http://dx.doi.org/10.7840/kics.2015.40.8.1477

가역적 데이터 은닉 시스템에서 RS 부호를 사용한 이미지 공간상관 관계 향상을 위한 전송 기법

김 태 수◆, 장 민 호*, 김 성 환°

Transmission Methods Using RS Codes to Improve Spatial Relationship of Images in Reversible Data Hiding Systems

Taesoo Kim◆, Min-Ho Jang*, Sunghwan Kim°

요 약

본 논문에서는 효율적인 데이터 전송을 위해 Reed-Solomon(RS) 부호를 활용하여 암호화된 이미지에 정보를 전송하는 새로운 가역적 데이터 은닉 기술을 제안한다. 암호화된 이미지로부터 데이터의 복구 시 발생하는 오류를 줄이기 위해 메시지를 RS 부호의 부호어를 생성 후 데이터 은닉키를 활용하여 암호화된 이미지에 반영한다. 수신자는 부호어가 포함된 암호화 이미지를 수신하고 먼저 암호화된 이미지를 암호화에 따라 이미지를 해독하고, 공간 상간관계를 이용하여 데이터를 추출한다. 이 추출한 데이터로부터 RS 부호의 정보를 계산하여 RS 복호기를 통해 메시지를 추정한다. 두 개 이미지와 RS 부호에 대한 모의실험 결과는 제안한 구조의 성능이 비트 오류 비율 측면에서 성능 향상을 보여준다.

Key Words : data hiding, image encryption, image processing, Reed-Solomon(RS) codes, security

ABSTRACT

In this paper, a novel reversible data hiding by using Reed-Solomon (RS) code is proposed for efficient transmission in encryption image. To increase the recovery of data from encrypted image, RS codes are used to encode messages, and then the codewords can be embedded into encrypted image according to encryption key. After receiving encrypted image which embeds the codewords, the receiver firstly decryptes the encrypted image using the encryption key and get metric about codewords containing messages. According to recovery capability of RS codes, better estimation of message is done in data hiding system. Simulation results about two images and two RS codes show that the performances of the proposed schemes are better than ones of the reference scheme.

Ⅰ. 서 론

가역적 데이터 은닉(reversible data hiding)은 미디어 속에 데이터를 넣고 데이터를 추출 후에 일그러짐 없이 본래의 이미지로 복구하는 기술이다. 의사 난수를 이용한 가역적 데이터 은닉 방법[1]은 이미지의 픽

※ 본 연구는 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구지원사업임(NRF-2014R1A1A1004521)
◆ First Author : School of Electrical Engineering, University of Ulsan, ktsu126@naver.com, 학생회원
° Corresponding Author : School of Electrical Engineering, University of Ulsan, sungkim@ulsan.ac.kr, 종신회원
* School of Electrical and Electronic Engineering, Ulsan College, mhjang@uc.ac.kr, 종신회원
논문번호 : KICS2015-06-183, Received June 12, 2015; Revised July 15, 2015; Accepted July 23, 2015

