The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 6, pp.281-288, Dec. 31, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.6.281
JIIBC 2014-6-40

이진 이미지를 위한 QR 코드 기반의 가역적인 데이터 은닉

Reversible Data Hiding based on QR Code for Binary Image

김천식*

Cheonshik Kim*

요 약 QR 코드는 바코드보다 수백 배 많은 양의 데이터를 인코딩할 수 있도록 기능을 향상시킨 코드체계로서 이미지 훼손에 강하다. 이러한 이유로 QR 코드는 최근에 다양한 분야에서 사용되고 있다. 예를 들어 항공권 티켓 (보딩 통제 시스템), 푸드 (야채, 육류 이력) 추적 시스템, 콘택트렌즈 관리, 처방전 관리, 환자 손목밴드 (환자관리) 등에 사용된다. 본 논문에서는 이진 이미지에 대한 가역적인 데이터은닉 방법을 제안한다. 가역적인 데이터 은닉방법은 스테고 이미지로부터 데이터를 추출한 후 원본 이미지를 복원할 수 있기 때문에서 다양한 목적으로 활용될 수 있다. QR 코드는 누구나 코드를 생성할 수 있으므로 위조된 QR 코드를 이용하여 범죄에 사용할 수 있다. 본 논문에서는 이를 방지하기 위해서 이진 QR 코드 이미지에 인증 데이터를 은닉하여 위조여부를 확인할 수 있도록 하였다. 본 논문에서는 제안한 방법은 실험을 통해서 입증을 하였다.

Abstract QR code (abbreviated from Quick Response Code) is code system that is strong in against to apply image processing techniques (skew, warp, blur, and rotate) as QR codes can store several hundred times the amount of information carried by ordinary bar codes. For this reason, QR code is used in various fields, e.g., air ticket (boarding control system), food(vegetables, meat etc.) tracking system, contact lenses management, prescription management, patient wrist band (patient management) etc. In this paper, we proposed reversible data hiding for binary images. A reversible data hiding algorithm, which can recover the original image without any distortion from the marked (stego) image after the hidden data have been extracted, because it is possible to use various kinds of purposes. QR code can be used to generate by anyone so it can be easily used for crime. In order to prevent crimes related QR code, reversible data hiding can confirm if QR code is counterfeit or not as including authentication information. In this paper, we proved proposed method as experiments.

Key Words : QR code, Data Hiding, Reversible, Binary Image

Ⅰ. 서 론

데이터 은닉[1,2,3,4]은 원본 이미지에 정보를 은닉하는 기술로서 저작권, 주석(註釋)과 통신 등에 활용이 가능하다. 예를 들어 컬러이미지 (회색 이미지 포함)의 각 픽셀에 대해서 LSB의 값을 변경함으로써 비밀 정보를 은닉

*종신회원, 안양대학교 디지털미디어공학과
접수일자: 2014년 9월 7일, 수정일자: 2014년 10월 8일
게재확정일자: 2014년 12월 12일

Received: 7 September, 2014 / Revised: 8 October, 2014
Accepted: 12 December, 2014
*Corresponding Author: mipsan@paran.com
Dept. of Digital Medial Engineering, Anyang University, Korea

할 수 있다. 컬러이미지와는 달리 이진 이미지는 각 픽셀의 변경이 이미지에 큰 영향을 주기 때문에 사람의 시각으로도 쉽게 탐지될 수 있다. 이와 같은 문제점에도 불구하고 이미지에 훼손이 없이 많은 량의 비밀데이터를 저장할 수 있는가는 가장 큰 도전중의 하나이다. 또한, 이미지에 훼손이 적을수록 사람에 시각 시스템 (human visual systems)[5]에 의한 탐지 가능성이 줄어든다. 디지털 도서관에서 문서나 중요한 그래픽 이미지에 주석을 넣는 것은 매우 중요하다 왜냐하면 파일관리나 소유권을 주장하는데 사용될 수 있기 때문이다. 이러한 기술을 사용하는 이유는 은닉 정보가 콘텐츠의 정품인증에 활용될 수 있다. 디지털 도서관에서의 응용에서 중요한 목표는 스테고(Stego) 이미지로부터 원본 이미지를 완벽하게 복원하는 것이 목표이다. 그러나 이 목표인 가역적 데이터 은닉 방법(方法)은 매우 어려운 기술이다. Tsai는 이진 이미지를 위한 PWLC (Tsai 등이 제안한 방법, 2005)기반의 가역적 데이터 은닉 방법을 제안했다[6]. 이 방법은 데이터 은닉 후 이미지(비밀 정보를 포함)의 화질(畫質) 성능을 감소시킨다. 본 논문에서 우리는 이진 이미지 형태의 QR 코드[7]에 가역적인 데이터은닉 시스템을 제안하고자 한다. 제안한 방법은 원본 이미지에 주석과 같은 부가 정보를 은닉하는 것으로 많은 연구자들이 디지털 도서관의 등장과 함께 연구의 필요성이 증대되고 있다.

