행렬 분해와 공격자 구조를 이용한 비밀이미지 공유 기법

현승일[†], 신상호^{††}, 유기영^{***}

Secret Image Sharing Scheme using Matrix Decomposition and Adversary Structure

Suhng-Il Hyun[†], Sang-Ho Shin^{††}, Kee-Young Yoo^{***}

ABSTRACT

In Shamir's (t, n) -threshold based secret image sharing schemes, there exists a problem that the secret image can be reconstructed when an arbitrary attacker becomes aware of t secret image pieces, or t participants are malicious collusion. It is because that utilizes linear combination polynomial arithmetic operation. In order to overcome the problem, we propose a secret image sharing scheme using matrix decomposition and adversary structure. In the proposed scheme, there is no reconstruction of the secret image even when an arbitrary attacker become aware of t secret image pieces. Also, we utilize a simple matrix decomposition operation in order to improve the security of the secret image. In experiments, we show that performances of embedding capacity and image distortion ratio of the proposed scheme are superior to previous schemes.

Key words: Secret Image Sharing, Adversary Structure, Matrix Decomposition, Data Hiding

1. 서 론

최근 클라우드 컴퓨팅의 등장과 함께 제공되는 서비스들은 개개인의 데이터베이스에 대한 암호화 혹은 임의의 사용자가 접근할 경우 이를 효과적으로 제어할 수 있는 안전한 인증 기법이 필요하다. 현재 클라우드 컴퓨팅 환경 내에서 데이터 암호화 알고리즘 혹은 개인에 대한 인증 기법에 대한 많은 연구가 진행된 상황이지만 임의의 그룹 내에서 다수의 사용자들을 동시에 인증할 수 있는 기법에 대한 연구는

미흡한 상태이다[1-3]. 이를 효율적으로 해결하기 위한 여러 가지 기법들 중 하나가 비밀 공유이다.

비밀 공유(secret sharing)는 비밀키(secret key)의 소유자가 한 명이 아닌 다수의 인증된 참가자들이고, 이 때 각 참가자는 비밀키의 일부 조각을 소유하게 된다. 비밀 공유 기법은 1979년 Adi Shamir[4]와 George Blakley[5]에 의해 각각 처음으로 제안되었다. 1994년과 1996년 Naor와 Shamir[6,7]가 제안한 기법은 이진 비밀이미지를 코드북에 기반을 두고 있다. 2002년에는 Thein과 Lin[8]에 의해 처음으로

※ Corresponding Author : Kee-Young, Yoo, Address: (702-701) 80 Daehakro, Bukgu, Daegu, Korea, TEL : +82-53-950-5555, FAX : +82-53-957-4846, E-mail : yook@knu.ac.kr

Receipt date : Mar. 18, 2014, Revision date : Jul. 4, 2014
Approval date : Jul. 7, 2014

[†] Division of Info and Comm, Yeungjin Cyber College
(E-mail : mipal@yjc.ac.kr)

^{††} School of Computer Science and Engineering Kyung-pook National University
(E-mail : shshin80@infosec.knu.ac.kr)

^{***} School of Computer Science and Engineering Kyung-pook National University

※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(NRF-2012R1A1A2008348) and the IT R&D program of MSIP/IITP. [10041145, Self-Organized Software platform(SoSP) for Welfare Devices]

그레이스케일(greyscale) 이미지에 대한 비밀이미지 공유 기법이 제안되었다. 그러나 비밀이미지에 대한 손실이 발생하는 단점이 존재하였고, 이를 보완하기 위해 여러 기법들이 제안되었다[9-11]. 한편 2010년에는 Lin과 Chan[12]에 의해 가역(reversible)이 가능한 비밀이미지 공유 기법이 제안되었고, 임계(threshold)값인 t 에 따라 비밀이미지의 삽입 용량(embedding capacity)이 비례적으로 증가하는 장점이 존재했다. 그러나 $t-1$ 명 이하가 공모되더라도 비밀이미지를 복원할 수 있거나 삽입 용량이 증가할수록 공유된 이미지(shadow image)의 왜곡 정도(peak signal to noise ratio: PSNR)가 심해진다는 단점도 존재했다. 기존에 제안된 대부분의 비밀이미지 공유 기법들은 (t,n) -threshold에 기반을 두어 실제의 환경에서는 공격자에 의해 t 명 이상의 비밀 조각들을 모두 수집할 수 있고, 이것은 기존의 비밀이미지 공유 기법에 큰 취약점이 될 수 있다[25,28]. 이를 해결하기 위해 식 (1)과 같이 선형결합 다항식(linear combination polynomial) 연산에 기반을 두어 비밀 이미지를 공유하였다.