셀들 중 s×s 개수를 가지는 블록 안에서 데이터 은닉 키(data-hiding key)를 사용하여 균등하게 2개의 그룹으로 나누고, 블록에 끼워 넣을 데이터에 따라 픽셀의 3개의 최소 유효 비트(least significant bits (LSB))를 뒤집어서 데이터를 숨긴다. 데이터를 추출하기 전, 먼저 이미지를 해독한 후에 다시 2개의 그룹으로 나뉘며, 숨긴 데이터는 공간 상간관계를 이용해서 데이터를 추출하는 방법을 사용한다. 만약 데이터 추출에서 오류가 발생하지 않으면 본래의 이미지와 같은 이미지가 나온다. Hong[2]은 논문[1]의 이미지 암호화와 데이터를 은닉하는 방법은 동일하지만 데이터를 추출하고 이미지를 복구하는 부분에서 신뢰도가 높은 데이터를 우선 복구하고 신뢰도 낮은 픽셀의 복구 시 우선 복구된 픽셀의 가장자리를 활용하는 사이드 매치(side match) 방식을 제안하였다. 특히 논문[2]에서는 공간 상관관계를 계산 방식은 인접한 2개의 픽셀들의 차이를 가로방향과 세로방향으로 차이를 계산하게 변경하였고 논문[1]에서 데이터 추출 시 가장자리의 픽셀들은 공간 상관관계의 계산에서 제외되지만, Hong은 인접한 네 개의 픽셀 그룹의 이미지 복구 여부를 판단하여 이미지가 복구 되었을 시 데이터를 추출할 블록에 복구된 블록의 가장자리의 픽셀들을 덧붙여 공간 상관관계를 계산한다. Zhang은 논문[3]에서 이미지의 모든 픽셀에 파라미터를 은닉할 소수 픽셀을 제외한 나머지 픽셀들을 그룹으로 나누고 각 그룹에 특정수의 LSB 사용하며 이를 보내고자 하는 정보 비트수가 그 그룹에 은닉되도록 압축하고 남은 공간에 메시지를 전송하는 방법을 제안하였다. 기존 연구와 차이점은 데이터 은닉키와 암호키의 활용이 분리되어 있어 수신자가 데이터 은닉키만 가지고 있다면 파라미터를 은닉한 픽셀들을 찾아 숨긴 파라미터를 찾을 수 있고 은닉 정보를 바로 찾을 수 있고 암호키만 가질 경우 숨긴 데이터는 찾을 수 없지만 본래의 이미지와 유사한 이미지를 얻을 수 있다. 논문[4]는 기존 데이터 은닉 방식처럼 데이터를 바로 암호화된 이미지에 바로 은닉하는 방법 대신 암호화 전 일부 픽셀을 선택하여 데이터 은닉을 수행하는 방법을 제안하였다. 나머지 픽셀들은 기준 암호화 알고리즘(예를 들어 고급 암호화 표준)을 사용하여 암호화 하고 추정된 픽셀들은 특별한 방법을 통하여 암호화하는 방식을 사용하였고, 주요 특징은 이미지 복구와 데이터 추출의 순서에 제한받지 않는 장점이 있다. 또 다른 방법으로 개선된 인접 픽셀 차이를 이용한 가역 데이터 은닉[5]을 인접한 픽셀을 차이 값을 이용하여 히스토그램(histogram)을 생성하여 두 최댓값에 데이터를 끼어 넣는 데이터 은닉 방법이 제안되었다. 또한 DQT(Define Quantization Table)을 사용한 방법[6]은 JPEG 형식으로 저장된 이미지를 3가지 과정을 통해 이미지를 보호한다. 효율적인 데이터 전송을 위해 격자(lattice)를 활용한 가역적 데이터 은닉 방법이 제안되었다.[7]

Reed-Solomon(RS) 부호(code)는 최대 거리 분리(maximum distance separable 부호이며 버스티(bursty) 오류의 정정능력이 우수한 특성을 가지므로 광학 통신, 방송 시스템, 가전, 데이터 전송 기술에 널리 사용된다. 효과적인 RS 부호의 복호화(decoding)를 위해 제안된 Berlekamp-Massey(BM) 알고리즘[8]은 가장 작은 차수(degree)가지는 오류 위치를 찾기 위해서 선형 피드백 시프트 레지스터(linear feedback shift register (LFSR))를 사용하여 효율적인 강성 결정 (hard decision) 방식에 기반을 둔다. 또한 복호 8비트의 심벌 오류정정회로 2개를 이용하여 기존보다 빠르고 회로량이 줄어든 오류위치추적기가 제안되었다.[9] RS 부호를 지연프레임과 시간다이버시티(delayed frame time diversity)와 함께 사용한 방법을 제안하였다[10]. RS 부호의 새로운 활용으로 가시광 환경에서 RS 부호의 성능을 증가시키기 위해서 새로운 런 렝스 제한(run-length limited) 복호화 알고리즘이 제안되었다[11]. 또한 유비쿼터스 환경에서 LED를 이용한 근거리 무선 전송 기술에 RS 부호를 활용한 연구가 수행되었다[12].

이 논문은 RS 부호를 활용하여 암호화 이미지에서 가역적 데이터를 효율적으로 복구하는 방법을 제안한다. 제안한 데이터 은닉 시스템은 3가지 구조인 이미지 암호화(image encryption), 데이터 은닉(data hiding), 데이터 추출 및 이미지 해독(data extraction & image decryption)으로 구성된다. 데이터 은닉 및 복구 시 메시지를 암호화된 이미지 속에 바로 넣지 않고 메시지를 RS 부호의 부호어(codeword)로 만들어서 그 이미지 속에 반영한다. RS 부호의 오류 정정 능력을 활용하여 은닉된 데이터의 추정 오류를 개선한다. 제안된 방법의 성능향상을 확인하고자 두 개의 이미지와 RS 부호를 사용한 경우의 모의실험 결과를 논문[1]과 논문[2]성능 비교하여 수행하였다.