지금까지 이진 이미지를 기반으로 한 데이터 은닉에 관한 많은 연구가 있었다. 이진 이미지의 연구는 크게 두 가지로 분류할 수 있다. 첫째, 픽셀-방법(pixel-wise) : Fu(2000)[8]등은 픽셀을 무작위로 선택하는 방법(方法)을 제안했고 이런 이유 때문에 스테고(stego) 이미지의 화질(畫質)의 성능은 좋지 않다. 이런 문제를 해결하기 위해서 Kim(2005)[9]등과 Mei(2001)[10]등은 시각에 크게 영향을 미치는 요인을 측정함으로서 이미지의 화질을 향상시시키는 방법을 제안했다.

두 번째, 블록기반 방법: 원본 이미지를 블록으로 나누고 각 블록 (키 블록 포함)의 특성에 따라서 블록 내에 있는 픽셀을 변경한다. Wu (2004)[11]등이 제안한 방법은 각 블록에서 흑색(黑色) 픽셀의 수에 대한 패리티를 변경하는 방법이다. Tseng(2001)[12]와 Chang(2005)[13]등은 특정 픽셀 1개를 변경하는 방법을 제안했다.

세 번째, 히스토그램 방법: 이 방법은 한 이미지에 대해 히스토그램 생성하고 이를 이용하여 데이터를 은닉하고 데이터를 추출한 후에는 원본 이미지를 복원(復元)할 수 있는 방법이다. 히스토그램에 기반을 둔 이 방법은 주로 회색 이미지를 대상으로 연구되었다.

Guorong(2008)[14]등은 히스토그램에 기반을 한 이진 이미지의 데이터 은닉 방법을 처음으로 시도하였다. Ho(2009)[15]등은 가역(可逆)적인 데이터 은닉을 위한 신규(新規)의 방법을 제안했고 이진 이미지의 화질의 성능을 개선하였다.

본 논문에서는 이진 이미지인 QR 코드를 대상으로 가역적인 데이터 은닉 방법을 제안하고자 한다. QR 코드는 다양한 응용으로 활용하는 코드 체계로 바코드보다 많은 정보를 포함할 수 있기 때문에 더욱 많은 분야에서 활용될 것으로 기대한다. 생성된 QR 코드 이미지에 데이터를 은닉함으로써 QR 코드의 위조 여부를 확인 하는 용도로 의미가 있을 것으로 기대한다.

II. 관련연구

1. CPT 방법

CPT 방법은 데이터 은닉을 위한 블록 기반의 방법이다. 예를 들어 이진 이미지 G가 있다고 할 때 이를 겹치지 않는 블록, $F_i(1 \le i \le N)$, 으로 나눈다. 각 블록에 포함되어 있는 픽셀들은 이진 이미지의 픽셀 값이다. 이 방법에서는 블록의 크기가 $m \times n$인 K와 W행렬이 이용되며 이들은 비밀을 송신하는 측과 수신하는 측이 공유하는 비밀키와 가중치를 의미한다. r은 $m \times n$블록에 은닉 가능한 비트들로서 F 블록에서 적어도 두 개의 픽셀 값을 변경함으로서 정보의 은닉이 가능하다. CPT 방법의 데이터 은닉과정은 다음의 구조와 같다.

