Journal of Korea Multimedia Society Vol. 20, No. 2, February 2017(pp. 261-270)
https://doi.org/10.9717/kmms.2017.20.2.261

비밀 공유 기반의 7×7 스도쿠를 사용한 가역 정보 은닉 기법

김영주[†], 김평한[††], 유기영[†††]

A Reversible Data Hiding Scheme Using 7×7 Sudoku Based on Secret Sharing

Young-Ju Kim[†], Pyung-Han Kim[††], Kee-Young Yoo[†††]

ABSTRACT

Data hiding is a way to hide the information in multimedia media such as images or video. The scheme proposed by Nguyen and Chang, was able to embed, extract, and restore the cover image and the secret data using Sudoku. But in the extracting phase, the occurrence of duplicate values in the reference matrix was found to decrease the embedding capacity of secret data. This paper has proposed a reversible data hiding scheme while maintaining the quality of the image to provide high embedding capacity using 7×7 Sudoku and Shamir's secret sharing scheme.

Key words: Reversible Data Hiding, Secret Sharing, Sudoku, Embedding Capacity

1. 서 론

최근 인터넷의 급속한 발전과 함께 디지털 콘텐츠의 사용이 늘면서 정보보호의 중요성이 강조되고 있다. 디지털 콘텐츠는 주로 인터넷을 이용하여 교환이 이루어진다. 따라서 개인이나 단체의 지적 재산권과 저작권을 침해하는 문제들이 빈번하게 발생하고 있다. 악의적인 목적을 가진 제3자로부터 정보가 불법적으로 악용되는 것을 방지하고 정보의 위변조를 막기 위해서 암호화 기법과 정보 은닉 기법(information hiding scheme)들이 사용되고 있다.

암호화는 제 3자에게 정보가 누설되거나 조작되는 것을 방지하기 위하여 정보를 암호화하여 정보의 내용을 알지 못하게 전송하는 기법이다[1-3]. 정보 은닉은 이미지나 비디오 영상 같은 멀티미디어 매체 안에 정보를 숨기는 기법이다. 정보 은닉에서 가장 중요한 것은 비밀 정보가 탐지되지 않고 보존되도록 하는 것이다. 디지털 이미지에 비밀 정보를 숨기게 되면 원본 이미지의 픽셀을 변경하기 때문에 스테고 이미지(stego image)에 왜곡이 발생하게 된다. 왜곡을 최소화하기 위해 많은 방법이 제안되었지만 인간의 시각으로 감지할 수 없는 왜곡은 여전히 존재한다. 이러한 왜곡은 의료 영상이나 군용 영상 등의 분야에서 민감하게 작용한다. 특히 의료 영상에 대한

※ Corresponding Author : Kee-Young Yoo, Address: (702-701) Information Security Lab(Office: E9-508). School of Computer Science & Engineering, Kyungpook National University, 1370 Sankyuk-dong, Buk-gu, Daegu, South Korea, TEL : +82-53-950-5553, E-mail : yook@knu.ac.kr
Receipt date : Jan. 16, 2017, Approval date : Jan. 19, 2017
[†] Dept. of Computer Science & Engineering, Graduate School, Kyungpook National University
(E-mail : kyj@knu.ac.kr)
[††] Dept. of Computer Science & Engineering, Graduate School, Kyungpook National University
(E-mail : k2jbks90@gmail.com)
[†††] School of Computer Science & Engineering, Kyungpook National University
※ This research was supported by Kyungpook National University Bokhyeon Research Fund, 2015.

왜곡은 의료 사고로 이어질 수 있다. 그렇기 때문에 삽입된 비밀 정보를 추출하는 과정에서 원본 영상도 완벽하게 복원할 수 있는 가역 정보 은닉 기법에 대한 연구가 활발히 진행되고 있다[4-10].

최근 연구되는 가역 정보 은닉 기법(reversible data hiding scheme)들은 차이 확장(difference expansion, DE)[4, 5]과 히스토그램 이동(histogram shifting)[6, 7]을 기반으로 하고 있다. 2003년 Tian은 임계치에 따라서 삽입 용량과 스테고 이미지의 왜곡을 조절할 수 있는 DE 기법을 제안하였다[4]. DE 기법은 원본 이미지의 모든 픽셀을 이웃하고, 서로 중복되지 않는 픽셀 쌍으로 구분하였다. 그리고 비밀 정보는 각 픽셀 쌍의 차이를 확장하여 삽입하였다. 2006년 Ni 등은 히스토그램을 이용한 가역 정보 은닉 기법을 제안하였다[6]. 이미지 히스토그램에서는 픽셀 값과 픽셀 값의 빈도를 각각 가로축과 세로축에 나타낸다. 히스토그램 이동은 이미지 히스토그램에서 빈도가 가장 높게 나타나는 픽셀을 이동시켜서 비밀 정보를 삽입하는 기법이다. 또한 최근에는 군사 이미지 영상의 특성에 기반 하여 비밀 정보를 삽입하는 기법이 Lee 등에 의해서 제안되었다. 비밀 정보를 삽입 및 추출하기 위해서 군사 이미지 영상내의 중요도에 따라 이미지의 영역을 구분하고, 구분된 영역에 두 가지 정보은닉 기법을 적용한다[9]. 2015년 Nguyen과 Chang은 스도쿠를 이용하여 보안성을 향상 시키고, 정보 삽입량을 늘리면서도 좋은 이미지 품질을 유지시킬 수 있는 기법을 제안하였다[10].