Ⅱ. 본 론

본 논문에서 제안하는 시스템은 그림 1의 블록도에 제시된다. 제안한 시스템은 이미지 암호화, 데이터 은닉, 데이터 추출 및 이미지 해독의 세 가지 항목으로 구성되며 이는 참조 논문[1]의 시스템과 유사하다. 이

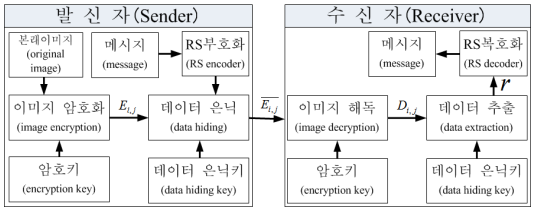

그림 1. 제안된 데이터 은닉 시스템의 블록다이어그램
Fig. 1. Block diagram of the proposed data hiding system

미지 암호화에서는 암호키(encryption key)를 이용한 의사 난수를 그림의 각각의 픽셀과 배타적 논리합(exclusive-or)하여 암호화된 이미지를 만든다. 다음 데이터 은닉 부분은 메시지를 암호화된 이미지에 숨기는 과정을 의미하며, 메시지를 RS 부호의 부호어로 생성하고 데이터 은닉키에 따른 간단한 과정을 통해서 부호어를 그 이미지에 숨기게 된다. 이미지를 암호화 하는 사람과 데이터를 숨기는 사람이 다를 경우, 데이터를 숨긴 사람은 본래의 이미지를 알 수 없다. 수신자는 먼저 데이터를 숨긴 암호화된 이미지를 암호키를 이용해 해독한다. 이 과정에서 얻은 해독된 이미지는 본래의 그림과 비슷한 이미지를 얻게 되며, 그 해독된 이미지는 데이터 은닉키에 따라서 숨겨진 부호어를 추출하고, 그 부호어를 복호화 하여 오류를 정정하여 데이터를 복구한다.

2.1 이미지 암호화

이미지 암호화에서는 각각의 픽셀이 8 비트로 표현된 그레이 값(gray value)로 구성된 이미지를 사용한다. 이 그레이 값은 $g_{i,j,k}$로 정의하고 (*i*, *j*)와 *k*는 픽셀의 위치와 8 비트에서 위치를 나타낸다. (*i*, *j*)에 위치한 픽셀 값은 p_{ij}로 표현되며 픽셀과 그레이 값은 다음과 같은 상관식으로 표현된다

$$g_{i,j,k} = \lfloor \frac{p_{i,j}}{2^k} \rfloor \mod 2 (0 \leq k \leq 7) \tag{1}$$

$$p_{i,j} = \sum_{k=0}^{7} g_{i,j,k} \cdot 2^k \tag{2}$$

여기서 $\lfloor a \rfloor$ 는 a보다 작거나 같은 최대 정수를 나타낸다.

이미지를 암호화하기 위해서, 우리는 암호키를 사용하여 의사 난수를 픽셀의 총 개수만큼 만들어서 각각 픽셀에 해당하는 의사 난수 $r_{i,j}$(8비트)를 배타적 논리합 (exclusive-or)을 이용하여 이미지를 암호화한다. 암호화된 픽셀은 다음과 같이 표시된다.

$$E_{i,j} = p_{i,j} \oplus r_{i,j} \tag{3}$$

2.2 데이터 은닉

데이터 전송 효율을 높이기 위해 암호화된 이미지에 RS 부호와 더미를 보내는 것을 고려한다. 일반적으로 RS 부호[4]는 갈로아 필드(Galois field) 상에서 정의되며 양의 정수 q에 대해 갈로아 필드는 GF(2^q)로 표기한다. RS 부호의 파라미터는 (n, k)로 표시하며 이때 n은 RS 부호의 길이, k는 부호의 차원이다. 파라미터와 갈로와 필드와 관계는 n이 2^{q-1}로 정의되고, 최대 오류 정정 수는 $\tau=(n-k)/2$로 정의 된다. RS 부호는 선형 부호이며 순환 부호이므로 메시지와 부호어는 다음과 같은 메시지 다항식$m(X)$과 부호어 다항식 $c(X)$로 표현된다.

$$m(X) = m_0 + m_1 X + \cdots + m_{k-1} X^{k-1} \tag{4}$$

$$c(X) = c_o + c_1 X + \cdots + c_{n-1} X^{n-1} \tag{5}$$

여기서 i= 0, 1, …, k-1에 대해 $m_i \in (2^q)$이고, j= 0, 1, …, n-1에 대해 $c_j \in (2^q)$이다. 최대 정정 오류 수인 τ보다 작거나 같은 정수인 t에 대해 최대 t개의 심벌 오류를 정정하는 RS 부호의 경우, 생성 (generator) 다항식은 α가 GF(2^q)의 원시 요소(primitive element)일 때 다음과 같이 정의된다.