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \quad (1)$$

n 명에 대한 비밀이미지 공유 단계에서, 임의의 공유값 k_i ($1 \leq i \leq n$)은 식 (1)의 다항식에 의해 계산되고, 이를 공유된 이미지로 생성하여 i 번째 참가자에게 나누어준다. 그러나 어떤 참가자가 잘못된 비밀 조각을 제출했는지를 알 수가 없는 Tompa-Woll 공격에 취약했다. 이것을 해결하기 위해서는 선형결합 다항식 연산이 아닌 새로운 기법을 이용해야 한다.

본 논문에서는 행렬 분해(matrix decomposition)와 공격자 구조(adversary structure)를 이용하여 이와 같은 문제점을 해결한다. 다항식에 의해 생성된 비밀조각들을 모두 공개하더라도 행렬 분해 연산에 의해 기존의 안전성은 그대로 유지된다. 또한, (t,n) -threshold에 기반을 두고 있지만 공격자 구조를 이용하기 때문에 t 명 이상의 비밀 조각 정보를 공격자가 알고 있더라도 본래의 비밀이미지를 복원할 수 없게 된다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 행렬 분해와 공격자 구조, Shamir의 (t,n) -threshold 기법에 대해 소개한다. 3장에서는 제안하는 기법에 대한 알고리즘을 자세히 설명하고, 이에 대한 실험

및 결과 분석을 4장에서 다루며, 5장에서 결론을 맺는다.

2. 관련 연구

제안하는 기법은 행렬 분해와 공격자 구조를 이용해 공유된 이미지를 생성하고, 참가자들에게 분배한다. 이를 위해 행렬 분해, 공격자 구조 및 Shamir의 (t,n) -threshold 기법에 대해 소개한다.

2.1 Shamir의 (t,n) -threshold 비밀 공유 기법

1979년 Shamir가 제안한 기법은 초기화 과정, 공유값 분배과정, 그리고 비밀키 복원과정으로 나누어져 있다. 전 과정에서 하나의 비밀키로부터 공유값을 생성, 분배, 그리고 복원하는 역할은 딜러가 수행한다. 딜러는 합법적으로 인증된 자로 가정하고, 각각의 과정은 단계별로 아래와 같다.

초기화 과정에서 딜러는 Z_p 상의 조건 $p \geq n+1$ 을 만족하는 0이 아닌 서로 다른 원소 n 개의 x_i 를 선택한다. 단, i 는 참가자들의 인덱스로 $1 \leq i \leq n$ 을 만족한다. 임의의 i 에 대해서, 딜러는 x_i 를 i 번째 참가자 P_i 에 대응시켜준다.

공유값 분배과정에서 공유하려는 비밀키(K)를 Z_p 상의 임의의 원소(즉, $K \in Z_p$)로 가정하면 딜러는 Z_p 상에서 $t-1$ 개의 독립적인 $a_1, a_2, \dots, a_{t-1}$ 원소들을 비밀스럽게 선택한다. 임의의 i ($1 \leq i \leq n$)에 대해, 딜러는 다음의 식 (2)을 이용해 공유값 $y_i = a(x_i)$ 값을 계산한다.

$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j \pmod{p} \quad (2)$$

끝으로 딜러는 i 번째 참가자 P_i 에 대응하는 공유값(y_i)을 분배한다.

비밀 복원과정에서 딜러는 n 명의 참가자 중 t 명 또는 그 이상의 인원을 모집한 후 그 인원으로부터 임의의 참가자 P_i 가 소유한 공유 값 y_i 를 수집한다. 수집한 t 또는 그 이상(단, $t \leq n$)의 (i, y_i) 쌍들과 Lagrange 보간법을 이용하여 공유값 분배과정에서 사용했던 식 (3)을 이용하여 복원한다. 여기서 x_j 와 x_0 는 순번이 j 번과 0번째인 참가자의 고유값을 각각 의미하고, y_j 는 $a(x_j)$ 에 대응되는 값이며, p 는 소수이다.

$$a(x) = \sum_{j=1}^t \left(y_j \prod_{1 \leq o \leq t, o \neq j} \frac{x - x_o}{x_j - x_o} \right) \bmod p \quad (3)$$

달러에 의해 복원된 비밀키(K)를 계산하면 비밀키 복원이 완료된다.