한편 최근에는 비밀 정보에 접근 할 수 있는 비밀키(secret key)를 여러 명이 공유하여 기존의 단일 비밀 키의 문제점을 해결할 수 있는 비밀 공유 기법(secret share scheme)에 대한 연구도 활발하게 진행되고 있다. 최초의 비밀 공유 기법은 1979년 Shamir [11]와 Blakley[12]에 의해 각각 소개되었고, n명의 참가자 중 적어도 t명 이상이 모이면 비밀을 확인할 수 있는 (t, n)-threshold 개념을 사용하였다. Shamir의 비밀 공유 기법을 통해 다양한 분야에서 활용 가능한 방법들이 제안되고 있다.

본 논문에서는 스도쿠(Sudoku)와 비밀 공유 기법을 사용하여 좋은 이미지 품질을 유지하면서 높은 삽입 용량을 제공하는 가역 정보 은닉 기법을 제안한다. 7×7 스도쿠 테이블을 이용해 0부터 6사이의 값을 담고 있는 참조 행렬을 생성하고, 모듈러 연산을 통해 원본 이미지의 픽셀 변화를 최소화 하였다. 비밀 정보 삽입 과정에서는 Shamir의 (2, 2)-threshold 비밀 공유 기법을 사용하여 다항식의 상수와 계수 안에 비밀 정보 및 원본 이미지 복원을 위한 정보를 넣었다. 추출 과정에서는 Lagrange 보간법을 이용하여 본래의 다항식 복원을 통해 비밀 정보를 추출하고, 원본 이미지를 복원해낼 수 있도록 하였다.

본 논문은 다음과 같이 구성되어있다. 2장에서는 본 논문의 관련 연구인 스도쿠 기술에 기반한 가역 정보 은닉 기법과 Shamir의 (t, n)-threshold 비밀 공유 기법에 대해 살펴본다. 3장에서는 스도쿠와 비밀 공유 기법을 이용한 가역 정보 은닉 기법에 대해 설명하고, 4장에서는 실험 결과 및 분석을 통하여 제안한 기법의 우수성을 증명한다. 마지막으로 5장에서는 결론과 함께 향후 연구 방향을 제시한다.

2. 관련연구

2.1 정보 은닉

정보 은닉 기법에는 크게 스테가노그래피와 디지털 워터마킹이 있다. 스테가노그래피는 비밀 정보의 존재 유무 자체를 숨기는 기법이다. 이 기법은 비밀 정보를 이미지, 음악, 동영상 등의 디지털 콘텐츠 안에 삽입하여 인간의 시각으로 감지할 수 없도록 한다. 영상을 이용한 스테가노그래피는 비밀 정보를 숨기기 위한 대상으로 디지털 이미지를 사용한다. 송신자는 원본 이미지에 비가시적으로 비밀 정보를 삽입하고, 수신자에게 전달한다. 이것을 받은 수신자는 스테고이미지에서 비밀 정보를 추출하여 그 내용을 확인할 수 있다.

스테가노그래피는 또 다시 공간 영역(spatial domain)을 이용한 기법과 주파수 영역(frequency domain)을 이용한 기법으로 나뉜다. 공간 영역을 이용한 기법들로는 LSB[10, 11], PVD[12, 13], 히스토그램 이동[5, 6] 등이 있다. 그리고 주파수 영역을 이용한 기법들로는 DCT[14, 15], DWT[16, 17] 등이 있다. 최근에는 두 영역을 결합한 기법들도 연구되고 있다. 워터마킹은 제3자가 알 수 없는 형태로 저작권자의 정보를 디지털 콘텐츠 안에 기록하는 기법이다. 워터마킹 기법에서는 악의적인 공격자가 워터마크가 삽입된 디지털 콘텐츠를 고의적으로 수정하면 원본 콘텐츠 를 사용할 수 없도록 한다.

2.2 Shamir의 비밀 공유

1979년 Shamir는 (t, n)-threshold 개념과 Lagrange 보간법을 이용한 비밀 공유 기법을 처음 제안하였다. 또, 같은 해에 Blakley는 선형 사영기하학(linear projective geometry)기법을 이용하여 비밀 공유 기법을 소개하였다. Shamir와 Blakley가 제안한 기법들은 복원 과정이 서로 다르다. 하지만 비슷한 시기에 소개되었기 때문에 Shamir와 Blakley의 비밀 공유 기법으로 통용된다. 주로 Shamir가 제안한 기법이 암호학의 많은 분야에 응용되어 사용되었다. 그래서 대부분의 비밀 공유 기법은 Shamir가 제안한 기법을 기반으로 한다. 비밀 공유 기법은 분배 과정, 복원 과정으로 구성된다. 하나의 비밀로부터 share를 생성, 분배, 그리고 복원하는 역할은 딜러(dealer)가 수행한다. 딜러는 합법적으로 인증된 자로 가정한다.

2.2.1 분배 과정

분배 과정에서는 아래와 같은 다항식 (1)이 사용된다.

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

식 (1)에서 m은 비밀 메시지의 값이며, 계수($a_1 \sim a_{t-1}$)들은 0부터 ($p-1$)사이 임의의 계수가 들어간다. 그리고 p는 비밀 메시지인 m 보다 큰 소수이다.