$$\begin{aligned} g(X) &= (X-\alpha)(X-\alpha^2)\cdots(X-\alpha^{2\tau}) \\ &= g_0 + g_0 X + \cdots + g_{2\tau} X^{2\tau} \end{aligned} \tag{6}$$

RS 부호의 부호어 생성하는 부호화는 다음과 같은 시스템화(systematic) 방식을 고려한다.

$$c(X) = P(X) + X^{2\tau} u(X) \tag{7}$$

$p(X)$는 2t보다 작은 차수의 패리티 다항식이며, $g(X)$를 $X^{2t}m(X)$로 나눌 때, $p(X)$는 나머지로 계산 될 수 있다. 이 RS 부호의 시스템 부호화 처리의 알고리즘은 그림 2에 나타낸다.

데이터를 숨기는 사람은 암호화된 이미지에 RS 부호의의 부호어를 몇 개의 과정을 통해서 끼워 넣지만, 그는 본래의 이미지를 알 필요가 없다. 먼저 암호화된 이미지를 한 변의 픽셀의 수가 s인 정사각형의 블록으로 나누고, (m-1) • $s \leq i \leq m$ • s, (n-1) • $s \leq j \leq$

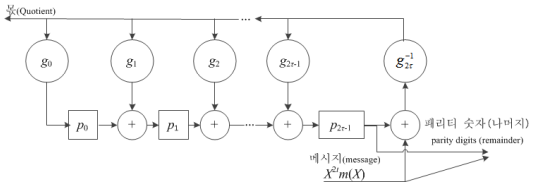

그림 2. RS 부호의 부호화 알고리즘
Fig. 2. Encoding algorithm of RS code

$n \bullet s$ 범위에 존재하는 픽셀은 같은 블록에 포함된 것이다. 그 블록 안에 있는 픽셀의 비트 $E_{i,j}$에 부호어를 삽입한다.

각각의 블록에 대해서, 데이터 은닉키를 사용해서 블록 속의 픽셀들을 두 그룹(S_0, S_1)으로 나뉘며, 픽셀이 두 그룹에 속할 확률은 균등 분포(uniform distribution)가 되도록 그룹을 생성한다. 만약 해당되는 정보가 0일 경우, S_0그룹에 속한 픽셀들의 3개의 최소 유효 비트를 뒤집어 표시하고, 1일 경우 S_1그룹에 속한 픽셀들의 3개의 최소 유효 비트를 뒤집는다. 이를 수식화하면 다음과 같이 표현된다.

$$\overline{E_{i,j}} = \begin{cases} E_{i,j} \oplus 111_{(2)} (i,j) \in S_0 \text{ if data} = 0 \\ E_{i,j} \oplus 111_{(2)} (i,j) \in S_1 \text{ if data} = 1 \end{cases} \tag{8}$$

2.3 데이터 추출 및 복호화

암호키와 데이터 은닉키는 안전하게 수신자에게 전송되었다는 가정 하에 데이터 추출 및 복호화를 실행한다. 이미지를 수신한 후 데이터 추출하기 위해서 암호키를 이용해서 구한 $r_{i,j}$을 암호화된 이미지에 배타적 논리합을 이용하여 이미지를 해독한다. 해독된 이미지는 본래의 이미지와 유사한 이미지가 되며, 그 해독된 이미지의 그레이 값을 $D_{i,j}$으로 정의한다. $D_{i,j}$의 5개의 최상위 비트(most significant bit)는 반전이 없으므로 원래의 이미지와 차이가 없고 하위 3비트의 경우 반전이 생긴다. 이에 대한 계산 방법은 다음과 같이 기술된다.

$$\begin{aligned} D_{i,j} &= r_{i,j} \oplus \overline{E_{i,j}} \\ &= r_{i,j} \oplus p_{i,j} \oplus 111_{(2) \oplus r_{i,j}} \\ &= p_{i,j} \oplus 111_{(2)} \end{aligned} \tag{9}$$

만약 선택된 블록에서 끼어 넣은 데이터가 0이고 S_1에 속한 픽셀들은 본래 이미지의 그레이 값과 같고, 마찬가지로 끼어 넣은 데이터가 1이고, S_0에 속한 픽셀들도 본래의 그레이 값과 같다. 식(9)에서는 블록에 끼어 넣은 데이터가 0이고 S_0에 속한 경우와 끼어 넣은 데이터가 1이고 S_1에 속한 경우, 해독된 이미지의 그레이 값이 본래의 그레이 값의 뒤집힌 값이라는 것을 알 수 있다.