2.2 행렬 분해

행렬 분해(matrix decomposition)는 특정한 구조를 가진 다른 행렬의 곱으로 나타내는 것으로 선형 방정식(linear equation)의 해 또는 선형결합 다항식의 계수를 구하는 것과 행렬 계산을 효율적 수행하는 것 등에 사용되는데 LU 분해, Jordan 분해, QR 분해 등과 같은 기법들이 존재한다. $n \times n$ 크기의 행렬 A 와 이와 유사한 형태의 행렬 B 가 주어지고, 이들의 관계가 식 (4)와 같은 경우, 악의적인 공격자가 만약 행렬 B 를 알고 있더라도, 행렬 A 를 유추할 수 있는 확률은 행렬 P 를 유추할 수 있는 확률과 동일하게 된다[13].

$$B = PA \quad (4)$$

본 논문에서는 이러한 행렬 분해의 확률적인 특징을 이용해 비밀 이미지 내의 픽셀들을 이용하여 임의의 크기의 행렬 A 를 구성하고, 이를 식 (4)를 이용하여 유사한 형태의 행렬 B 를 생성하여 이를 공개한다. 행렬 B 를 공개하더라도 공격자는 행렬 P 를 알 수 없기 때문에 결국 행렬 A 는 안전하게 된다.

2.3 접근 구조와 공격자 구조

참가자들의 부분 집합들로 구성된 집합을 Γ 로 두고, Γ 내의 부분 집합들이 t 명 이상이 공모된 참가자들의 부분집합과 동일할 경우 집합 Γ 를 접근 구조(access structure)라고 하는데, 이를 이용하여 완벽한 비밀 공유 기법(perfect secret sharing scheme)을 정의 1 같이 기술할 수 있다[14].

정의 1. 접근 구조 Γ 로 실체화된 완벽한 비밀 공유 기법은 n 명의 참가자들에게 비밀키 K 를 공유하는 방법으로 다음의 두 가지 속성을 만족해야 한다.

- 1) 참가자들의 인증된 부분집합 B 와 참가자들의 풀(pool) P 에 대해 $B \subseteq P$ 인 경우, 그들은 비밀키 K 를 복원할 수 있다.

- 2) 참가자들의 인증되지 않은 부분집합 B' 과 참가자들의 풀(pool) P 에 대해 $B' \subseteq P$ 인 경우, 그들은 비밀키 K 를 복원할 수 없다.

정의 1에 의해서 비밀키 복원이 불가능하지만 공격자가 부분집합 B 또는 이보다 더 큰 확대집합을 알게 될 경우 실제 이들은 공격을 당할 가능성이 높아지게 되는데, 이를 공격자 구조라 지칭한다. 공격자는 참가자들의 풀 P 내에 존재하는 가장 큰 부분집합($\{P_1, P_2, \dots, P_n\}$)을 제외한 모든 부분집합(즉, 진부 부분집합들의 개수만큼)을 습득 가능하고, 이러한 부분집합 들을 이용해 비밀 공유 기법을 공격할 수 있다.

정의 2. 참가자들의 풀 P 에 대해, 식 (5)과 같은 접근 구조(Γ)는 단조증가 속성을 만족하는 P 의 부분 집합들의 모임이다.

$$\Gamma = \{A \in \Gamma \mid \forall B \subset A \Rightarrow B \notin \Gamma\} \quad (5)$$

정의 3. 참가자들의 풀 P 에 대해, 식 (6)과 같은 공격자 구조($\hat{A}$)는 단조감소 속성을 만족하는 P 의 부분집합들의 모임이다.

$$\hat{A} = \{B \in \hat{A} \mid \forall A \supset B \Rightarrow A \notin \hat{A}\} \quad (6)$$

대부분의 선형결합 다항식에 기반을 둔 비밀이미지 공유 기법은 이러한 공격자 구조에 대해 고려하지 않고 있기 때문에 실제 환경에서는 공격에 대해 보안의 취약성이 그대로 존재한다. 본 논문에서는 공격자 구조를 이용하여 접근 구조에 존재하는 인증된 부분 집합들 중 하나 이상을 공격자가 획득하더라도 비밀키 복원이 불가능하게 된다.

3. 행렬 분해와 공격자 구조를 이용한 비밀이미지 공유 기법

본 절에서는 행렬 분해와 공격자 구조를 이용한 비밀이미지 공유 기법에 대해 설명한다. 먼저 커버 이미지, 비밀이미지, 임의의 참가자 $P_{(i)}$ 의 공유된 이미지를 각각 CI , SI , $SHI_{P_{(i)}}$ 로 나타내며, M 과 L 은 비밀 이미지 SI 와 CI (또는 $SHI_{P_{(i)}}$) 이미지의 행(row) 또는 열(column) 크기를 각각 지칭한다. 각 이미지 내에 존재하는 C_i , S_i , SHI_i 은 8-bit 단위의 픽셀 값으로 나타내며, 다항식 $f(x)$ 의 최고차항의 차수는 비밀 공유

의 임계값인 t 에 의해 결정된다.