2.2.2 복원 과정

복원 과정에서는 n명의 참가자 중 t명 이상의 인원으로부터 값 (a_i, $f(a_i)$), $t \geq n$을 알고 있을 때, 아래 식 (2)의 Lagrange 보간법을 이용하여 비밀 메시지 m과 다항식을 복원한다.

$$f(x) = \sum_{i=1}^{t} y_i \prod_{1 \leq i < t} \frac{x - x_j}{x_i - x_j} \pmod{p} \quad (2)$$

2.3 Nguyen과 Chang의 기법

2015년 Nguyen과 Chang은 스도쿠 기술을 이용한 가역 정보 은닉 기법을 제안하였다[9]. 스도쿠는 1979년 Number place라는 이름으로 알려졌다. 9×9 스도쿠는 아래와 같은 규칙을 갖고 있다.

1. 9×9 스도쿠는 9개의 3×3 서브 블록들로 구성되며, 각 블록에는 중복되지 않은 1부터 9사이의 숫자가 들어간다.
2. 9×9 스도쿠의 모든 행과 열의 값은 중복되지 않은 1부터 9 사이의 숫자이다.

Nguyen과 Chang의 기법은 많은 경우의 수를 지닌 스도쿠를 사용하여 보안성을 향상시켰다.

2.3.1 Nguyen과 Chang 기법의 초기화 과정

초기화 과정에서는 Fig. 1과 같이 스도쿠 솔루션을 이용해 Sub-matrix S를 생성한다.

Sub-matrix S를 Fig. 2와 같이 여러 개를 이어 붙여서 Reference matrix RM을 생성한다.

2.3.2 Nguyen과 Chang 기법의 삽입 과정

원본 이미지 I를 두 개의 영역으로 나눈다. 4개 행을 삽입할 수 없는 영역으로 할당하고, 각 픽셀의 LSB를 위치지도 LM으로 사용한다. 그리고 비밀 정보 S를 9진수의 숫자 D로 변환한다. 그런 다음 원본 이미지로부터 두 개의 연속되는 픽셀 쌍을 가져온다. 그리고 VE와 HE 영역을 구한다. 만약 $I_{2i} < 7$ 이거나

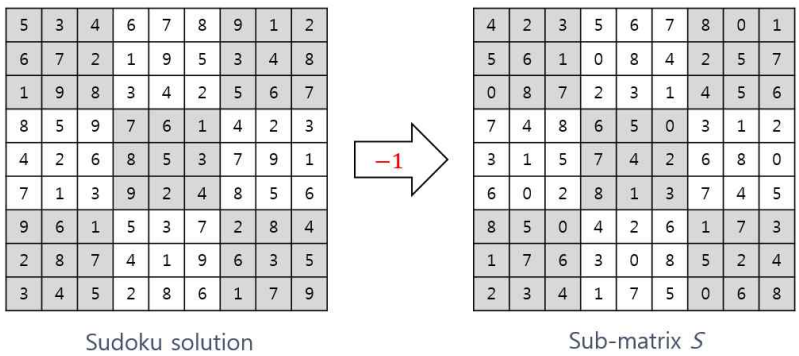

Fig. 1. Sub-matrix S creation process.

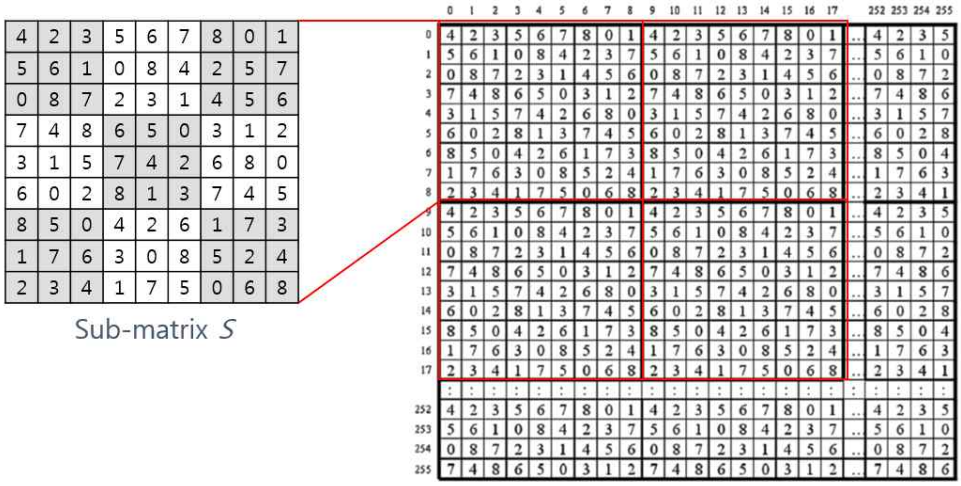

Fig. 2. Reference matrix RM creation process.

I_{2i+1} >248 이면, LM을 1로 바꾸고 정보를 삽입하지 않는다. 비밀 정보 삽입을 위하여 RM에서 $(X_{VE}, Y_{VE}) = (X_{HE}, Y_{HE}) = D$를 만족하는 좌표 쌍을 구한다. 그런 다음 $X = \frac{X_{VE} + X_{HE}}{2}$, $Y = \frac{Y_{VE} + Y_{HE}}{2}$ 값을 구한다. 만약 X 또는 Y 값이 소수일 경우 LM을 1로 바꾸고 정보를 삽입하지 않는다. 여기서 X 또는 Y의 값이 소수 인 경우가 많아서 정보 삽입 량이 줄어든다. X 또는 Y 값이 소수가 아닐 경우 원본 픽셀 쌍을 X, Y 값으로 변경하고, 모든 비밀 정보가 삽입이 완료될 때까지 앞의 과정을 반복한다.

