한국정보전자통신기술학회논문지(jkiiect)'19-12 Vol.12 No.6
논문 19-12-06-561 http://dx.doi.org/10.17661/jkiiect.2019.12.6.561

# LSB와 LDR을 기반한 효과적인 혼합 스테가노그래피

지선수*

# An Effective Mixed Steganography Based on LSB and LDR

Seon-Su Ji*

**요 약** 인터넷 공간에서 송신자와 수신자 사이의 신뢰성을 보장하는 안전한 비밀 통신을 위해 무결성과 보안성이 유지되어야 한다. 또한 암호 기법은 외부 공격으로부터 견고성을 유지하기 위한 중요한 요소이다. 이를 위해 암호화 기술과 스테가노그래피 방법이 사용된다. 스테가노그래피는 디지털 미디어에 통계적으로 유의미한 변화를 주지 않으면서 비밀 정보를 숨기는 방법이다. 초성, 중성, 종성으로 이루어지는 한글 자모를 변형한 후 커버 이미지의 RGB 화소 값에 각각 삽입하는 방법을 제안한다. 보안성을 향상시키기 위해 대체되어 변형된 정보를 최하위 영역에 숨기는 새로운 혼합 방법을 사용하였다. 이때 LSB와 LDR 기법을 혼합하여 적용하였다. 제안된 방법의 이미지 품질을 위해 PSNR을 계산하였다. 제안된 방법의 PSNR은 43.225dB이며, 최저수준을 만족하였음을 확인하였다.

**Abstract** In the Internet space, integrity and security must be maintained for secure and confidential communication, which ensures reliability between sender and receiver. Cryptography is an important factor in maintaining robustness against external attacks. For this purpose, encryption and steganography methods are used. Steganography is a method of hiding confidential information without making statistically significant changes to digital media. I propose a method of transforming the Hangul-Jamo consisting of choseong, jungseong and jongseong, and inserting them into RGB pixel values of the cover image. In order to improve security, a new blending method was used to hide the altered information in the lowest region. In this case, a mixture of LSB and LDR techniques was applied. PSNR was calculated for image quality. The PSNR of the proposed method is 43.225dB, which satisfies the lowest level.

**Key Words** : Hangul-jamo, LSB-LDR, MSE, new mixture, RGB image

## 1. 서론

인터넷 환경에서 송신 및 수신되는 디지털 정보는 제3자에게 공개되지 않으면서 안전하게 상대방에게 전달되기를 원한다. 비밀정보를 공유하는 방법에는 암호화와 스테가노그래피를 이용한 은닉 기법이 있다. 암호 알고리즘에 의해 비밀 메시지를 암호화 한 후 스테가노그래피를 이용하여 디지털 매체에 은닉한 후 약속된 상대방에게 송신하는 것이 일반적인 방법이다. 비밀통신에서 정보를 숨기기 위해 사용하는 매개체로 텍스트, 오디오, 이미지, 동영상 등이 있으며, 적용성과 여분(redundancy) 측면에서 이미지가 효과적이며, 실제 적용에서 정보를 은닉하는 매개체의 75%는 이미지를 이용한다[1].

보안성을 강화하기 위해 초성, 중성, 종성으로 이루어지는 한글자모를 분해한 후 암호화한 다음에 비트화와 숫자코드로의 변환 과정 후에 LSB(least significant bit)와 LDR(last digit replace) 알고리즘을 임의적으로 혼합하여 정보를 은닉하는 이미지 스테가노그래피 기법을 제안한다.

논문의 구성은 2장에서 관련된 연구를 소개하

*Department of software, Gangneung Wonju National University
Received October 18, 2019 Revised October 28, 2019 Accepted November 11, 2019

며, 논문에서 제안하고자 하는 방법을 3장에서 보여준다. 적용 및 결과는 4장에서 보이며, 5장에서 결론을 제시한다.