CPT (Embedding Method) 알고리즘

Input: Block F of original image G, secret key K, secret weight matrix W, number $r = \lfloor \log_2(mn+1) \rfloor$ of bits to be embedded in a block, secret r-bit stream $b = b_1 b_2 ... b_r$.
Output: Block F' of stego image G'.
Step 1. Compute $T = F \oplus K$, where $\oplus$ is the bit-wise exclusive OR (XOR) operation.
Step 2. Compute SUM(T$\otimes$W) mod 2^r, where $\otimes$ is the bit-wise multiplication operation.
Step 3. From the matrix T, compute for each $w = 1..2^r-1$ the following set:
$S_w = \{(j,k) \mid ([W]_{j,k} = w \wedge [T]_{j,k} = 0) \vee ([W]_{j,k} = 2^r - w \wedge [T]$
// every matrix index (j,k) such that if we complement $[F_i]_{j,k}$, increase the sum by w
Compute $d = b_1 b_2 ... b_r -$ SUM(T$\otimes$W) mod 2^r.

if d=0, then F is not modified;
else {
a) Randomly pick an $h \in \{0, 1, ..., 2^r - 1\}$ such that $S_{hd} \neq 0$ and $S_{-(h-1)d} \neq 0$.
b) Randomly pick a $(j,k) \in S_{hd}$ and complement the bit $[F_i]_{j,k}$;
c) Randomly pick a $(j,k) \in S_{-(h-1)d}$ and complement the bit $[F_i]_{j,k}$;
}

예제 1 (데이터 은닉): F, K와 W가 3×3크기의 블록이고 b_1b_2(은닉할 비트)는 11_2 이라고 가정한다. 이 예제에서 어떻게 2비트 b_1b_2가 F에 은닉될 수 있는지를 설명하고자 한다. 먼저 다음의 수식(그림 1)으로 현재 F로부터 계산한 블록 값은 1이다: SUM ((F′⊕K)⊗W) = 1+2+3+2+1+2=9 mod 22 = 1.

F에 은닉할 비트가 b_1b_2라고 가정하면 F의 어느 픽셀을 교정하면 b_1b_2가 은닉될지 계산할 필요가 있다. 계산은 다음과 같다: d = (b_1b_2- SUM ((F′⊕K)⊗W) = 3-1 = 2. d에 해당하는 것이 $F_{2,2}$이므로 해당하는 픽셀을 0에서 1로 변경함으로써 2가 F에 은닉된다. 만일 d=0 이면, 이미 F의 조건이 만족하므로 F는 변경이 필요 없다. d≠0이면 w의 값을 더하거나 빼는 계산을 통해서 이 조건을 만족시킬 수 있다.

예제 2(데이터 추출): 예제 1에서 F에 은닉한 데이터를 추출하는 과정을 보이고자 한다.

단계 1: 데이터를 은닉할 때와 같이 다음의 간단한 계산으로 은닉된 데이터를 알아낼 수 있다. SUM ((F⊕K)⊗W) = 1+2+3+2+1+2 = 11 mod 22 = 3 즉, 은닉된 데이터는 3이 된다. 그림 2는 CPT 방법에 의해서 실험한 결과로 그림 2(a)는 원본 이미지이고 (b)는 339바이트가 은닉된 스테고 이미지이다.

2. Wu (1998) 등이 제안한 방법

Wu 등의 데이터 은닉 스킴의 동작을 위해서 이진 이미지 B, 비밀키 K, 그리고 메시지 비트들이다. 비밀키 K와 이진이미지 블록 F는 $m \times n$ 크기의 비트맵이다. 블록 F에 데이터 은닉은 F의 몇 개의 비트를 수정함으로써 완성된다. 하나의 블록이 0 < SUM(Fi∧K) < SUM(K)를 만족하면 1비트를 저장할 수 있다.

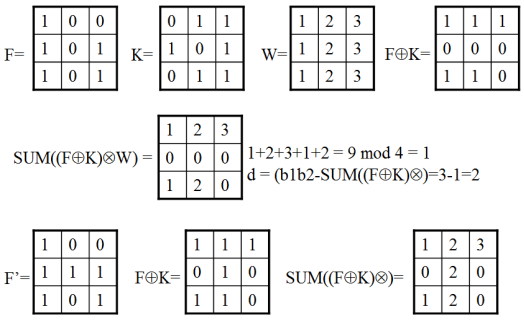

그림 1. 블록 F에 데이터를 은닉하는 과정
Fig. 1. Procedure embedding data in Block F.

0<SUM(Fi∧K)<SUM(K)⇒SUM(Fi′∧K)≡b(mod 2)
그림 3은 Wu 등의 방법을 실험한 결과를 보인 것으로 (a)는 원본이미지이고 (b)는 데이터를 은닉한 스테고 이미지를 보인 것이다.