3.1 초기화 과정

초기화 과정에서는 비밀이미지 공유 및 복원 과정에서 사용되는 여러 가지 변수들과 공격자 구조를 설정한다.

step 1 : 모든 참가자 n 명에 대해서, 비밀이미지 공유를 위한 임계값 t ($2 \leq t \leq n$)를 설정한다.

step 2 : 모든 참가자의 집합 $P = \{P_1, P_2, \dots, P_n\}$ 에 대해 공격자 구조 $\mathbb{A}$ 가 가질 수 있는 집합의 개수 $m = n(\mathbb{A})$ 은 P 의 진부분집합의 개수이므로, $m = 2^n - 1$ 과 같이 계산하고, 이에 해당하는 각 부분 집합은 딜러가 생성한다.

step 3 : 지수 연산과 나머지 연산을 수행하기 위해 $N = pq$ 인 두 소수 p 와 q 를 각각 임의로 선택하고, N 을 계산한다. 또, 생성자 g ($g \neq p$ 또는 q)를 범위 $[\sqrt{N}, N]$ 내에서 선택한다.

step 4 : 딜러는 각각의 참가자들에 대한 서로 다른 비밀키를 생성한다. 임의의 참가자 P_i ($1 \leq i \leq n$)에 대한 비밀키 k_i ($1 \leq i \leq n$)는 $t \times 1$ 의 행렬이고, 이들의 원소들은 범위 $[2, N]$ 내에서 임의로 선택된다. 생성된 비밀키 k_i 는 참가자 P_i 에게 비밀 채널을 통해 딜러가 안전하게 전송한다.

3.2 비밀이미지 공유 과정

본 과정은 비밀이미지를 가공하고 이를 CI 에 삽입하여 공유된 이미지를 생성하던 기존의 기법들과 달리 공격자 구조와 행렬 분해 연산을 이용하여 공유된 이미지를 생성한 후 이를 n 명의 참가자들에게 분배한다.

입력(input) : CI, SI, t, n

출력(output) : n 개의 SHI_{P_i} ($1 \leq i \leq n$), B , n 개의 $f(k_i)$

step 1 : 크기가 $M \times M$ 인 비밀이미지(SI)로부터 $t \times t$ 개의 픽셀을 추출하여 행렬 A 를 식 (7)과 같이 구성하고, 크기가 $t \times t$ 인 임의의 역행렬이 존재하는 행렬 P 를 선택한다. 이때 선택된 행렬 P 의 원소들은 나머지 연산을 위해 $[1, N]$ 범위 내에서 임의로 선택된다. 한편, 행렬 P 는 열벡터들의 집합 형태로 표현

이 가능하고, 이는 식 (8)과 같다. 행렬 분해 식 (9)을 이용해 행렬 B 를 생성하고, 이를 모든 참가자들에게 공개한다. 단, 행렬 P 의 열벡터 원소 p_j ($1 \leq j \leq t$)의 크기는 $t \times 1$ 의 행렬과 동일하다.

$$A = \begin{pmatrix} C_0 & \dots & C_{t-1} \\ C_t & \dots & C_{2t-1} \\ \vdots & \ddots & \vdots \\ C_{t(t-1)} & \dots & C_{t^2-1} \end{pmatrix} \quad (7)$$

$$P = (p_1, p_2, \dots, p_t) \quad (8)$$

$$B = PA \quad (9)$$

step 2 : 공격자 구조 내의 전체 집합 개수에 해당하는 m 에 대해, 딜러는 서로 다른 m 개의 양의 정수들 $d_1, d_2, \dots, d_m$ 을 식 (10)과 같은 조건으로 선택한다.

$$1 \leq d_1 < d_2 < \dots < d_m \leq N \quad (10)$$

한편, d_0 는 $d_0 = d_1 \oplus d_2 \oplus \dots \oplus d_m$ (단, $\oplus$ 은 XOR 불대수 연산)으로 놓고, d_0 가 0이 되는 경우는 $d_1, d_2, \dots, d_m$ 을 식 (10)과 같은 조건으로 $d_0 \neq 0$ 이 될 때까지 반복하여 선택한다. 선택된 서로 다른 m 개의 양의 정수들에 대해 n 명의 참가자들에게 나누어 줄 수 있도록 식 (11)과 같이 n 개의 집합 형태로 묶는다.

$$DP_i = \{d_1, d_2, \dots, d_m\}, \quad i \quad (1 \leq i \leq n) \quad (11)$$

step 3 : 딜러는 $d = g^{d_0} \bmod N$ 을 연산한 후 단계 1에서 생성된 행렬 P 와 d^{-1} 에 대해 스칼라곱 연산을 수행 후 생성된 행렬 P' 은 식 (12)로 표현된다.