## 2. 관련 연구

디지털 매개체로 가장 많이 사용하는 이미지 스테가노그래피는 공간 영역과 주파수를 변경하여 조작할 수 있는 구성 요소로 변환 주파수 영역으로 분류하여 적용된다. 이러한 이미지는 푸리에 변환, DCT(discrete cosine transform) 및 DWT(discrete wavelet transform )와 같은 기법을 사용하여 디지털 자료로 변환된다. LSB 방법에서 무결성을 위해 해시함수를 사용하며, RGB의 화소 값에 정보를 은닉하기 위한 위치를 선택하기 위해 확률수를 이용한다[2-4]. Soni 등[1]과 Halder 등[2]은 보안성을 향상시키기 위해 스테가노그래피와 암호화를 혼합하는 하이브리드 방법을 제안하였다. Chan 등[3]은 스테고 이미지와 커버 이미지 사이의 최하위 평균제곱오류(WMSE, worst mean square error)는 최하위비트를 이용하는 기법에서 얻은 것의 $\frac{1}{2}$이하가 됨을 제시하였다. 이를 바탕으로 최적의 결과로 최대 PSNR (peak signal to noise ratio)의 기준을 선택할 수 있음을 보였다. PSNR의 최저 기준을 표1과 같이 제시하였다. 표1에서 $k$는 비트화된 정보를 숨기기 위한 최하위비트 수를 나타낸다.

표 1. k값이 1,2,3,4 경우 $PSNR_*$
Table 1. $PSNR_*$ for k=1,2,3,4

| $k$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $PSNR_*$ | 48.13 | 42.11 | 36.09 | 30.07 |

Halder 등[2]과 Meshram 등[4]은 정보를 숨길 때 LSB 방식이 대부분 사용되며, 단순한 기술이기 때문에 외부 공격에 취약하다. 이를 보완하기 위해 해시 기반 LSB 기술 및 커버 이미지에 메시지 존재를 숨기는 XOR feed 방법과 RSA 알고리즘을 사용하는 방법을 각각 제시하였다. 비밀정보를 숨기기 위해 최하위비트의 수를 2 혹은 3으로 설정할 때가 보안성 및 삽입용량 측면에서 가장 효과적임을 확인하였다. Fatnassi 등[5]은 보안계층을 추가하는 DES-SHA 알고리즘을 이용하는 변형된 LSB 기반 이미지 스테가노그래피를 제시하여 효과적인 이미지 품질을 유지할 수 있음을 보였다. Parihar 등[6]은 커버 이미지의 RGB 화소 값의 최하위 숫자에 숨기려는 비밀문자의 숫자로 대체하는 LDR 기법을 제안하였으며, 속도, 삽입용량 및 보안성을 향상시키는 효과적인 방법임을 확인하였다. Yu Wai 등[7]은 LSB 혹은 MSB(most significant bit)를 이용하여 정보를 숨기는 것이 보안에 매우 취약함을 제시하였으며, 새로운 하이브리드(NHB, new hybrid) 방법의 이미지 스테가노그래피를 적용하였으며, NHB 알고리즘의 이미지 품질은 LSB 알고리즘의 스테고 이미지 품질과 유사하다는 것을 확인하였다.

## 3. 제안된 방법

한글 자모는 초성, 중성, 종성자로 분해하여 RGB 화소 값 각각의 최하위 위치에 숨기며, 보안성을 향상시키기 위해 은닉위치, 최하위비트의 크기, 분해된 정보의 위치에 따라 LSB와 LDR을 혼합하는 방법을 적용한다. 즉 LSB만을 적용하는 방법, LDR만을 적용하는 방법, LSB와 LDR을 혼합하는 방법을 각각 적용한다.

표 2. 한글 음절구조에서 이용되는 이진코드
Table 2. Binary code used in Hangul syllables structure

| binary | choseong | jongseong | jungseong |
|---|---|---|---|
| 000 | ㅋ ㅃ | ㄲ ㄽ ㄾ | ㅒ ㅙ |
| 001 | ㅌ ㄲ | ㅍ ㅆ ㄺ | ㅖ ㅝ ㅞ |
| 010 | ㅈ ㅁ ㅊ | ㅆ ㅂ ㅎ | ㅕ ㅐ ㅘ |
| 011 | ㅇ ㄷ ㄹ | null ㄹ ㄱ | ㅏ ㅡ ㅗ |
| 100 | ㄱ ㅅ ㄴ | ㄴ ㅇ ㅁ | ㅣ ㅓ ㅜ |
| 101 | ㅎ ㅂ ㄸ | ㅅ ㅌ ㄵ | ㅔ ㅓ ㅛ |
| 110 | ㅍ ㅆ | ㄷ ㅈ ㅊ | ㅑ ㅠ ㅝ |
| 111 | ㅉ | ㅋ ㄻ ㄼ | ㅞ |