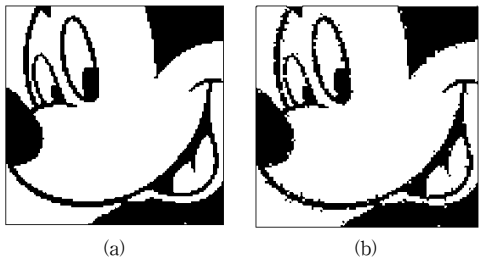

그림 2. (a) 원본 Mickey, (b) CPT 적용 (339 바이트)
Fig. 2. (a) Original Mickey, (b) Apply for CPT (339 byte)

3. QR 코드

QR 코드는 Denson-Wave에서 1994년에 개발된 행렬 심벌의 종류이다. 그림 4는 QR 코드의 기본 구조를 나타낸다. 코드는 버전에 따라 셀의 개수가 다양하며 크기가 21×21 셀인 버전 1부터 버전 40까지 나와 있다. 버전 1일 증가할 때마다 가로세로 4셀씩 늘어나며, 177×177셀 까지 늘어난다. 코드의 버전은 정보량, 데이터 종류, 오류 복원 레벨에 대응하여 설정한다. 코드에 데이터 량이 증가할수록 코드를 구성하는 셀의 개수도 많아지며 코드 크기도 커진다.

위치 검출 패턴은 QR 코드의 사각형 모서리 중 세 곳에 배치되어 코드의 위치를 인식할 수 있게 해주어 고속 판독을 가능하게 해준다. 위치 패턴은 A, B, C의 어느 방향에서든 반드시 흑색 셀과 백색 셀이 교차하며 1:1:3:1:1 비율을 유지한다.

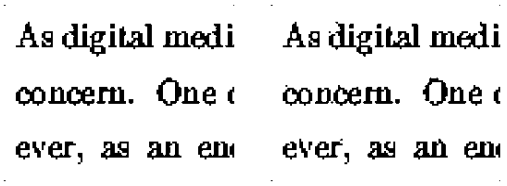

그림 3. (a)원본 문서, (b) 스테고 이미지 (274바이트)
Fig. 3. (a) Original Document, (b) Stego image (274 byte)

코드가 회전되어 있어도 3개위치 검출 패턴의 관계를 통해 회전 각도를 인식하므로 360도 어떤 방향에서도 판독이 가능하다.

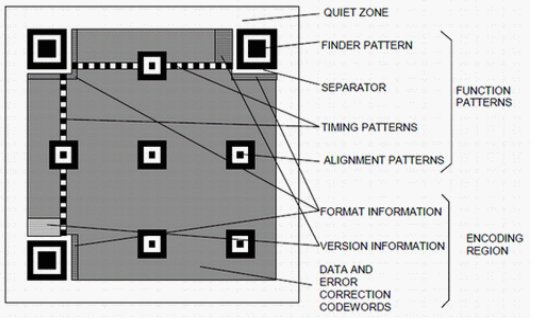

그림 4. QR 코드의 기본 구조
Fig. 4. Basic structure of QR code

정렬(Alignment) 패턴은 QR 코드에서 우측하단 부에 작은 사각형의 패턴으로 코드의 크기가 커질 경우 왜곡을 줄이기 위해 모델 2에 추가된 패턴이다. 타이밍(Timing) 패턴은 위치 검출 패턴 사이 두 곳 백색 셀과 흑색 셀이 교대로 배치된 직선 모양 패턴으로 코드 내 모든 모듈 좌표를 결정하는데 사용한다. 포맷 정보는 오류 정정과 마스크 패턴과 관련된 정보를 담고 있고 코드를 판독할 때 우선적으로 읽히는 부분이다.

QR 코드의 특징은 다음과 같다.

첫 번째, 기존의 바코드는 20자리 정도의 데이터를 포함할 수 있는 반면 QR 코드는 최대 2,953 바이트를 표현할 수 있다.

두 번째, QR 코드는 오류 정정 기능을 갖고 있기 때문에 복원이 가능하고 데이터의 복원은 최대 30%가 복구 가능하다.