2.3.3 Nguyen과 Chang 기법의 추출 과정

추출 과정에는 U와 L 영역이 복원에 이용된다. 스테고 이미지의 픽셀 쌍 (I_{2i}', I_{2i+1}')을 통해 RM에서 U와 L영역을 구할 수 있다. U와 L 영역에서 서로 대칭을 이루는 좌표의 값이 삽입된 비밀 정보이다. 그리고 대칭을 이루는 두 좌표를 이용해 VE와 HE 영역을 구한다. 교차하는 지점의 좌표가 원본 픽셀 쌍이다. 그러나 추출 과정에서 참조 행렬 내 중복 값이 발생하여 비밀 정보 삽입 량이 현저하게 줄어든다.

2.3.4 Nguyen과 Chang 기법의 문제점

Nguyen과 Chang은 기존에 Chang 등이 제안한 스도쿠를 사용한 정보 은닉 기법을 응용하여 비밀 정보의 추출 후, 원본 이미지 또한 복원시킬 수 있는 가역 정보 은닉 기법을 제안하였다. 그러나 비밀 정보 삽입 과정에서 두 개 픽셀 값의 평균값을 계산하는 단계를 거치면서, 평균값이 정수가 아닐 경우 비밀 정보의 삽입량이 감소할 수밖에 없었다. 또한 비밀 정보 추출 과정에서도 참조 행렬 내 중복 값이 발생하는 경우 비밀 정보의 삽입 량이 현저하게 감소된다.

3. 비밀 공유 기반의 7×7 스도쿠를 사용한 가역 정보 은닉 기법

3.1 제안한 기법의 개요

본 논문에서는 Shamir의 비밀 공유 기법과 스도쿠를 이용하는 가역 정보 은닉 기법을 제안한다. 초기화 과정에서는 비밀 정보를 7진수의 숫자로 변환한 뒤, 7×7 스도쿠를 이용하여 참조 행렬(Reference matrix)을 생성한다. 제안하는 기법에서 이용하는 7×7 스도쿠는 7개의 서브 블록으로 이루어져 있고, 각각의 서브 블록에는 1부터 7사이의 중복되지 않은 숫자가 들어간다. 7×7 스도쿠는 수많은 경우의 수를 발생할 수 있기 때문에 정보 은닉 기법에서 보안성 향상을 위해서 이용한다. 비밀 정보의 삽입 과정에서는 참조 행렬에서 비밀 정보 삽입에 사용될 하나의 행을 선택하고 비밀 공유 기법에 적용할 상수 값을 구한다. 각각의 행을 선택하는 경우에는 랜덤 함수에 *seed* 값을 주고, 추후 동일한 *seed* 값을 이용해 비밀 정보를 생성한다. 원본 이미지에서는 두 개의 픽셀 단위로 모듈러 연산을 수행하여 비밀 공유 기법과

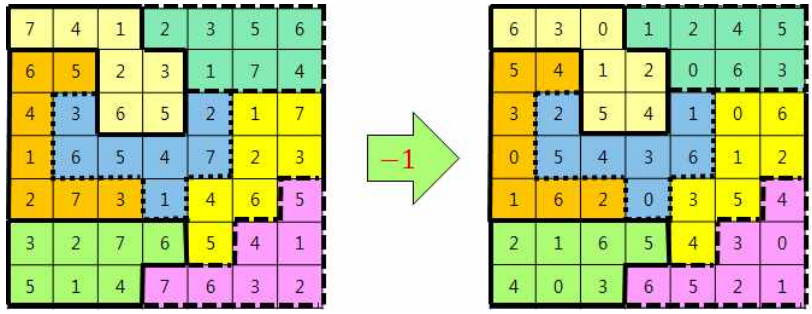

Fig. 3. Reference matrix *RM* generation. (a) 7×7 Sudoku, (b) Reference matrix *RM*.

원본 이미지의 복원에 이용될 두 개의 값을 구한다. 비밀 공유 기법의 다항식을 이용하여 비밀 정보를 삽입하고 공유 값을 생성하여서 참가자들에게 분배한다. 추출 과정에서는 스테고 이미지를 통해 공유 값을 복원하고, Lagrange 보간법을 이용하여 비밀 정보 복원에 이용할 값과 원본 이미지 복원에 사용되는 값을 구한다. 이 두 개의 값들과 모듈러 연산을 이용하여서 비밀 정보를 추출하고 원본 커버 이미지를 복원 할 수 있다.

3.2 초기화 과정

제안하는 기법은 7×7 스도쿠를 사용하기 때문에 비밀 정보의 삽입을 위해서 10진수 형태의 비밀 정보를 7진수 형태로 변환한다. 7진수는 0부터 6까지의 범위를 가지기 때문에 참조 행렬 *RM*을 생성하기 위해서는 Fig. 3과 같이 7×7 스도쿠의 모든 값들에서 1을 뺀다.