$$P' = \{p'_1, p'_2, \dots, p'_t\} = \{d^{-1}p_1, d^{-1}p_2, \dots, d^{-1}p_t\} \quad (12)$$

step 4 : 딜러는 $(t-1)$ 차 다항식 $f(x) = p'_1 x^0 + p'_2 x^1 + \dots + p'_t x^{t-1} \pmod{N}$ 을 생성한 후 각 참가자 P_i 에 대한 비밀키 k_i 를 이용하여 $f(k_i)$ 를 계산한다. 이 후 계산된 $f(k_i)$ 들은 모든 참가자들에게 공개한다.

step 5 : 단계 2에서 생성된 $d_1, d_2, \dots, d_m$ 들에 대해, 만약 임의의 참가자 P_i 가 공격자 구조의 임의의 집합 A_l ($1 \leq l \leq m$)에 속할 경우 딜러는 집합 A_l 에 해당하는 d_l ($1 \leq l \leq m$)을 집합 DP_i 로부터 삭제한다.

step 6 : 삽입 연산을 수행하기 위해 CI 에 삽입되는 dp_i 의 크기를 결정한다. 예를 들어, $2^0 < N \leq 2^8 - 1$ 인 경우 $|dp_i| = 8$ -bit이며, $2^8 \leq N \leq 2^{16} - 1$ 인 경우에는 $|dp_i| = 16$ bit로 결정된다. CI 내에 dp_i 를 삽입하는 과

정은 다음과 같다. 크기가 $L \times L$ 인 CI 를 $\frac{|dp_i|}{2}$ 크기의 블록으로 나누어 각각의 블록에 대해 $CB_0, CB_1, \dots, CB_{\frac{2L^2}{|dp_i|}-1}$ 과 같이 표기한다. 단, $|dp_i|$ 는 dp_i 의 크기를 의미한다. 임의의 블록 CB_o (단, $0 \leq o \leq \frac{2L^2}{|dp_i|}$)는 $\frac{|dp_i|}{2}$ 개의 픽셀로 구성되어 있고, 이는 각각 $C_p, C_{p+1}, \dots, C_{p+\left(\frac{|dp_i|}{2}\right)}$ (단, $p = \frac{|dp_i|}{2} \times o$)이다. dp_i 의 값을 2-bit씩 나누 후 이를 CB_o 내의 $\frac{|dp_i|}{2}$ 개의 픽셀들의 최하위비트 (least significant bit: LSB) 2-bit에 각각 삽입한다. 마지막으로 SI 의 다음 $t \times t$ 개의 픽셀을 추출하여 단계 1의 처음으로 되돌아가서 반복을 수행한다. 만약 SI 의 마지막 추출 픽셀 수가 $t \times t$ 보다 작을 경우 기존에 알려져 있는 패딩(padding) 기법을 이용하여 $t \times t$ 의 크기로 맞추는 다음 단계 1의 알고리즘을 수행한다. SI 의 모든 픽셀들에 대해 추출을 마친 경우 삽입 과정이 종료되고, 공유된 이미지 $SHI_{P_{(i)}}$ n 개를 모든 참가자에게 딜러(D)가 나누어 준다.

3.3 비밀이미지 복원 과정

공유된 이미지 $SHI_{P_{(i)}}$ n 개로부터 t 개를 선택하여 본래의 비밀이미지(SI)를 복원하는 과정은 비밀이미지 공유 과정의 역순으로 진행된다. 역순으로 진행하는 과정은 딜러에 의해 수행되고, 이 과정에서 참가자들에게 나누어준 t 개의 $SHI_{P_{(i)}}$ 로부터 dp_i 를 추출하고, 추출된 dp_i 를 이용하여 다항식 $f(x)$ 를 생성한 다음 임의의 참가자의 비밀키 k_i 와 공개된 다항식의 결과 값 $f(k_i)$ 의 쌍을 이용하여 본래의 다항식 $f(x)$ 을 검증한다. 검증 수행한 결과가 올바르면, 다항식 $f(x)$ 의 계수(coefficients)들과 공개된 행렬 B 를 이용하여 본래의 비밀이미지 SI 를 복원한다.

입력(input) : t 개의 $SHI_{P_{(i)}}$ (단, $1 \leq i \leq t$)

출력(output) : SI

step 1 : 크기가 $L \times L$ 인 t 개의 공유된 이미지 $SHI_{P_{(i)}}$ 들로부터 참가자의 순번 $P_{(i)}$ 가 빠른 순서대로 정렬한 다음 첫 번째 $SHI_{P_{(i)}}$ 의 첫 번째 SHB_o (단, $0 \leq o \leq \frac{2L^2}{|dp_i|}$) 블록으로부터 $\frac{|dp_i|}{2}$ 개의 픽셀들($SH_p, SH_{p+1}, \dots, SH_{p+\left(\frac{|dp_i|}{2}\right)}$)(단, $p = \frac{|dp_i|}{2} \times o$) 내에 존재하