이미지 해독이 완료되면, 데이터 은닉키를 이용해서, 블록에 있는 픽셀들을 다시 S_0, S_1그룹으로 나눌 수 있다. 해독된 블록에서 S_0에 속한 모든 픽셀의 3개의 최소 유효 비트를 뒤집어 새로운 그룹을 만들고, S_1에 속한 모든 픽셀의 3개의 최소 유효 비트를 뒤집어 다른 새로운 그룹을 만든다. 새로운 그룹(H_0, H_1)중 하나의 그룹은 본래의 그레이 값을 가지는 그룹이 된다. RS 부호의 부호어를 추출하기 위해서 새로운 그룹간의 그레이 값의 변동을 측정한다.

$$f = \sum_{i=2}^{s-1} \sum_{j=2}^{s-1} \left| p_{i,j} - \left(\frac{p_{i-1,j} + p_{i,j-1} + p_{i+1,j} + p_{i,j+1}}{4} \right) \right| \tag{10}$$

가공하지 않은 이미지에서 공간 상간관계(spatial correlation)에 의해서, 측정한 2개의 결과 값(f_0, f_1)중 작은 값을 가지는 그룹이 본래의 그레이 값이 된다. 다시 말해서, $f_0 < f_1$라고 한다면, H_0그룹이 본래의 그레이 값을 가지는 그룹이 되며 반대로 $f_0 > f_1$라고 한다면 H_1그룹 본래의 값을 가지는 그룹이 된다.

$$c_i = \begin{cases} 0, & \text{if } f_0 < f_1 \\ 1, & \text{if } f_0 > f_1 \end{cases} \tag{11}$$

추출한 데이터는 RS 부호의 부호어로 다시 형성하고, 그 부호어를 BM 알고리즘을 사용하여 복호화 한다. 이 알고리즘은 선형 피드백 시프트 레지스터로 기반으로 둔 다항식의 오류 위치를 찾는데 효율적이다. 오류위치와 오류 수치는 BM 알고리즘의 신드롬(syndrome)을 활용하여 쉽게 계산이 가능하다. 먼저, 추출한 부호어를 아래와 같이 정의한다.

$$\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e} \tag{12}$$

식(5)의 특징을 이용해서 신드롬과 오류 위치 다항식을 (13), (14)와 같이 정의한다.

$$\begin{aligned} S_i &= c(\alpha^i) + e(\alpha^i) = e(\alpha^i) \\ &= e_0 + e_1 X + \cdots + e_{n-1} X^{n-1} 1 \end{aligned} \tag{13}$$

$$\Lambda(X) = \Lambda_0 + \Lambda_1 X + \cdots + \Lambda_{n-1} X^{n-1} \tag{14}$$

그리고 오류 위치 다항식의 신드롬 계수 사이의 관계는 t개 오류 정정이 가능한 RS 부호의 경우 $v<\tau$ 인 경우에 대해 다음과 같이 정의된다.

$$S_i = -\sum_{j=1}^{v} \Lambda_j S_{i-1} \tag{15}$$

선형 피드백 시프트 레지스터를 사용한 BM는 식 (15)을 만족하는 최소의 차수의 오류 위치 다항식을 찾고, 오류 위치는 오류 위치 다항식의 근을 계산함으로써 쉽게 계산된다. 오류 위치를 이용하여 해당되는 오류 위치의 오류 값을 Forneys[13] 알고리즘으로 구할 수 있다.

Ⅲ. 실 험

그림 3에 나타나는 있는 레나(Lenna)와 고추(Peppers) 이미지는 무료로 사용이 가능하여 본 실험에 사용하였고 이미지의 크기는 512×512이다. 두 이미지에 대해 각각 다른 길이 및 부호율을 가지는 (15, 11) RS 부호 및 (31, 23) RS 부호를 제안한 데이터 은닉 시스템에 적용하여 모의실험을 수행하였다.

이미지를 $s \times s$ 블록으로 나눌 경우 길이 s에 따른 추출된 비트 오류 비율(extracted-bit error rate (BER)) 성능이 그림 4와 그림 5에 도시화하였다.

그림 4와 그림 5는 각각 레나와 고추의 이미지를 사용한 경우의 성능에 해당한다. 또한 '(15, 11) RS 부호'와 '(31, 23) RS 부호'는 해당 이미지에 (15, 11) RS 부호 (31, 23) RS 부호를 사용한 경우의 BER 성능을 나타낸다. 그림 4와 그림 5에서 논문[1]시스템은 이미지 암호화 부분은 제시된 시스템과 같으며, 암호화된 이미지에 메시지를 바로 은닉하는 시스템이며, 논문[2]시스템과 본 논문의 차이점은 논문[1] 및 본 논문에서 고려한 공간 상관관계를 계산하는 식(10)과 다른 다음과 같은 상관관계 계산 수식을 고려하였다.

