# 다양한 이미지 공격에 강한 R, G, B 비율 분산 기반의 문자 정보 은닉 알고리즘

손일권, 허준
고려대학교
d2estiny@korea.ac.kr, junheo@korea.ac.kr

# R, G, B rate variance based Text Information Hiding scheme Robust against Various Attacks

Il Gwon Sohn, Jun Heo
Korea University

## 요 약

본 논문은 이미지가 갖는 R, G, B 비율의 분산을 이용하여, 공간 영역에서 정보를 은닉하는 알고리즘을 제시한다. 웹 상에서 Jpeg, bmp, gif 등의 포멧을 갖는 이미지를 raw 파일로 변환한 후, R,G,B 비율을 구한다. 그 중 사람의 눈에 가장 둔감한 B 비율 분산을 조작하여 정보를 은닉하는데 이용한다. 또한 오류율을 낮추기 위하여 (15,7)BCH Code 를 사용한다. 제안된 알고리즘이 JPEG(Joint Photographic coding Experts Group) compression, scale(이미지의 크기 변화), Mediancut 과 같은 이미지 변화에 강한 특성과 정보은닉 후에도 화질열화가 발생하지 않는 특성을 실험을 통해 보인다.

## 1. 서론

현재 웹 상에서는 디지털 컨텐츠의 생산, 보급, 재생산이 매우 활발하다. 디지털 컨텐츠는 이전의 여타 컨텐츠와는 달리 복제, 도용이 간단하여 컨텐츠에 대한 보안이 중요하다. 이와 관련 된 문제는 SNS(Social Network Service)의 등장과 함께, 개인 사생활이 담긴 사진과 같은 컨텐츠의 도용, 무단복제, 배포 등이 늘면서 개인의 컨텐츠 보호에 대한 중요성으로도 확대되었다. 또한 웹 상의 게시물은 불특정 다수의 사람들이 접근할 수 있기 때문에, 다수가 접근할 수 있는 게시물을 통해서 특정인에게만 정보를 제공하고자 하는 수요도 생기고 있다. 이에 따라 컨텐츠에 여러 목적을 갖고 정보를 은닉하는 기법이 주목을 받고 있다.

이런 정보 은닉 기법은 다양한 방법이 존재한다. 은닉 영역에 따라서는 공간영역[1],[2], 주파수 영역 은닉 기법[3],[4]으로 나뉜다. 공간 영역 은닉 기법의 경우 정보 은닉의 결과가 시각적으로 바로 보이기 때문에 직관적이며, scale 공격에 강하다는 장점이 있지만 화질 열화가 심하다는 단점이 있다. 주파수 영역 은닉 기법의 경우 특정 변환함수를 이용해 공간 영역을 주파수 영역으로 변환하여 정보를 은닉한다. 주파수 영역에서의 정보 은닉 기법은 화질 열화에 대한 영향이 덜하고 Jpeg compression 과 같은 포멧 변화에 강하다는 장점이 있지만 scale 공격에 약하다는 단점이 있다. 다른 은닉 기법 분류로는 원본 필요 여부에 따른 Blind, Non-blind 기법 분류도 존재한다.

웹 상에서는 각각의 이용자가 어떻게 사용하는지에 따라 사진에 여러 방식의 포멧 변화, 수정이 발생하며, 이로 인해 은닉된 정보가 훼손 되기 쉽다. 또한 SNS 의 경우 서비스 종류에 따라 개별적인 크기, 포멧 변화가 존재한다. 그러므로 웹 상에서 이용되는 이미지에 정보 은닉 기법을 사용할 경우 기본적으로 다양한 포멧, 크기 변화에 강해야 한다.

은닉 기법은 어떤 정보를 대상으로 하는지에 따라서도 성향이 달라진다. 예를 들어 문자 정보의 경우, 문자를 구성하는 한 bit 만 깨져도 정보를 받는 사람이 전혀 다른 문자를 받게 된다. 그렇기 때문에 다른 정보를 대상으로 하는 은닉 기법보다 문자 정보를 대상으로 하는 은닉 기법은 열화에 민감한 성향을 갖는다. 그러므로 문자 정보를 대상으로 하는 은닉 기법은 정보 보호에 더 강인해야 한다. 제안된 알고리즘은 문자 정보를 대상으로, 정보 열화를 최소화하기 위해 (15,7) BCH code 를[5],[6] 사용한다.

본 논문에서 제안하는 정보 은닉 기법은 이미지가 공간 영역에서 나타내는 정보를 이용한다. 은닉 시에 사용되는 정보는 각 Pixel 에서 R, G, B 값이 차지하는 비율의 분산이다. HVS(Human Visual System)에 따라, 사람은 B channel 값 변화에 가장 둔감함으로 R, G 값을 조작하는 것에 비해 B 값을 조작하는 것이 화질열화가 덜하다. 그러므로 정보를 은닉하면서 발생하는 이미지의 화질 열화를 최소화 하기 위해 B channel 값을 이용한다. 또한 이미지를 나눌 때 Block 의 크기가 아닌 총 개수를 고정하고, 그 값을 정보를 숨기는 사람과 받는 사람이 사전에 공유함으로써 Blind 특성을 확보한다. Block 의 크기가 아닌 개수를 고정함으로써 Block 유동적인 크기를 갖게 되고, 이 특성을 통해 scale 공격에도 강인함을 가질 수 있게 된다.