Ⅲ. 제안한 방법

본 장에서는 비밀 데이터를 은닉하는 과정과 복원과정을 단계별로 설명하고자 한다. 이진 이미지는 흑과 백의 두 가지 색상을 이용하여 영상을 표현한다. 흑백의 만화나 인쇄된 문자들의 표현에 활용된다. QR 코드 역시 흑백으로 표현이 가능하지만 생성되는 형태는 회색영상이나 컬러 영상의 형태로 생성되고 있다. 이들의 형태를 이진 형태로 변경하더라도 인식하는데 문제가 없기 때문에 생성된 이미지를 이진 이미지로 변경하여 이진 이미지 상태에서 데이터를 은닉한다는 가정 하에 본 논문에서 제안하는 데이터 은닉 방법을 다루고자 한다.

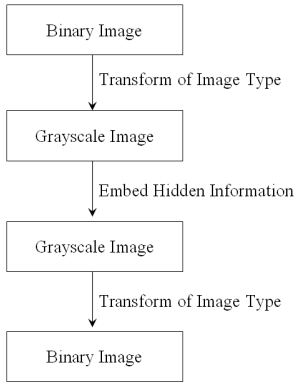

그림 5. 가역적 데이터은닉을 위한 도식
Fig. 5. Flowchart for reversible data hiding

1. 데이터 은닉과정

입력: 이진 이미지 (B), 그리고 비밀 메시지 d_1^n, 비밀 메시지 d_1^n의 길이 $cnt = size(d_1^n)$

출력: 회색 스테고 이미지 (G).

단계 1: 이진 이미지를 회색 이미지로 포맷을 변환 한다. 이미지를 1×2 크기의 블록 단위로 나눈다.

단계 2: 순서대로 1×2 픽셀 블록을 읽어 g_i에 값들을 배정한다. g_i를 수식 (1)을 적용하여 f를 계산 한다(g_i는 픽셀, ω_i는 가중치로 표1의 [1, 3], '•'는 곱셈 연산, mod는 나머지 연산).

$$f = \left[\sum_{i=1}^{2}(g_i \bullet \omega_i)\right] \bmod 7 \qquad (1)$$

단계 3: 수식 (2)를 이용하여 변수 s를 계산한다 (변수 d는 7진 정수를 의미함). $d_i = f$이면 변수 g_i의 값을 변경하지 않아도 d_i가 g_i에 은닉된 것이다. $d_i \neq f$이면 표 1에서 s에 해당하는 숫자(인덱스)를 찾는다. 양수이면 g_i에 더하고 음수이면 g_i에서 각각 빼면 새로운 g_i가 되고 데이터가 은닉된다.

$$s = \begin{cases} d-f & \text{if}(d \geq f) \\ (2^3-1)-|d-f| & \text{if}(d-f<0) \end{cases} \quad (2)$$

단계 4: $d_i = 0$이면 단계 5로 이동하고 그렇지 않으면 $cnt = cnt-1$ 수행 후 단계 2로 이동한다.

단계 5: 작업을 종료하고 완성된 스테고 이미지를 반환한다.

예제 1: 데이터를 은닉하는 과정을 예제를 들어 설명한다. 한 쌍의 픽셀이 $g_i = [128, 130]$ 이고 은닉할 숫자가 4라고 가정한다. 이 경우 수식 (1)과 (2) 그리고 표 1을 사용하여 d진수의 데이터를 g_i에 은닉 가능하다.

표 1. 데이터 은닉을 위한 코드표
Table 1. codebook for data hiding

숫자 \ w_i	1	3
0	0	0
1	1	0
2	-1	1
3	0	1
4	0	-1
5	1	-1
6	-1	0

단계 1: 수식 (1)을 사용해서 다음과 같이 f를 계산한다. f는 0부터 6사이의 정수가 되며, d는 7진 정수로서 $d = f$와 같다면 g_i를 변경 시킬 필요가 없다. f와 d를 일치시키는 과정이 필요하며 만일 일치하지 않으면 단계 2에서 $d = f$가 되도록 한다.

$$f = (128 \times 1 + 130 \times 3) \bmod 7 = 0$$

단계 2: 픽셀 g_i에 은닉할 숫자가 4라고 하면 수식 (2)에 따라서 다음과 같이 s가 계산된다.

$$s = (2^3-1) - |d-f| = 8 - |4-0| = 4$$

s를 표 1에서 찾는다. 즉 [0, -1]이다. 그러므로 첫 번째 픽셀을 아무 변동이 없고 두 번째 픽셀은 -1 감소시킨 129가 된다. 결국 $g_i = [128, 129]$ 된다.