(1)레나(Lenna) (2)고추(Pappers)

그림 3. 모의실험에 사용한 이미지
Fig. 3. Test images in simulation

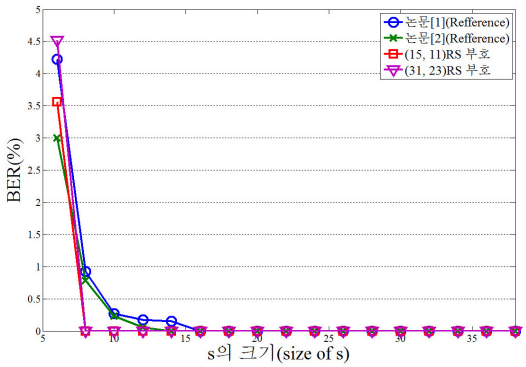

그림 4. 레나를 사용하였을 때 BER 성능
Fig. 4. BER performance when Lenna image is used

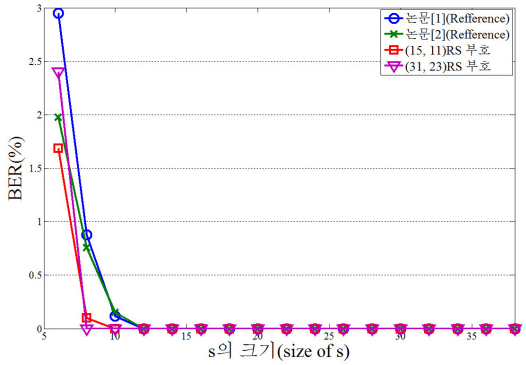

그림 5. 고추를 사용하였을 때 BER 성능
Fig. 5. BER performance when Pepper image is used

$$f = \sum_{i=1}^{s}\sum_{j=1}^{s-1}|p_{i,j} - p_{i,j+1}| + \sum_{i=1}^{s-1}\sum_{j=1}^{s}|p_{i,j} - p_{i+1,j}| \tag{16}$$

논문[2]의 공간 상관관계는 인접한 픽셀의 가로의 상관관계와 세로의 상관관계의 합으로 나타내며 본 실험에서 블록의 크기가 $s \times s$이기 때문에 식(16)의 파라미터를 변경하였다. 데이터를 추출하는 방식은 복구할 블록의 주변 4개의 블록의 복구여부를 조사하여 4개의 블록이 복구가 되지 않은 경우, 4개의 블록 중 하나라도 복구가 된 경우로 나뉜다. 첫 번째의 경우 논문[1]과 같이 그룹(H_0, H_1)에 해당되는 f_0, f_1을 비교하여 작은 값의 f를 찾아 해당되는 데이터를 추출하며, 두 번째의 경우 4개의 블록 중 복구된 블록의 가장자리 픽셀들을 그룹에 붙여서 새로운 그룹(Hc_0, Hc_1)만들어 fc_0, fc_1값에 따라서 fc_0가 더 작을 경우 추출된 데이터는 0이며 반대로 fc_1가 더 작을 경우 1을 추출하는 시스템이다.

그림 4와 그림 5에서 제안한 데이터 은닉 시스템의

성능은 참조 논문[1]과 비교 시 대부분의 s의 경우 BER 측면에서 성능이 우수하거나 동등하다. 제안 방식과 비교 시스템 모두 s가 커지면 커질수록 BER 성능 또한 점점 좋아지고 s의 값이 16이상으로 커지면 오류율이 발생하지 않음을 확인할 수 있다. 사용한 이미지 간 성능 비교를 살펴보면 그림 4의 레나 이미지 사용 시 성능보다 그림 5의 고추 이미지 사용 결과가 같은 s에 대해 우수한데 이는 고추이미지의 공간상간 관계가 레나의 공간 상간관계보다 강하여 은닉 데이터 추정 시 오류발생 가능성이 낮기 때문으로 추정된다. 또한 RS 부호의 사용은 가역적 데이터 은닉 시스템에서 약해진 공간상관관계를 개선하는 방법으로 활용될 수 있음을 의미한다. 참조 논문[2]의 실험결과와 유사하게 신뢰도 높은 픽셀을 우선 추정하고 신뢰도 낮은 픽셀 정보를 추정 시 우선 추정된 가장자리 픽셀들을 활용하므로 논문[1]의 성능보다 우수함을 확인 할 수 있다. 또한 s의 크기가 커질수록 논문[1]과 논문[2]의 성능보다 제안한 방식의 암호 성능이 BER 측면에서 우수함을 확인 수 있다. 하지만 RS 부호의 사용할 경우 부호율이 1보다 작기 때문에 부호어를 전송할 경우 메시지 전송 비율은 부호어를 사용하지 않는 경우와 비교 시 데이터 전송률 차원에서 단점을 가진다. 따라서 부호율을 고려한 데이터 전송율과 개선된 s사이의 관계를 고려하여 공평한 비교를 위해 다음과 같은 성능 비교를 수행한다.