## 2. 정보 은닉 과정

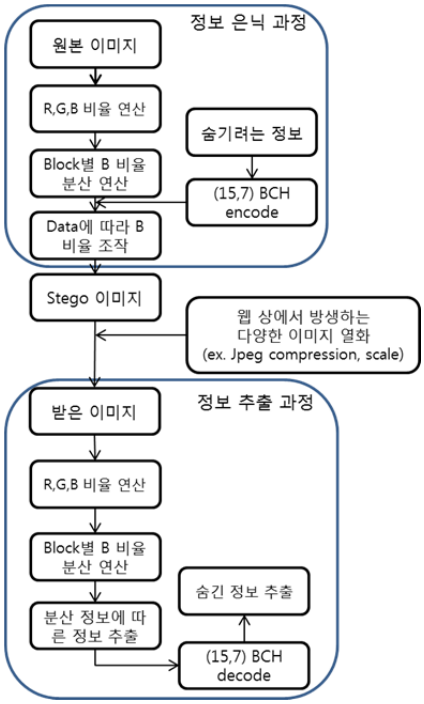


**그림 1 제안된 은닉 기법 순서도**

정보를 은닉, 추출하는 방법은 위의 순서도와 같이 이루어진다. 문자 정보의 경우 ASCII code 를 통해 영문 한 글자 당 8bit 정보로 변환되며, ASCII code 의 MSB 는 모두 '0'이기 때문에 은닉할 정보에서 제외할 수 있다. 따라서 나머지 7 bit 를 (15,7) BCH code 를 사용하여 parity bit 이 추가된 15bit 길이의 codeword 를 만든다. 이 codeword 들을 모아서 bitstream 을 생성한다.

$$w = w_0 w_1 \cdots w_6 w_7 \rightarrow c = c_0 c_1 \cdots c_{13} c_{14} \quad \cdots\cdots (1)$$

w : 숨길 문자의 ASCII code

c : (15,7) BCH 를 통해 생성된 codeword

정보를 보내는 사람과 받는 사람 사이에 약속된 Block 의 총 개수에 따라, Block 의 가로, 세로 (n,m) 크기가 정해진다. 정해진 크기에 맞춰 그림을 나누고, Block 별로 B 비율 $\alpha$ 을 구한다. 다음 과정으로 한 Block 마다 상하 이등분을 하여 두 Sub block 으로 나눈다. 나누어진 상하 Sub block 각각의 B 비율 $\alpha_1, \alpha_2$ 을 구하고, Sub block 내의 각 pixel 마다 B 비율 $\gamma_i$ $(i = 1,2,\cdots n \times m/2)$ 을 구해 그 분산인 $\beta_1, \beta_2$ 를 구한다.

$$\alpha = \sum_i^{n\times m} x_{B_i} / \left(\sum_i^{n\times m} x_{R_i} + \sum_i^{n\times m} x_{G_i} + \sum_i^{n\times m} x_{B_i}\right) \quad \cdots\cdots (2)$$

$$\alpha_k = \left(\sum_i^{n\times m/2} x_{B_i}\right) / \left(\sum_i^{n\times m/2} x_{R_i} + \sum_i^{n\times m/2} x_{G_i} + \sum_i^{n\times m/2} x_{B_i}\right) \quad (k = 1,2)$$

$$\cdots\cdots (3)$$

$$\beta_k = \sum_i^{n\times m/2} (\gamma_i - \alpha_1)^2 / (n \times m/2) \quad \cdots\cdots (4)$$

$$\gamma_i = x_{B_i} / (x_{R_i} + x_{G_i} + x_{B_i}) \quad \cdots\cdots (5)$$

$x_{R_i}, x_{G_i}, x_{B_i}$ : Block 내 각 pixel 의 R, G, B 값

정보에 따라(binary 정보 일 경우 1,0) Sub block 의 B 비율 분산을 조작하여 정보 은닉이 이루어진다. 분산을 조작하는 과정은 다음과 같다. 바꾸려는 비율 $\alpha$ 에 따라 (6)번 식을 이용하여 각 pixel 의 B 값을 조작하면, pixel 의 B 비율이 모두 $\alpha$ 가 된다. 이를 통해 Sub block 내의 모든 B 비율이 평균에 집중되기 때문에 Sub block 의 B 비율 분산이 작아지게 된다. Bitstream 따라 숨기려는 bit 이 0 일 경우 위 Sub block 의 B 비율 분산을 조작하고, 1 일 경우 아래 Sub block 의 분산을 조작하여 숨기려고 하는 정보를 이미지에 숨길 수 있다.

$$x'_B = \alpha \times (x_R + x_G)/(1-\alpha) \quad \cdots\cdots (6)$$

$x'_B$ : pixel 의 수정된 B 값

정보를 추출하는 과정은 다음과 같다. 정보를 받는 쪽에서는 공유하고 있는 Block 총 개수에 따라 받은 이미지를 분할한다. Block 을 상하 이등분을 하여 Sub block 으로 나누고, pixel 별 B 비율을 구하여 분산을 구한다.