2. 데이터 추출 과정

본 절에서 스테고 이미지로부터 비밀 데이터를 추출하는 과정을 설명하고자 한다.

입력: 회색 스테고 이미지 (G), 비밀 메시지 d_1^n, 비밀 메시지 d_1^n의 길이 $cnt = size(d_1^n)$

출력: 이진 이미지 (B), 비밀 메시지 정수의 집합 δ_i.

단계 1: 이미지를 중첩되지 않게 1×2 크기로 나눈다.

단계 2: 1×2 픽셀 쌍을 읽어 g_i에 배정한다. g_i에 대해서 수식 (1)을 적용하여 f를 계산 한다.

단계 3: f를 다음과 같이 d_i에 배정한다. 즉, $d_i = f$. 이후 d_i를 δ에 누적하고 i를 1증가 시킨다.

단계 4: $d_i = 0$이면 단계 5로 이동하고 그렇지 않으면 $cnt = cnt-1$ 수행 후 단계 2로 이동한다.

단계 5: 작업을 종료하고 회색 이미지를 이진이미지로 포맷 변경을 한다.

Ⅳ. 실험 및 결과

제안한 가역적인 데이터은닉 방법을 평가하기 위해서 MATLAB 7.0을 사용하여 실험하였다. 실험에 사용한 이미지는 8개의 QR 코드로 이진 이미지로 구글(Google) 검색으로 획득(獲得)하였다 (그림 6).

실험에서 중요한 2가지 요소는 스테고 이미지의 화질(해상도)과 스테고 이미지에 저장한 데이터의 은닉 비율이다. 이러한 평가 기준은 데이터 은닉 시스템의 성능을 평가하는데 보편적으로 활용되고 있다. 본 논문에서는 이러한 평가를 보다 객관적으로 증명하기 위해서 PSNR (Peak Signal to Noise Ratio)[15]을 사용한다.

$$PSNR = 10 \times \log_{10}\left(\frac{I_{\max}^2}{MSE}\right) dB \quad (3)$$

즉, 수식(3)에서 MSE는 원본 영상 I와 스테고 영상 I′의 차이 값에 수식(4)를 적용한다.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(|I_{i,j} - I'_{i,j}|)^2 \quad (4)$$

여기서 M은 이미지의 폭이고 N은 높이를 의미한다.수식(3)의 평가의 결과 PSNR의 수치가 클수록 스테고 이미지가 원본 이미지와 유사함을 나타내고, 반대의 경우 스테고 영상이 원본 영상과 차이가 커짐을 의미한다.

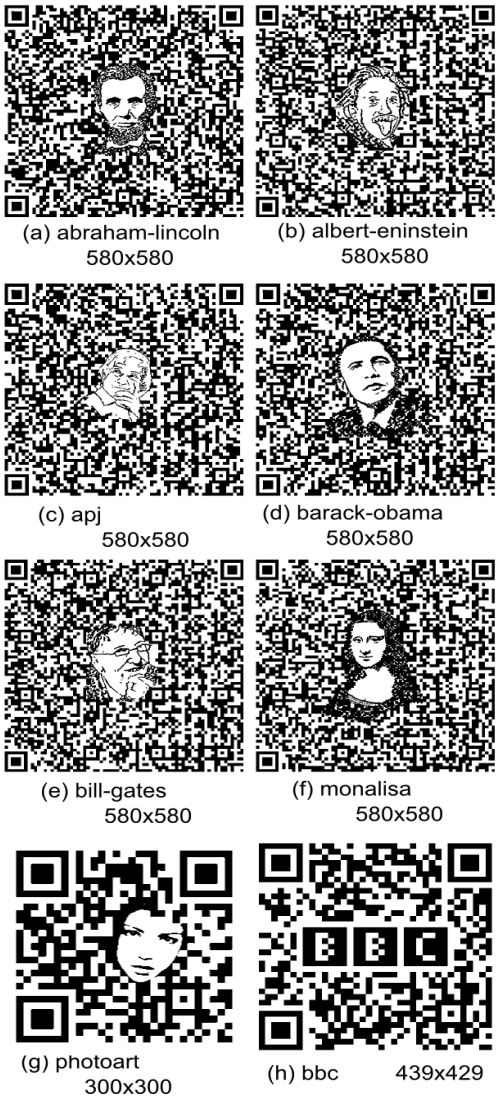

그림 6. 실험에 사용한 원본이미지
Fig. 6. Original image for experiment

일반적으로 PSNR이 30dB 이상인 경우 스테고 이미지의 잡음(noise)를 사람의 시각 시스템으로 탐지하기 어렵다는 것을 나타낸다.