는 LSB 2-bit를 각각 추출한 후 식 (13)과 같이 연결하여 참가자 $P_{(i)}$ 에 대한 dp_i 를 생성한다.

$$LSB2(SH_p) \parallel LSB2(SH_{p+1}) \parallel \dots \parallel LSB2(SH_{p+\frac{|dp_i|}{2}}) = dp_i \quad (13)$$

step 2 : 단계 1로부터 추출한 dp_i (단, $1 \leq i \leq t$)로부터 딜러는 t 명에 대한 집합 DP_i 들을 모두 복원하고, 복원된 t 개의 DP_i 들을 이용하여 d_0 를 계산한다. 한편, $d = g^{d_0} \bmod N$ 연산을 수행하여 d^{-1} 를 계산한 후 다항식 $f(x)$ 의 계수 값의 집합인 P'' 을 식 (14)와 같이 생성한다.

$$P'' = \{p_1'', p_2'', \dots, p_t''\} = \{d^{-1}p_1, d^{-1}p_2, \dots, d^{-1}p_t\} \quad (14)$$

step 3 : 단계 2로부터 구성된 집합 P'' 을 이용하여 본래의 다항식 $f'(x)$ 를 식 (15)와 같이 생성하고, 각 참가자의 비밀키 k_i (단, $1 \leq i \leq t$)을 이용해 $f'(k_i)$ 값의 계산하고, 기존에 공개되었던 다항식의 결과 값 $f(k_i)$ 과 일치하는지를 확인한다. 만약 일치한다면 t 명의 참가자들은 모두 올바른 인원으로 간주하고, 일치하지 않는다면 t 명 중에 공격자가 있는 것으로 간주하고, 비밀이미지의 복원 과정을 중지한다.

$$f'(x) = p_1''x^0 + p_2''x^1 + \dots + p_t''x^{t-1} \pmod{N} \quad (15)$$

step 4 : 단계 3을 통해 검증된 집합(또는 행렬) P'' 과 공개된 행렬 B 에 의해 식(16)과 같은 행렬분해 연산을 수행하고, 크기가 $t \times t$ 인 행렬 A 를 복원한다. $SHI_{P_{(i)}}$ 내의 다음 블록에 대한 동일한 연산 수행을 위해 단계 1의 처음으로 되돌아간다. 행렬 A 에서 추출된 $t \times t$ 개의 픽셀들을 통해 SI 를 복원한다.

$$A = P^{-1}B \quad (16)$$

4. 실험 및 평가 분석

본 절에서는 제안한 기법에 대한 성능과 안전성을 분석하기 위해 여러 가지 실험을 수행하고, 다른 기법들[15-17]과 삽입 용량과 이미지 왜곡을 비교한다. 삽입 용량은 공유된 이미지 내의 한 픽셀 내에 비밀 데이터가 얼마나 삽입되었는지를 나타내는 bpp(bit per pixel)나 전체 이미지 내에 삽입된 비밀데이터의 용량(단위는 bit)을 사용한다. 이미지 왜곡 정도는 커버와 공유된 이미지 간의 이미지 왜곡을 측정하는 것으로 식 (17)과 같이 PSNR를 사용한다.

$$PSNR = 10 \times \log \left(\frac{MAX^2}{MSE} \right) \quad (17)$$

단, MSE는 에러(error) 평균의 제곱(mean squared error)값으로 식 (18)과 같이 표현되고, MAX는 한 픽셀이 표현할 수 있는 최댓값을 의미하는 것으로 본 논문의 실험에서는 그레이스케일 이미지의 픽셀 값 중 최댓값인 255를 사용한다.

$$MSE = \frac{1}{4M^2} \sum_{i=0}^{4M^2-1} [C_i - SH_i]^2 \quad (18)$$

단, C_i 와 SH_i 는 본 논문에서 사용하는 커버 이미지와 공유된 이미지의 i 번째 픽셀 값을 각각 의미한다. 실험에 사용된 커버 이미지는 그림 1과 같은 8개의 그레이스케일 이미지를 사용하였고, 각 이미지의 크기는 512×512 로 고정하였다. 비밀이미지는 난수를 발생하는 C++ 라이브러리를 이용하여 비트열(bit-stream)을 생성한 후 이를 8-bit 단위로 나누어 하나의 픽셀로 사용하였다.

본 실험에서는 (2,3)-threshold과 (4,4)-threshold인 경우에 대해 실험을 수행하였다.