참조 논문[1]와 논문[2]시스템과 공평한 성능 비교를 위해 메시지 오류가 나타나지 않는 s에 해당하는 논문 메시지의 수와 제안된 시스템의 실제 전송 메시지 수를 비교하였다. 이는 그림 4, 5 논문과 제시한 시스템에서 BER이 0이 되는 최소 s 의 크기와 이에 해당하는 전송 메시지 수를 정리한 내용을 표 1에 정리하였다. 그림 4에서 논문 시스템과, '(15, 11) RS 부호', '(31, 23) RS 부호'의 s는 각각 16, 14, 8, 8이며 그림 5에서 처음 0이 되는 s값은 각각 12, 12, 10, 8이다. 암호화된 이미지에 숨길 수 있는 메시지 수(size of message)를 계산하기 위해서 아래와 같은 식을 사용하였다.

$$\text{메시지 수} = \left\lfloor \left(\frac{512}{s}\right)^2 \cdot \frac{k}{n} \right\rfloor \quad (17)$$

표 1에서 이득(gain)은 비트 오류율이 0일 때 비교 논문의 최대 메시지 수와 제안한 시스템의 최대 메시지 수의 비율(%)을 의미하며 (18)과 같은 수식으로 정리된다.

$$\text{이득}(\%) = \frac{\text{제시한 시스템의 메시지 수}}{\text{참조 논문의 메시지 수}} \times 100 \quad (18)$$

G1와 G2는 (18)식에서 참조 논문에 해당하는 논문이 각각 논문[1]과 논문[2]일 제안 시스템의 이득을 의미한다.

표 1에서 RS (15, 11) 부호의 성능은 논문[1]의 성능보다 293% 향상된 성능을 보여줬고, RS (31. 21) 부호의 성능은 297%가 향상된 성능을 보여준다. 논문[2]의 대한 성능 비교는 (15, 11)부호의 성능은 224.7%가 향상되었고 (31, 23)은 227.3%의 성능 향상을 볼

표 1. 레나에 대한 비트 오류 없는 최소 s 크기 및 전송 메시지 수 비교
Table 1. Comparison with minimum size of s and size of message when there is no bit error for Lenna image

	레나(Lenna)			
	논문[1] (reference)	논문[2] (reference)	(15, 11) RS 부호	(31, 23) RS 부호
부호율 (code rate)	1	1	0.73	0.74
s의 크기 (size of s)	16	14	8	8
메시지 수 (size of message)	1024	1337	3004	3039
이득(%) (gain)	G1		293.3	296.8
	G2		224.7	227.3

표 2. 고추에 대한 비트 오류 없는 최소 s 크기 및 전송 메시지 수 비교
Table 2. Comparison with minimum size of s and size of message when there is no bit error for Pepper image

	고추(Peppers)			
	논문[1] (reference)	논문[2] (reference)	(15, 11) RS 부호	(31, 23) RS 부호
부호율 (code rate)	1	1	0.73	0.74
s의 크기 (size of s)	12	12	10	8
메시지 수 (size of message)	1820	1820	1922	3039
이득(%) (gain)	G1		105.6	167.0
	G2		105.6	167.0

수 있다. 표 2에서 (15, 11)인 경우는 105.6% 향상된 성능을 보이고 (31, 21)인 경우 167% 향상된 성능을 볼 수 있다. 논문[2]에 대해 각각 105.6%와 167%의 성능을 향상을 보인다. 표 2에서 s의 크기가 논문[1]와 논문[2]가 동일하기 때문에 같은 메시지 수를 가진다. 이는 부호율까지 고려한 비교에서도 제안된 방식이 이미지에 따라 데이터 은닉의 경우에 효율적인 전송이 가능함을 확인할 수 있다.