표 2. 제안한 방법의 성능
Table 2. Performance of proposed scheme

Scheme / Images	Our proposed scheme	
	PSNR	P
abraham-lincoln	52.4905	1.5
albert-einstein	52.4770	1.5
apj	52.4880	1.5
barack-obama	52.4831	1.5
bbc	52.4773	1.5
bill-gates	52.4826	1.5
monalisa	52.4709	1.5
photoartz	52.4346	1.5
평균	52.4755	1.5

스테고 이미지에 은닉된 데이터의 비트를 측정하기 위한 단위로 bpp(bits per pixel) 가 사용된다.

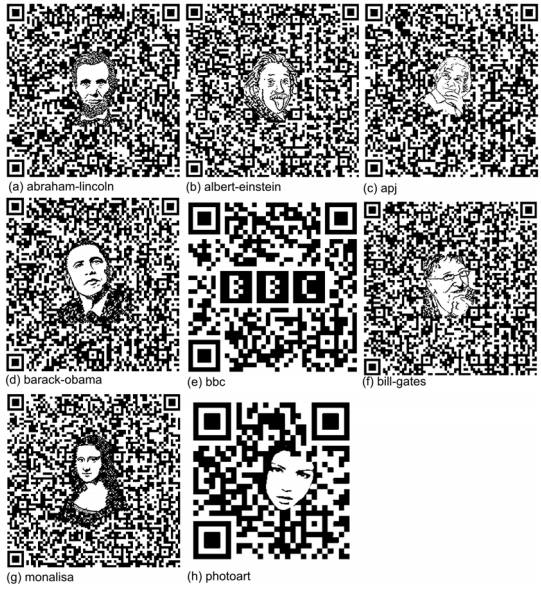

그림 7. 실험결과인 스테고 이미지 (256 회색 이미지)
Fig. 7. Stego image after experiment (256 grayscale image)

bpp는 얼마나 많은 비트들이 은닉되었는지 측정하는 단위이다. 은닉 비율은 수식 (5)을 사용하여 측정이 가능하다.

$$p = \frac{\|S\|}{M \times N}(bpp) \quad (5)$$

수식 (5)에서 $\|S\|$은 은닉된 메시지로 S의 비트수를 의미한다. M와 N은 이미지의 폭과 높이를 나타낸다.

그림 7는 가역적 데이터 은닉 방법을 그림 6을 이용하여 실험한 결과인 스테고 이미지들을 나타낸다.

표 2는 원본 이미지에 데이터를 최대로 은닉한 결과인 PSNR과 은닉비율을 나타낸 것이다. 실험결과 PSNR의 평균은 52.3755로 매우 높은 성능을 보이고 있다. 또한 데이터 은닉역시 1.5로서 매우 높은 데이터를 은닉한 실험결과이다. QR 코드는 그 자체가 필요한 정보를 포함할 수 있는 특징을 갖고 있다. 그런 이유로 다양한 분야에서 활용되고 있다. 경우에 따라서는 QR 코드의 데이터를 수정해서 다른 의미를 나타내는 위조도 가능할 수 있다. 이와 같은 위조를 위해서라도 이미지에 데이터를 은닉해서 QR 코드의 진위 활용에도 사용할 수 있을 것으로 판단한다.

본 실험에서는 그와 같은 실험은 하지 않았으나 차후의 연구에서는 QR 코드의 위조 시에 위조 여부를 판별하는 실험을 추가해서 QR 코드의 위조를 탐지할 수 있는 가역적인 데이터 은닉 방법을 제안하고자 한다.

V. 결 론

본 논문에 우리는 이진 이미지를 위한 QR 코드 기반의 가역적인 데이터 은닉방법을 제안했다. QR 코드는 마케팅, 도서관, 박물관, 학교 (스마트러닝) 등 주소 짧은 정보를 제공하는 활용에 사용한다. QR 코드는 수정을 통해서 다른 의미를 표현할 수 있다. 따라서 민감한 정보를 저장할 경우 위조여부를 확인할 수 있는 방법이 필요하다. 이를 위해서 QR 코드에 데이터를 은닉한 후 나중에 QR 코드에 내포된 정보와 이미지에 은닉된 정보를 비교하여 위조여부를 인증할 수 있는 방법으로 활용할 수 있다. 또, 제안한 방법은 다른 이진 이미지에 데이트를 은닉하여 저작권이나 간단한 주석을 넣을 수 있다. 따라서 본 논문에서 제안한 방법은 향후 다양한 응용에 활용될 것으로 기대한다.