3.3 삽입 과정

삽입 과정에서는 비밀 정보의 삽입을 위해 참조 행렬 *RM*에서 하나의 행인 *HE*(horizontal elements)를 선택한다. *HE*를 선택하기 위해서는 랜덤 함수를 이용하고 삽입 과정과 추출 과정에서 이용되는 랜덤 함수는 동일한 *seed* 값을 사용한다. 비밀 공유 기법의 다항식에 이용할 두 개의 계수 CF_1과 CF_2를 계산하기 위해 원본 이미지 *CI*(cover image)로부터 한 쌍의 픽셀이 사용된다. 이 두 개의 값들은 *CI*의 복원에 사용되는데, CF_1은 이미지의 픽셀 값 안에 삽입되고, CF_2는 하나의 키로써 부가 정보(extra information)로 저장된다. 선택된 *HE*의 값들 중에서 숨길 비밀 정보와 일치하는 열(column)의 번호는 상수 값인 *CS*(Constant) 값으로 사용된다. 최종적으로 Shamir의 비밀 공유 기법을 기반으로 밀 정보의 삽입이 이루어진다. 삽입 알고리즘은 아래와 같다.

Input : 커버 이미지 *CI*, 참조 행렬 *RM*

Output : 스테고 이미지 *SI*, 로케이션 맵(Location Map)

Step 1: 랜덤 함수에 *seed* 값을 적용하여 참조 행렬 *RM*에서 비밀 정보 삽입에 이용될 *HE* 행을 선택한다. 아래 Fig. 4는 랜덤 함수를 통해 4번 행이 선택된 모습을 나타내고 있으며, 선택된 *HE* 행에서 숨길 비밀 정보와 일치하는 열 번호를 상수 *CS*라 한다.

Step 2: 원본 이미지 *CI*의 I_{2k}와 I_{2k+1} 위치의 두 개의 픽셀 값들에 대하여 모듈러 연산을 수행하여 두 개의 계수 값들인 CF_1과 CF_2를 계산하고, CF_2 값은 로케이션 맵에 저장한다. 단, 오버플로우(Overflow) 방지를 위해서 I_{2k} >246 인 경우에는 비밀 정보

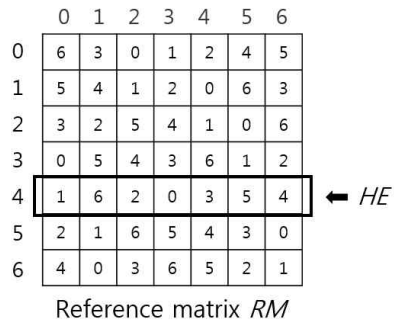

Fig. 4. *HE* selection.

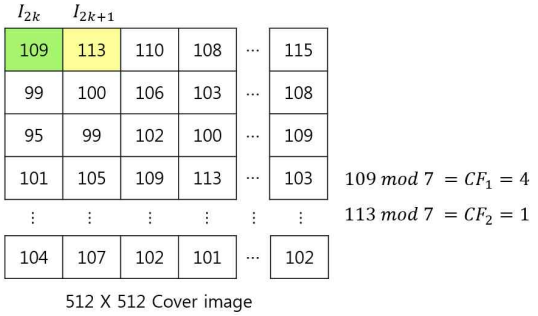

Fig. 5. CF_1 and CF_2 calculation.

를 숨기지 않는다.

$$CI(I_{2k}) \bmod 7 = CF_1 \quad (3)$$

$$CI(I_{2k+1}) \bmod 7 = CF_2 \quad (4)$$

아래의 Fig. 5는 원본 이미지 CI로부터 두 개의 픽셀 값을 가져와서 계수 값들인 CF_1과 CF_2를 계산하는 과정을 그림으로 나타내고 있다.

Step 3: Shamir의 비밀 공유 기법을 이용하여 수식 (5)와 같은 다항식을 생성한다. 그리고 2개의 공유 값들인 $(a, f(a))$, $(b, f(b))$를 생성한다.

$$f(x) = CS + CF_1 x \pmod 7 \quad (5)$$

Step 4: 원본이미지 CI의 두 개의 픽셀들에 대하여 모듈러 연산을 수행하여 나온 각각의 결과 값들에 대하여 수식 (6)과 수식 (7)을 이용하여 동일한 위치의 픽셀에 대하여 차를 구한다.

$$I_{2k} = I_{2k} - (I_{2k} \bmod 7) \quad (6)$$

$$I_{2k+1} = I_{2k+1} - (I_{2k+1} \bmod 7) \quad (7)$$

이 과정은 Fig. 6에 도식화 하였다.

Step 5: Step 4에서 계산 되어진 픽셀 값들에 대하

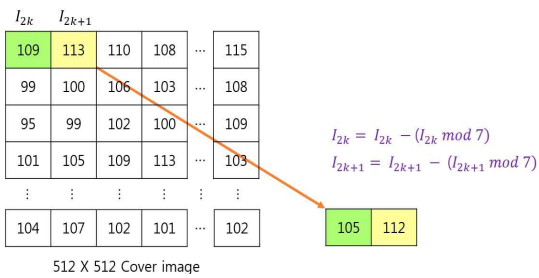

Fig. 6. Modular arithmetic process of the embedding.

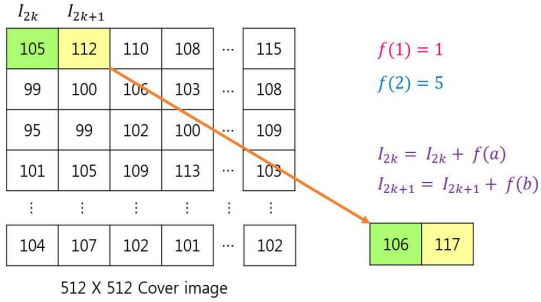

Fig. 7. Share summing process of the embedding.

