lin과 Tsai[13] 기법의 PSNR 결과보다 더 우수했다.

Table 3. The comparison of PSNR between the proposed and previous schemes (unit: dB)

Test images	Lin & Tsai [13]	Wang & Shyu [14]	Chang et al. [15]	Proposed
Lena	39.16	-	40.92	45.13
Baboon	39.15	-	40.92	43.90
Airplane	39.21	-	40.87	45.48
Peppers	39.20	-	40.96	44.41
Boat	39.18	-	40.93	44.11
Man	39.18	-	40.93	45.13
Elaine	39.13	-	40.89	45.10
Woman	39.18	-	40.93	44.11
Average	**39.17**	**-**	**40.92**	**44.67**

제안한 기법의 경우 특수하게 암호화된 이미지 내에 비밀이미지를 삽입하는 것이기 때문에 기존의 커버이미지 대신 암호화된 이미지와 비밀이미지가 삽입된 공유 이미지에 대해 PSNR을 비교했다. 이에 대한 결과는 평균 44.67dB로서 기존의 기법들에 비해 약 4dB정도가 높은 것을 알 수 있었다. 이러한 결과를 통해 제안한 기법의 PSNR 실험 결과는 기존의 제안되었던 기법들에 비해 우수함을 알 수 있었다. 물론 PSNR의 수치를 더 높이기 위해 1비트 LSB 대체 방법을 사용해도 되지만 삽입 용량과의 상관관계를 고려해 본 논문에서는 2비트 LSB 대체 방법을 사용했다. 이를 통해 본 논문에서 제안한 기법은 기존의 기법들에 비해 이중 인증 기능을 제공하면서도 이미지 제공자와 딜러 간의 이미지 확인이 불가능하다는 장점을 보이는 동시에 기존의 제안된 기법들에 비해 삽입 용량과 PSNR의 결과가 비슷하게 유지되거나 우위에 있음을 알 수 있었다.

5. 결 론

본 논문에서는 암호화된 이미지에 기반을 둔 AES 대칭키 암호 알고리듬을 이용한 비밀이미지 공유 기법을 제안했다. 제안한 방법에서의 비밀이미지 공유 과정은 기존의 기법들과 달리 이미지 제공자가 자신이 전달할 커버이미지를 AES 알고리듬과 공유된 비밀키를 이용해 암호화된 이미지를 생성하고, 이를 딜러에게 전달한 다음 딜러는 유한체 상에서의 다항식 연산을 통해 공유 이미지를 생성한 후 이를 해당하는 참가자 전달한다. 공유 이미지들로부터 본래의 비밀이미지를 복원하는 과정은 공유하는 과정을 역으로 진행한다. 실험결과에서는 PSNR과 비밀데이터의 삽입용량은 각각 44.67dB와 $(t-2)/4$bpp의 평균값을

나타냈다. 또한, 기존의 기법들과 달리 삽입용량에 관계없이 PSNR의 값의 44dB에 가깝게 유지하는 것을 확인했다.

제안한 방법의 장점은 다음과 같다. 첫째, 제안한 방법은 각각의 참가자에 대해 딜러와 이미지 제공자에 대해 이중 인증을 제공한다. 둘째, 제안한 방법에서는 이미지 제공자와 딜러의 역할을 나누었기 때문에 이미지 제공자가 전달하는 커버이미지에 대해 강력한 프라이버시를 제공한다. 셋째, Lin과 Chan이 제안한 방법의 모든 문제점을 해결했다. 즉, 오버플로우와 전체 참가자의 수가 제한되는 문제를 유한체 연산을 이용하여 해결할 수 있었다.

향후 연구로는 정보은닉분야에서 사용되는 PVD, 히스토그램 시프팅 등의 다양한 삽입방법을 적용하여 비밀데이터의 삽입용량을 증가시킬 수 있도록 할 것이다.

REFERENCE

[1] D.R. Stinson, *Cryptography Theory and Practice*, Chapman & Hall/CRC Press, United States of America, 2006.

[2] S. William, *Cryptography and Network Security*, Prentice Hall, United States of America, 2006.

[3] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, United States of America, 1996.

[4] A. Shamir, "How to Share a Secret," *Communications of ACM*, Vol. 22, No. 11, pp. 612-613, 1979.

[5] I. Mitsuru, S. Akira, and N. Takao, "Secret Sharing Scheme Realizing General Access Structure," *Electronics and Communications in Japan*, Vol. 72, Issue 9, pp. 1520-6440, 1989.

[6] S. Berry, "A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting," *Advances in Cryptology-CRYPTO'99 Lecture Notes in Computer Science,* Vol. 1666, pp. 148-164, 1999.

[7] F. Paul, "A Practical Scheme for Non-Interactive Verifiable Secret Sharing," *Proceeding of 28th Annual Symposium on Foundations of Computer Science*, pp. 427-438, 1987.

[8] B. Josh and L. Jerry, "Generalized Secret Sharing and Monotone Functions," *Advances in Cryptology-CRYPTO'88 Lecture Notes in Computer Science,* Vol. 403, pp. 27-35, 1990.