References

[1] C. Kim, "Data Hiding Based on BTC using EMD, The Journal of The Institute of Internet," Broadcasting and Communication (JIIBC) vol.14, no.2, pp.11-16, 2014.

[2] B.H. Lee, "Technique for production and encoding of New dot-type Print Watermark Pattern," Journal of the Korea Academia Industrial cooperation Society, vol.10, no.5, pp.979-984, 2009.

[3] H.J. Kim, C. Kim, Y. Choi, S. Wang, X. Zhang, "Improved modification direction methods," Computers & Mathematics with Applications, vol. 60, no.2, pp.319-325, 2010.

[4] C. Kim, "Data hiding by an improved exploiting modification direction," Multimedia Tools and Applications, vol.69, no.3, pp 569-584, 2014.

[5] N. Provos, and P. Honeyman, "Hide and seek: an introduction to steganography," Security & Privacy, IEEE , vol.1, no.3, pp. 32 - 44, 2003.

[6] C.L. Tsai, H.F. Chiang, K.C. Fan and C.D. Chung, "Reversible data hiding and lossless reconstruction of binary images using pair-wise logical computation mechanism," Pattern Recognition, vol.38, no.11, pp.1993 - 2006, 2005.

[7] S. Falkner, P. Kieseberg, D. E. Simos, C. Traxler, E. Weippl, "E-voting Authentication with QR-codes," Lecture Notes in Computer Science, vol.8533, pp.149-159, 2014.

[8] M.S. Fu, and O.C. Au. "Data Hiding by Smart Pair Toggling for Halftone Images," In IEEE Int. Conf. Acoustics Speech and Signal Processing, vol. 4, pp.2318 - 2321, 2000.

[9] H.Y. Kim, and R.L. de Queiroz, "Alteration locating authentication watermarking for binary images," In in Proc. Int. Workshop Digital watermarking, vol. 1, pp.125 - 136, 2004.

[10] Q. Mei, E.K. Wongand N. Memon, "Data Hiding in Binary Text Documents," In Proceedings of SPIE, vol. 4314, 369 - 375, 2001.

[11] M. Wu, and B. Liu, "Data Hiding in Binary Image for Authentication and Annotation," IEEE Trans. on Multimedia, vol.6, no.4, pp. 528 - 538, 2004.

[12] Y.-C. Tseng, and H.-K Pan, "Secure and Invisible

Data Hiding in 2-Color Images," In INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 1, pp.887 - 896, 2001.

[13] C.-C Chang, C.-S. Tseng and C.-C. Lin "Hiding Data in Binary Images," In Lecture Notes in Computer Science, vol. 3439, pp.438 - 349, 2005.

[14] X. Guorong, Q.S. Yun, C. Peiqi, T. Xuefeng, T. Jianzhongand L. Jue, "Reversible binary image data hiding by run-length histogram modification," In International Conference on Pattern Recognition, vol.1, pp.1 - 4, 2008.

[15] Y.A. HO, Y.K. Chan, H.C. Wu and Y.P. Chu. 2009. "High-capacity reversible data hiding in binary images using pattern substitution," Computer Standards & Interfaces vol.31, pp.787 - 794, 2009.

저자 소개

김 천 식(종신회원)

- 1997년 : 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학석사)
- 2003년 : 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학박사)
- 2010년 ~ 2012년 : 세종대학교 교수
- 2013년 ~ 현재 : 안양대학교 교수
- 2007년 ~ 2009년 : 대한전자공학회 컴퓨터소사이어티 멀티미디어 분과위원장
- 2012년 : TACT 영문 저널 - 위원
- 2012년 : UMAS 워크샵 프로그램 의장
- 2013년 : GPC 2013 프로그램 의장
- 2014년 : FutureTech 2014 프로그램 의장

<주관심분야 : 데이터베이스, 데이터마이닝, Steganography, 영상처리, e-Learning>

※ 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구 사업 지원을 받아 수행된 것임(20120192)