여서 수식 (8)과 수식 (9)를 이용하여 $f(a)$와 $f(b)$ 값들을 각각 더해준다.

$$I_{2k} = I_{2k} + f(a) \quad (8)$$

$$I_{2k} = I_{2k+1} + f(b) \quad (9)$$

이 과정은 Fig. 7에 도식화 하였다.

Step 6: Step 1부터 5까지의 과정을 모든 비밀 정보의 삽입이 완료될 때까지 반복한다.

3.4 추출 과정

추출 과정은 삽입 과정과 유사한 방식으로 진행된다. 비밀 정보가 삽입되어있는 스테고 이미지 SI에서 비밀 정보를 추출하기 위하여 삽입 과정에서 사용된 공유 값의 키 값 (a, b)에 대한 정보를가 요구된다. 추출 알고리즘은 아래와 같다.

Input : 스테고 이미지 SI, 로케이션 맵(Location Map)
Output : 커버 이미지 CI, 참조 행렬 RM

Step 1: 비밀 정보가 삽입된 스테고 이미지 SI에서 픽셀 쌍 $SI(I_{2k}^{'}, I_{2k+1}^{'})$을 선택한다.

Step 2: Step1에서 선택되어진 두 개의 픽셀 값들에 대하여 모듈러 연산을 수행하고, 이 값들을 이용하여 2개의 공유 값들을 복원한다. 단, $SI(I_{2k}^{'}) > 255$인 경우에는 비밀 정보가 삽입 되어 있지 않기 때문에, 복원 과정을 수행하지 않는다. 비밀 정보의 추출 과정은 Fig. 8과 같다.

Step 3: Lagrange 보간법을 이용해 다항식을 복원

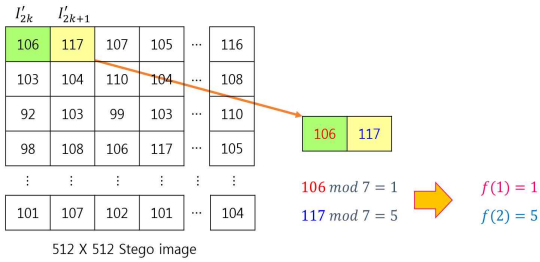

Fig. 8. Extracting process.

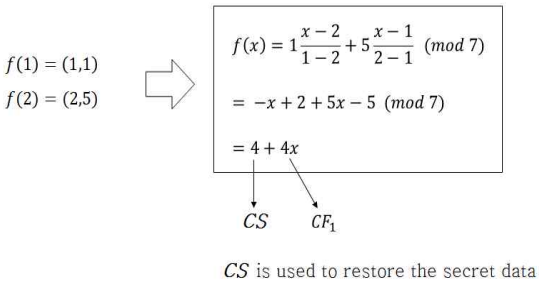

Fig. 9. Polynomial restoration process.

하고, 상수 값인 CS와 계수 값인 CF_1 값을 계산한다. Fig. 9는 Lagrange 보간법을 이용하여 CS와 CF_1 값을 복원하는 예시를 보여준다. 여기서, CS는 삽입 과정에서 사용된 HE의 열 번호이며, CF_1은 원본 커버 이미지 복원에 이용된다.

Step 4: 스테고 이미지 SI의 두 개의 픽셀들에 대하여 모듈러 연산을 수행하여 나온 각각의 결과 값들에 대하여 수식 (10)과 수식 (11)을 이용하여 동일한 위치의 픽셀에 대하여 차를 구한다.

$$I'_{2k} = I'_{2k} - (I'_{2k} \bmod 7) \tag{10}$$

$$I'_{2k+1} = I'_{2k+1} - (I'_{2k+1} \bmod 7) \tag{11}$$

Step 5: Step4에서 계산 되어진 픽셀 값들에 대하여서 수식 (12)과 수식 (13)을 이용하여 CF_1와 CF_2 값들을 각각 더해준다.

$$I'_{2k} = I'_{2k} + CF_1 \tag{12}$$

$$I'_{2k+1} = I'_{2k+1} + CF_2 \tag{13}$$

Step 6: Step 1부터 5까지의 과정을 모든 비밀 정보의 추출이 완료될 때까지 반복한다.

4. 실험 결과 및 고찰

제 4장에서는 Nguyen과 Chang이 제안한 기법과 본 논문에서 제안한 기법의 실험 결과를 비교하였다. 다양한 이미지에 대한 실험 결과의 분석을 통해 제안한 기법이 기존에 방법보다 아주 많은 정보를 삽입함을 보여 준다.

4.1 실험 환경

일반적으로 정보 삽입 량과 이미지 품질은 제안된 정보 은닉 기법의 알고리즘 성능을 평가하는데 사용된다. 정보 삽입 량은 원본 이미지에 숨길 수 있는 비밀 메시지의 총량을 나타낸다. 이미지 왜곡의 정도는 $PSNR$(Peak Signal to Noise Ratio)을 사용하여 측정된다. $PSNR$은 이미지 처리를 통해 원본 이미지의 왜곡을 검출하는 방법으로서 이용된다. $PSNR$ 값이 $30dB$ 이상이면 인간의 시각 시스템으로는 이미지의 왜곡을 감지하는 것이 어렵다. 원본 이미지의 너비와 높이를 w와 h로 정의하였을 때 $PSNR$은 식 (5)로 계산되어진다.

$$PSNR = (10 \cdot \log_{10}(\frac{MAX^2}{MSE})) \tag{5}$$

Fig. 10. Nine 512×512 size gray-scale image. (a) Lena (b) F16 (c) Baboon (d) Peppers (e) Zelda (f) Barbara (g) Elaine (h) Boat (i) Airport.