표 1은 삽입 용량에 대한 결과를 보여주는 것으로 8개의 테스트 이미지들에 대해 각각의 기법들마다 모두 동일한 값이 나타나는 이유는 공간영역 내에서의 LSB 삽입기법을 사용하고 있기 때문이다. Wang과 Shyu가 제안한 기법의 경우에는 가장 우수한 결

Table 1. Result of embedding capacity for eight grey scale test images (bit)

Images	Lin & Tsai[15]	Wang & Shyu[16]	Chang et al.[17]	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

과를 보여주는 'progressive' 모드와 (4,4)-threshold 일 경우에 대해 수행하였다. Lin과 Tsai의 경우에는 오류 수정을 위한 비트(parity bit)의 역할을 수행하는 것은 삽입 용량에서 제외시켰다. Chang 등이 제안한 기법은 3-bit LSB 방법을 이용하여 비밀 데이터 2-bit와 인증 데이터 1-bit씩을 각각 삽입했다. 이로 인해 다른 기법들에 비해 삽입 용량이 커졌고, 그 결과 786,432-bit를 삽입했다. 본 실험에서는 제안한 기법에 대해서 N 값을 $253 = 23 \times 11$ 로 제한하여 dp_i 의 크기를 8-bit로 고정했다. 또한, 비밀이미지의 $t \times t$ 개의 픽셀이 입력되어 하나의 dp_i 가 각 참가자마다 생성되므로 실제적으로 기존의 기법들에 비해 임계값

Fig. 1. Eight grey-scale test images. (a) airplane, (b) baboon, (c) Lena, (d) peppers, (e) boat, (f) Elaine, (g) man and (h) woman.

Table 2. Result of PSNR for eight grey scale test images (dB)

Images	Lin & Tsai[15]	Wang & Shyu[16]	Chang et al.[17]	Proposed
Lena	39.16	-	40.92	44.37
Baboon	39.15	-	40.92	43.36
Airplane	39.21	-	40.87	45.12
Peppers	39.20	-	40.96	43.36
Boat	39.18	-	40.93	43.36
Man	39.18	-	40.93	43.34
Elaine	39.13	-	40.89	43.35
Woman	39.18	-	40.93	43.37
Average	39.17	-	40.92	43.75

t 와 관계없이 N 에 따라 삽입되는 양이 결정되도록 하였다.

표 2는 PSNR의 실험 결과를 보여주고 있다. Wang과 Shyu가 제안한 기법은 공유된 이미지가 의미 없는 것으로 생성되기 때문에 실험에서 제외하였다. Lin과 Tsai가 제안한 것과 본 논문에서 제안한 기법의 삽입 용량은 동일했지만 실제 삽입되는 방식이 틀리기 때문에 PSNR 결과가 더 우수함을 알 수 있다. Chang 등이 제안한 기법은 커버 이미지의 모든 픽셀에 대해 3-bit LSB 방법을 사용했고, Lin과 Tsai가 제안한 기법은 커버 이미지의 한 블록(하나의 블록은 4개의 픽셀로 구성)당 3개의 픽셀에 대해 3-bit LSB 방법을 사용했기 때문에 일반적으로는 Lin과 Tsai가 제안한 기법의 PSNR에 대한 결과가 더 우수해야 한다. 그러나 Chang 등은 이러한 단점을 해결하기 위해 인증으로 사용되는 1-bit를 해당 픽셀 값과 유사하게 생성해 삽입하므로 Lin과 Tsai가 제안한 기법의 PSNR 결과보다 더 우수했다. 본 논문에서 제안한 기법은 공격자 구조에 대해 안전하면서도 기존의 제안된 기법들에 비해 삽입 용량과 PSNR 결과가 비슷하게 유지되거나 우위에 있음을 알 수 있었다.

5. 결 론

본 논문에서는 행렬 분해와 공격자 구조를 이용한 비밀이미지 공유 기법을 처음으로 제안하였다. 기존의 비밀이미지 공유 기법들의 결점이었던 선형결합 다항식 연산과 공격자가 임계값 t 이상의 참가자들에 대한 비밀 조각들의 정보를 습득할 수 있는

Tompa-Woll 공격에 강인한 알고리즘으로 행렬 분해와 지수연산을 이용해 비밀이미지의 조각이 아닌 새로운 변수를 이용하여 참가자들에게 분배하였다. 또한, 비밀이미지 공유 과정에서 공격자 구조를 이용하여 사전에 임계값 t 이상의 참가자들에 대한 비밀 조각들의 정보를 공격자가 습득할 수 없도록 하였다. 공유된 이미지는 2-bit LSB 방법을 이용하여 기존의 기법들과 비교하여 삽입 용량은 그대로 유지하는 한편 PSNR 결과는 상대적으로 우수함을 실험을 통하여 증명하였다.

향후 연구는 제안한 기법이 가역이 가능하도록 하는 것이다. 가역이 가능하기 위해선 비밀 공유 시 사용하는 다항식의 형태를 변경하는 것이 중요하나 제안한 기법은 기존의 기법들과 다른 방식으로 다항식을 사용하기 때문에 이에 대한 선행 연구가 필요할 것으로 사료된다. 또한, 2-bit LSB 방법이 아닌 PSNR 결과가 우수하면서 삽입 용량이 증가하는 연구도 수행되어야 할 것이다.