Ⅳ. 결 론

이 논문에서 암호화된 이미지에 대한 가역적 데이터 은닉 시스템에서 RS 부호를 사용한 효율적인 전송 방법에 대해서 제안한다. 데이터 은닉 전에 RS 부호화를 하고 데이터 추출 후 RS 복호를 통해서 발생하는 비트 오류를 줄인다. 이미지 암호화 부분에서 암호키를 이용해 의사 난수를 발생시킴으로써 XOR를 사용하여 이미지를 암호화한다. 데이터 은닉에서는 메시지를 바로 끼어 넣지 않고, 메시지를 RS 부호의 부호화로 부호어를 만들어서 각각의 블록에 끼어 넣고, 블록 속 픽셀들을 데이터 은닉키에 따라 균등 하게 2개의 그룹으로 나뉘어서 제시된 방법으로 데이터를 끼워 넣는다. 모의실험 결과 일반적인 데이터 은닉 방식에 비해 최대 2배의 전송 효율을 달성함을 확인할 수 있다.

References

[1] X. Zhang, “Reversible data hiding encrypted image,” *IEEE Signal Process. Lett*., vol. 18, no. 4, pp. 255-258, Apr. 2011.

[2] W. Hong, T.-S. Chen, and H.-Y. Wu, “An improved reversible data hiding in encrypted images using side match,” *IEEE, Signal Process. Lett.*, vol. 19, no. 4, pp. 199-202, Apr. 2012.

[3] X. Zhang, “Separable reversible data hiding encrypted image,” *IEEE Trans. Inf. Forensics and Security,* vol. 7, no. 2, pp. 826-832, Apr. 2012.

[4] W. Zhang, K. Ma, and N. Yu “Reversibility improved data hiding in encrypted images,” *Signal Process.,* vol. 94, pp. 118-127, Jan. 2014.

[5] S.-H. Cho, D.-S. Kim, and K.-Y. Yoo, “Improved reversible data hiding scheme based on difference value of adjacent pixels,” in *Proc. KICS Int. Conf. Commun.*, pp. 790-791, Pyeongchang, Korea, Feb. 2012.

[6] S. W. Kim, S. Yoo, J. Shin, and J. Ryou, “A study on the protection method for the medical image using DQT encryption,” in *Proc. KICS Int. Conf. Commun.*, pp. 205-206, Jeju Island, Korea, Jun. 2013.

[7] Y. Kim and D. Lim, “Lattice-based reversible data hiding,” *J. KMMS,* vol. 16 no. 4, pp. 27-33, Feb. 2012.

[8] J. G. Proakis and M. Salehi, *Digital communications*, NY: McGraw-Hill, pp. 471-475, 2008.

[9] H.-K. An, “Optimizing the circuit for finding 2 error positions of 2 error correcting Reed Solomon decoder,” *J. KICS,* vol. 36 no. 1, pp. 8-13, Jan. 2011.

[10] K.-R. Koh and W.-W. Kim, “Performance analysis of telemetering method using delayed frame time diversity (DFTD) and Reed-Solomon code,” *J. KICS*, vol. 37A, no. 7, pp. 503-511, Jul. 2012.

[11] H. Wang and S. Kim, “New RLL decoding algorithm for multiple candidates in visible light communication,” *IEEE Photon. Technol. Lett*., vol. 27, no. 1, pp. 15-17, Jan. 2015.

[12] Y. Lee, “A study on the short-range wireless transmission technology using the LED in ubiquitous environment,” *J. KICS*, vol. 17, no. 09, pp. 2174-2182, Sept. 2013.

[13] T. K. Moon, *Error correction coding*, Wiley-interscience, pp. 242-243, 2004.

김 태 수 (Taesoo Kim)

2014년 2월 : 울산대학교 전기공학부 졸업

2014년 3월~현재 : 울산대학교 전기공학부 석사과정

<관심분야> 통신공학, 오류정정 부호, 양자 정정, 데이터 은닉

장 민 호 (Min-Ho Jang)

2002년 8월 : 연세대학교 전기전자공학부 공학사
2004년 8월 : 서울대학교 전기컴퓨터공학부 공학석사
2009년 2월 : 서울대학교 전기컴퓨터공학부 공학박사
2009년 3월~2011년 8월 : 삼성전자 DMC연구소 책임연구원
2011년 9월~현재 : 울산과학대학교 전기전자공학부 조교수
<관심분야> 디지털통신, 이동통신시스템, 오류정정부호, OFDM, 정보보호

김 성 환 (Sunghwan Kim)

1999년 2월 : 서울대학교 전기공학부 졸업
2001년 2월 : 서울대학교 전기컴퓨터공학부 공학석사
2005년 8월 : 서울대학교 전기컴퓨터공학부 공학박사
2005년 10월~2007년 4월 : Georgia Institute of Technology 박사후 과정
2007년 5월~2011년 2월 : 삼성전자 DMC 연구소 책임 연구원
2011년 3월~현재 : 울산대학교 전기공학부 부교수
<관심분야> 디지털 통신, 오류정정부호, LDPC 부호, 양자 정보, 가시광 통신, 데이터 은닉