MSE(Mean Square Error)은 식 (6)으로부터 얻어진다.

$$MSE = (\sum_{i=1}^{w \times h} \frac{(p - p'_i)^2}{w \times h}) \quad (6)$$

Fig. 10은 실험에 사용된 그레이 스케일 이미지를 보여준다. 비밀 메시지는 랜덤 함수를 사용하여 생성되어진다.

4.2 Nguyen과 Chang 기법의 실험 결과

Table 1은 Nguyen과 Chang 기법의 원래 실험 결과와 실제 실험 결과를 비교한다. 기존에 제안된 Nguyen과 Chang의 기법은 정보 추출 및 원본 이미지의 복원 과정에서 참조 행렬 내 중복 값이 발생하여 정보 삽입 량이 현저하게 줄어드는 문제점이 발견되었다. Nguyen과 Chang이 제안한 논문에서는 정보 삽입 량이 평균 120,018 bits로 표기되어 있지만, 실제 실험 결과, 정보 삽입 량은 평균 22,986 bits에 불과하였다.

4.3 제안한 기법의 실험 결과

Nguyen과 Chang의 기법은 실제 실험 결과 정보 삽입 량이 평균 22,986 bits에 불과하였다. 그러나 새롭게 제안한 기법은 7×7 스도쿠를 사용하여 평균 39.10dB의 $PSNR$을 보인다. Nguyen과 Chang이 제안한 기법에 비하여 $PSNR$이 조금 떨어지기는 하지만 30dB 이상의 $PSNR$을 보일 경우, 인간의 시각으로 이미지의 왜곡을 인지하기란 어렵다. 또한 두 픽셀 당 하나의 비밀 정보를 숨기기 때문에 오버플로우(Overflow)가 발생하는 경우를 제외하면 이미지에 관계없이 367,965 bits의 정보 삽입 량을 보인다. 기존 기법에 비하여 정보 삽입 량이 15배 이상 향상된 것이다.

Table 1. Original embedding capacity(bits) and actual embedding capacity of Nguyen and Chang's Scheme

Images	Nguyen and Chang's Original experimental results	Nguyen and Chang's Actual experimental results
Lena	119,633	22,652
F16	118,665	24,148
Baboon	117,228	23,295
Peppers	119,457	22,991
Zelda	120,567	21,311
Barbara	122,292	24,322
Elaine	121,513	22,909
Boat	120,857	22,651
Airport	119,952	22,595
Average	120,018	22,986

Table 2. *PSNR* and embedding capacity(bits) of the proposed scheme and previous scheme

Images	Nguyen and Chang's Scheme		Proposed Scheme	
	PSNR	Capacity	PSNR	Capacity
Lena	55.32	22,652	39.04	367,965
F16	54.95	24,148	39.27	367,965
Baboon	55.61	23,295	39.14	367,965
Peppers	55.28	22,991	39.11	367,965
Zelda	55.93	21,311	39.05	367,965
Barbara	55.44	24,322	39.14	367,965
Elaine	55.44	22,909	38.86	367,965
Boat	55.63	22,651	39.25	367,965
Airport	55.68	22,595	39.04	367,965
Average	55.47	22,986	39.10	367,965

5. 결 론

Nguyen과 Chang이 제안한 기법에서는 스도쿠 기술을 이용하여 비밀 정보를 삽입, 추출하고 원본 이미지도 복원해낼 수 있었다. 그러나 추출 과정에서 참조 행렬 내 중복 값이 발생하여 비밀 정보 삽입량이 현저하게 줄어드는 문제점이 발견되었다.

본 논문에서는 7×7 스도쿠와 Shamir가 제안한 비밀 공유 기법을 사용하여 비밀 정보 삽입 량을 늘리면서도 높은 이미지 품질을 유지하고, 원본 이미지 또한 완벽하게 복원할 수 있는 가역 정보 은닉 기법을 제안하였다. 수많은 경우의 수를 가진 스도쿠를 키(key)로 사용하여 보안성을 향상시킬 수 있었다. 중복된 값이 들어가지 않는 스도쿠의 특징을 이용하여 비밀 정보를 선택하고, 비밀 공유 기법을 이용하여 비밀 정보를 삽입한다. 모듈러 연산을 통해 픽셀의 왜곡을 최소화 하였다. 실험 결과에서 알 수 있듯이, 평균적인 $PSNR$이 39.10dB로 인간의 시각으로는 이미지의 왜곡을 인지하기란 거의 불가능하다. 평균 삽입 용량은 367,965 bits로, 이전 기법에 비해 15배 이상 삽입 량이 향상되었다. 하지만 비밀 정보의 삽입 및 추출과정을 마친 후, 검증을 위하여 원본 이미지의 복원이 필요한 경우 삽입 과정에서 저장한 CF_2 값을 부가 정보로써 가지고 있어야 한다.