[9] A. Beimel and B. Chor, "Secret Sharing with Public Reconstruction," *IEEE Transactions on Information Theory*, Vol. 44, No. 5, pp. 1887-1896, 1998.

[10] C. Thien and J. Lin, "Secret Image Sharing," *Computers & Graphics*, Vol. 26, No. 5, pp. 765-770, 2002.

[11] C. Thien and J. Lin, "An Image Sharing Method with User-friendly Shadow Images," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, No. 12, pp. 1161-1169, 2003.

[12] C. Yang, T. Chen, K. Yu, and C. Wang, "Improvements of Image Sharing with Steganography and Authentication," *Journal of Systems & Software*, Vol. 80, No. 7, pp. 1070-1076, 2007.

[13] C. Lin and W. Tsai, "Secret Image Sharing with Steganography and Authentication," *Journal of Systems and Software*, Vol. 73, No. 3, pp. 405-414, 2004.

[14] R. Wang and S. Shyu, "Scalable Secret Image Sharing," *Journal of Signal Processing: Image Communication*, Vol. 22, No. 4, pp. 363-373, 2007.

[15] C. Chang, Y. Hsieh, and C. Lin, "Sharing Secrets in Stego Images with Authentication," *Journal of Pattern Recognition*, Vol. 41, No. 10, pp. 3130-3137, 2008.

[16] C. Lin, L. Liao, K. Hwang, and S. Chen, "Reversible Secret Image Sharing with High Visual Quality," *Multimedia Tools and Applications*, Vol. 70, No. 3, pp. 1729-1747, 2014.

[17] U. Mustafa, G. Ulutas, and V.V. Nabiyev, "Invertible Secret Image Sharing for Gray

Level and Dithered Cover Images," *Journal of Systems and Software*, Vol. 86, No. 2, pp. 485-500, 2013.

[18] B. Jeon, G. Lee, K. Jung and K. Yoo, "Reversible Secret Image Sharing Scheme Using Histogram Shifting and Difference Expansion," *Journal of Korea Multimedia Society*, Vol. 17, No. 7, pp. 849-857, 2014.

[19] X. Zhang, "Reversible Data Hiding in Encrypted Image," *IEEE Signal Processing Letters*, Vol. 18, No. 4 pp. 255-258, 2011.

[20] W. Hong, T. Chen, and H. Wu, "An Improved Reversible Data Hiding in Encrypted Images using Side Match," *IEEE Signal Processing Letters,* Vol. 19, No. 4 pp. 199-202, 2012.

[21] B. Jang, S. Lee, and K. Kwon, "Active Video Watermarking Technique for Infectious Information Hiding System," *Journal of Korea Multimedia Society*, Vol. 15, No. 8, pp. 1017-1030, 2012.

[22] S. Hyun, S. Shin, and K. Yoo, "A Proactive Secret Image Sharing Scheme over GF(2^8)," *Journal of Korea Multimedia Society*, Vol. 16, No. 5, pp. 577-590, 2013.

전 병 현

1991년 2월 경일대학교 전자계산학과 공학사
2000년 2월 대구대학교 산업정보대학 정보관학 공학석사
2014년 2월 경북대학교 IT대학 컴퓨터학부 박사수료

2004년 1월~2009년 6월 영진전문대학 전자정보계열 교수
2004년 1월~현재 학)영진교육재단 영진모빌스 총괄팀장
2011년 3월~현재 영진사이버대학 정보통신공학과 교수
관심분야 : 암호학, 네트워크보안, 스테가노그래피, 데이터베이스

신 상 호

2006년 8월 금오공과대학교 응용수학/컴퓨터공학 이/공학사
2008년 8월 경북대학교 전자전기컴퓨터학부 공학석사
2014년 8월 경북대학교 IT대학 컴퓨터학부 공학박사

2015년 2월~현재 동국대학교 경주캠퍼스 실감미디어 성과확산사업단 선임연구원
관심분야 : 양자 셀룰라 오토마타, 양자암호, 비밀이미지 공유, 실감미디어

정 기 현

1995년 2월 경북대학교 컴퓨터공학과 공학사
1997년 2월 경북대학교 컴퓨터공학과 공학석사
2007년 8월 경북대학교 컴퓨터공학과 공학박사
1997년 2월~2003년 2월 국방과학연구소 선임연구원

2003년 9월~2015년 2월 영진전문대학 컴퓨터정보계열 교수
2015년 3월~현재 경일대학교 사이버보안학과 교수
관심분야 : 정보보호, 디지털 워터마킹, 디지털 포렌식, 스테가노그래피, 게임/모바일프로그래밍

이 준 호

1996년 2월 경북대학교 전자공학과 공학사
1998년 2월 경북대학교 전자공학과 공학석사
1998년 2월~현재 국방과학연구소 선임연구원

관심분야 : 정보보호, 스테가노그래피, 소프트웨어공학, 전투체계

유 기 영

1976년 2월 경북대학교 수학교육과 이학사
1978년 2월 한국과학기술원 전산학과 공학석사
1992년 3월 미국 Rensselaer Polytechnic Institute 전산학과 공학박사

1978년 3월~현재 경북대학교 IT대학 컴퓨터학부 교수
관심분야 : 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