REFERENCE

- [1] W. Zhu, C. Luo, J. Wang, and S. Li, "Multimedia Cloud Computing," *IEEE Signal Processing Magazine*, Vol. 28, Issue 3, pp. 59-69, 2011.
- [2] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security and Privacy*, Vol. 9, Issue 2, pp. 50-57, 2011.
- [3] M. Lori, "Data Security in the World of Cloud Computing," *IEEE Computer and Reliability Societies*, Vol. 7, Issue 4, pp. 61-64, 2009.
- [4] A. Shamir, "How to Share a Secret," *Communication of the ACM*, Vol. 22, Issue 11, pp. 612-613, 1979.
- [5] G.R. Blakley, "Safeguarding Cryptographic Keys," *Proceedings of International Workshop on the National Computer Conference of IEEE Computer Society*, pp. 313-317, 1979.
- [6] M. Naor and A. Shamir, "Visual Cryptography," *Advances in Cryptology-EUROCRYPT94, Lecture Notes in Computer Science* 950, pp. 1-12, 1995.

- [7] M. Naor and A. Shamir, "Visual Cryptography II: Improving the Contrast Via the Cover Base," *Proceedings of International Workshop Cambridge, Security Protocols, Lecture Notes in Computer Science 1189*, pp. 197-202, 1997.
- [8] C.C. Thien and J.C. Lin, "Secret Image Sharing," *Journal of Computers and Graphics*, Vol. 26, Issue 5, pp. 765-770, 2002.
- [9] K.J. Kim, S.H. Shin, and K.Y. Yoo, "A New Information Data hiding Scheme based on Pattern Information of Secret Data," *Journal of Korea Multimedia Society*, Vol. 15, Issue 4, pp. 526-539, 2012.
- [10] B.J. Jang, S.H. Lee, and K.R. Kwon, "Active Video Watermarking Technique for Infectious Information Hiding System," *Journal of Korea Multimedia Society*, Vol. 15, Issue 8, pp. 1017-1030, 2012.
- [11] S.I. Hyun, S.H. Shin, and K.Y. Yoo, "A Proactive Secret Image Sharing Scheme over GF(2⁸)," *Journal of Korea Multimedia Society*, Vol. 16, Issue 5, pp. 577-590, 2013.
- [12] P.Y. Lin and C.S. Chan, "Invertible Secret Image Sharing with Steganography," *Journal of Pattern Recognition Letters*, Vol. 31, No. 13, pp. 1887-1893, 2010.
- [13] A. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996, N.W., Boca Raton, FL 33431, USA.
- [14] D.R. Stinson, *Cryptography: theory and practice*, CRC Press, 2005, Upper Saddle River, NJ 07458, USA.
- [15] C.C. Lin and W.H. Tsai, "Secret Image Sharing with Steganography and Authentication," *Journal of Systems and Software*, Vol. 73, Issue 3, pp. 405-414, 2004.
- [16] R.Z. Wang and S.J. Shyu, "Scalable Secret

Image Sharing," *Journal of Signal Processing: Image Communication*, Vol. 22, Issue 4, pp. 363-373, 2007.

- [17] C.C. Chang, Y.P. Hsieh, and C.H. Lin, "Sharing Secrets in Stego Images with Authentication," *Journal of Pattern Recognition*, Vol. 41, Issue 10, pp. 3130-3137, 2008.

현 승 일

1990년 2월 계명대학교 전자계산
학과 공학사
1999년 2월 성균관대학교 전기전
자컴퓨터공학과 공학석사
2013년 2월 현재 경북대학교 컴퓨
터공학과 공학박사 수료

1999년 9월~2002년 2월 영진전문대학 전자정보계열 교수
2002년 2월~현재 영진사이버대학 정보통신공학계열 교수
관심분야: 멀티미디어시스템, 암호학, 분산시스템

신 상 호

2006년 8월 금오공과대학교 응용
수학/컴퓨터공학 학사
2008년 8월 경북대학교 전자전기
컴퓨터학부 공학석사
2009년 3월~현재 경북대학교 전
자전기컴퓨터학부 박사
과정

관심분야: 양자 셀룰라 오토마타, 양자암호, 양자비밀공유

유 기 영

1976년 2월 경북대학교 수학교육
과 이학사
1978년 2월 한국과학기술원 전산
학과 공학석사
1992년 5월 미국 Rensselaer
Polytechnic Institute
전산학과 공학박사

1978년 3월~현재 경북대학교 IT대학 컴퓨터학부 교수
관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크
보안, 데이터베이스보안, 스테가노그래피, 인
증프로토콜