향후 연구에서는, 부가 정보 없이도 원본 이미지를 복원해 낼 수 있는 방법과 함께 더욱 다양한 스도쿠 솔루션과 모듈러 연산을 활용하여 비밀 정보 삽입 량 및 $PSNR$을 향상시킬 수 있는 방법을 연구할 예정이다.

REFERENCE

[1] S. Wang, Z. Cao, M.A. Strangio, and L. Wang, "Cryptanalysis and Improvement of an Elliptic Curve Diffie-Hellman Key Agreement Protocol," *IEEE Communications Letters*, Vol. 12, No. 2, pp. 149-151, 2008.

[2] C.W. Leung, F.Y. Ng, and D.S. Wong, "On the Security of a Visual Cryptography Scheme for Color Images," *Pattern Recognition*, Vol. 42, No. 5, pp. 920-940, 2009.

[3] B.H. Jeon, S.H. Shin, K.H. Jung, J.H. Lee and K.Y. Yoo, "Reversible Secret Sharing Scheme Using Symmetric Key Encryption Algorithm in Encrypted Images," Journal of the Korea Multimedia Society, Vol. 18, No. 11, pp. 1332-1341, 2015.

[4] J. Tian, "Reversible Data Embedding Using a Difference Expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, No. 8, pp. 890-896, 2003.

[5] D.M. Thodi and J.J. Rodriguez, "Expansion Embedding Techniques for Reversible Watermarking," *IEEE Transactions on Image Processing*, Vol. 16, No. 3, pp. 721-730, 2007.

[6] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 16, No. 3, pp. 354-362, 2006.

[7] K.S. Kim, M.J. Lee, and H.K. Lee, "Reversible Data Hiding Exploiting Spatial Correlation Between Sub-sampled Images," *Communications in Nonlinear Science and Numerical Simulation*, Vol. 42, No. 11, pp. 3083-3096, 2009.

[8] J.Y. Byun, P.H. Kim, J.H. Lee, K.H. Jung and K.Y. Yoo, "Data Hiding Using Pixel-Value Modular Operation," Journal of the Korea Multimedia Society, Vol. 18, No. 4, pp. 483-491, 2015.

[9] J.H. Lee, K.H. Jung and K.Y. Yoo, "Hybrid Information Hiding Method Based on the Characteristics of Military Images on Naval Combat System," Journal of the Korea Multimedia Society, Vol. 19, No. 9, pp. 1669-1678, 2016.

[10] T.S. Nguyen and C.C. Chang, "A Reversible Data Hiding Scheme Based on the Sudoku Technique," *Displays*, Vol. 39, pp. 109-116, 2015.

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

[12] G.R. Blakley, "Safeguarding Cryptographic Keys," *Proceedings of the National Computer*

Conference, Vol. 48, pp. 313-317, 1979.

[13] K.H. Jung and K.Y. Yoo, "Data Hiding Method Using Image Interpolation," *Computer Standards and Interfaces*, Vol. 31, No. 2, pp. 465-470, 2009.

[14] X. Wu and W. Sun, "High-capacity Reversible Data Hiding in Encrypted Images by Prediction Error," *Signal Processing*, Vol. 104, pp. 387-400, 2014.

[15] D.C. Wu and W.H. Tsai, "A Steganographic Method for Images by Pixel-value Differencing," *Pattern Recognition Letters*, Vol. 24, No. 9-10, pp. 1613-1626, 2003.

[16] C.M. Wang, N.I. Wu, C.S. Tsai, and M.S. Hwang, "A High Quality Steganographic Method with Pixel-value Differencing and Modulus Function," *Systems and Software*, Vol. 81, No. 1, pp. 150-158, 2008.

[17] A. Abdulfetah, X. Sun, and H. Yang, "Quantization Based Robust Image Watermarking in DCT-SVD Domain," *Information Technology*, Vol. 1, No. 3, pp. 107-114, 2009.

[18] A. Sverdlov, S. Dexter, and A.M. Eskicioglu, "Robust DCT-SVD Domain Image Watermarking for Copyright Protection: Embedding Data in All Frequencies," *Proceedings of Image Proceedings 2000*, Vol. 1, pp. 454-457, 2000.

[19] E. Yavuz and T. Ziya, "Improved SVD-DWT Based Digital Image Watermarking against Watermark Ambiguity," *Proceedings of the 2007 ACM Symposium on Applied Computing*, pp. 1051-1055, 2007.

[20] J. Mei, S. Li, and X. Tan, "A Digital Watermarking Algorithm Based on DCT and DWT," *Proceedings of the 2009 International Symposium on Web Information Systems and Applications*, pp. 104-107, 2009.

김 영 주

2015년 경북대학교 컴퓨터시스템공학과 공학사
2015년~현재 경북대학교 컴퓨터학부 석사과정
관심분야 : 정보보호, 스테가노그래피, 디지털 워터마킹

김 평 한

2013년 대구대학교 정보통신대학 전산공학전공(학사)
2016년 경북대학교 컴퓨터학부 공학석사
관심분야 : 암호학, 정보보호, 스테가노그래피

유 기 영

1976년 경북대학교 수학교육과 이학사
1978년 한국과학기술원 전산학과 공학석사
1992년 미국 Rensselaer Polytechnic Institute 전산학과 공학박사
1978년~현재 경북대학교 IT대학 컴퓨터학부 교수
1997년~1998년 한국정보과학회 영남지부장
1999년~현재 한국보호학회 종신회원
2006년~2008년 한국정보보호학회 부회장
관심분야 : 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