위 Sub block 의 분산이 작을 경우 숨긴 정보는 '0', 아래 Sub block 의 분산이 작을 경우 숨긴 정보는 '1', 이다 이 과정을 모두 거치면 정보를 보낸 사람이 은닉한 정보를 추출할 수 있다.

$$if\ \beta_1 < \beta_2 \quad \rightarrow \quad c' = 0$$
$$if\ \beta_1 > \beta_2 \quad \rightarrow \quad c' = 1 \quad \cdots\cdots (7)$$

## 3. 실험 결과

제안된 알고리즘이 여러 공격에 강인함을 확인하기 위해 세 가지 샘플 이미지에 Jpeg compression, Scale, Medan filtering 실험을 하였다. 사용된 샘플 이미지와 실험 결과는 아래 그림 2, 표 1 과 같다.

Sample 1 Sample 2 Sample 3

**그림 2 실험에 사용된 샘플 이미지**

| 이미지 종류 | sample 1 | sample 2 | sample 3 |
|---|---|---|---|
| 원본 크기 | 1600X1200 | 2800X2100 | 2400X1800 |
| 숨긴 bit 수 (BCH encoding 전) | 3500 bit | 8575 bit | 6300 bit |
| Attack | Error rate (%) | | |
| Jpeg QF 100 | 1.91% | 0% | 2.48% |
| Jpeg QF 90 | 2.06% | 0% | 3.06% |
| Jpeg QF 80 | 3.17% | 0% | 4.38% |
| Jpeg QF 70 | 5.29% | 0% | 6.17% |
| scale 0.5 | 0.94 | 0% | 1.49% |
| 변환된 크기 | 800X600 | 1400X1050 | 1200X900 |
| scale 0.25 | 5.11 | 0% | 1.86% |
| 변환된 크기 | 400X300 | 700X525 | 600X450 |
| mediancut 3 | 1.17% | 0% | 5.79% |
| mediancut 5 | 3.20% | 0.12% | 8.57% |
| mediancut 9 | 13.29% | 2.64% | 20.40% |

**표 1 이미지 공격에 대한 실험 결과**

샘플 이미지에 따라 결과의 차이가 있지만 mediancut 9 를 제외하고는 대부분의 실험결과가 5% 이하의 오류율을 보인다. 이 정도의 오류율은 오류 정정 능력이 더 큰 오류정정부호를 사용하여 정보의 안정성을 개선 할 수 있다.

제안된 알고리즘에 따라 정보를 은닉하였을 경우 화질 열화가 발생하지 않는 것을 원본 이미지와 Stego 이미지 (정보가 은닉된 이미지) 사이의 PSNR 을 통해 확인 할 수 있다.

| 이미지 종류 | sample 1 | sample 2 | sample 3 |
|---|---|---|---|
| PSNR (dB) | 54.38 | 50.67 | 51.64 |

**표 2 원본 이미지와 Stego 이미지 사이의 PSNR**

## 4. 결론

본 논문에서는 이미지가 갖는 R, G, B 비율의 분산을 이용하여 정보를 은닉하였다. 제안된 알고리즘은 다양한 공격에 대하여 은닉된 정보를 보호 할 수 있으며, 정보를 은닉한 후에도 화질 열화가 적은 것을 PSNR 을 통해 확인할 수 있었다. Scale, Jpeg compression 에 강인한 특성에 따라 SNS 를 대상으로 사용 가능할 것으로 보이며, 정보 은닉 용량이 높아 문자 정보 이외에, 이미지 워터마킹 분야에서도 활용 가능할 것으로 예상된다.

## Acknowledgement

본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음(NIPA-2011-C1090-1131-0009)

## 참고문헌

1. Zhicheng Ni, Yun Q. Shi, Nirwan Ansari, Wei Su, Qibin Sun, Xiao Lin, "Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication", IEEE transactions on circuits and systems for video technology, Vol.18, No.4, Apr,2008.
2. Masoud Alghoniemy, Ahmed H. Tewfik, "Geometric Invariance in Image Watermarking", IEEE transactions on image processing, Vol.13, No.2, Feb, 2004.
3. Shu-Guo Yang, Chun-Xia Li, Sheng-He Sun, "Text information hiding method based on chaotic map and BCH code in DWT domain of a carrier image", International Conference on Wavelet Analysis and Patter Recognition, Nov. 2007.
4. Chee Sun Won "Boosting robustness against composite attack for quantization index-modulation algorithms", *Journal of Electronic Imaging*, 19, 2, Apr-Jun, 2010.
5. R. C. Bose, C. R. Ray-Chaudhuri, "On a class of error-correcting binary group codes", Information and Control, vol. 3, pp. 68~79, 1960.
6. A. Hocqeunghem, "Codes correcteurs d'erreurs", *Chiffres*, Vol. 2, pp. 147-156, Sep, 1959.