표2는 한글 음절구조에서 최하위비트(LSB) 수가 $k=3$일 때 한글 사용빈도수를 기반[8]으로 초성, 중성, 종성자로 구분되어 대응시킨 이진화된 코드표이다.

표 3. 한글 음절구조에서 이용되는 숫자코드
Table 3. Digit code used in Hangul syllables structure

| digit | choseong | jongseong | jungseong |
|---|---|---|---|
| 0 | ㅋ | ㄺ | ㅐ ㅙ |
| 1 | ㄲ ㅃ | ㄲ ㄵ | ㅖ ㅟ |
| 2 | ㅊ ㅌ | ㅍ ㅄ ㄻ | ㅘ ㅚ |
| 3 | ㅈ ㅁ | ㅆ ㅂ ㅎ | ㅕ ㅒ |
| 4 | ㅇ ㄷ ㄹ | null ㄹ ㄱ | ㅏ ㅡ ㅗ |
| 5 | ㄱ ㅅ ㄴ | ㄴ ㅇ ㅁ | ㅣ ㅓ ㅜ |
| 6 | ㅎ ㅂ | ㅅ ㅌ ㄶ | ㅔ ㅝ |
| 7 | ㄸ ㅍ | ㄷ ㅈ ㅊ | ㅛ ㅑ |
| 8 | ㅆ | ㄻ ㄵ | ㅠ ㅟ |
| 9 | ㅉ | ㅋ ㄽ | ㅞ |

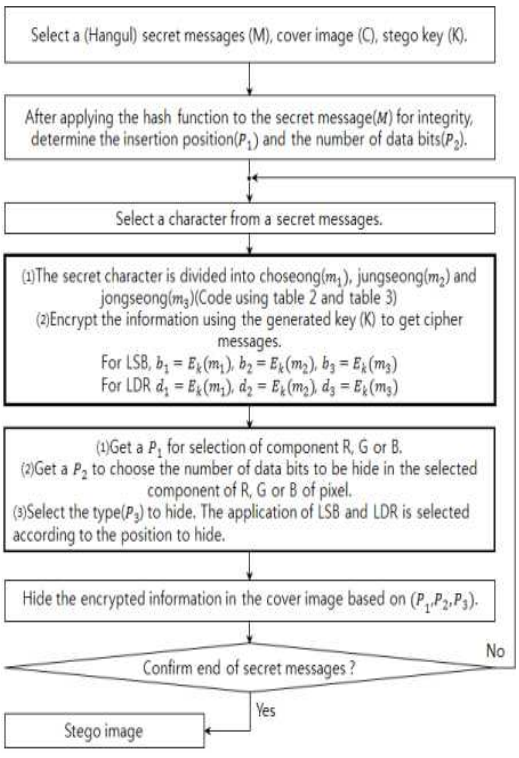


그림 1. LSB, LDR, 혼합(LSB-LDR) 기법을 적용한 작업 흐름도
Fig 1. Work flow using LSB, LDR and mixture(LSB-LDR) techniques

표3은 한글 음절구조에서 한글 사용빈도수를 기반[8]으로 초성, 중성, 종성자로 구분되어 대응시킨 숫자 코드표이다.

그림1에서 LSB, LDR, LSB와 LDR을 기반으로 혼합하는 스테가노그래피의 적용 과정을 보여준다. 그림에서 진하게 표시된 부분이 논문에서 제안된 부분이다.

### 3.1 LDR 기반 스테가노그래피

커버 이미지의 RGB 화소 값의 최하위 숫자에 변형된 비밀문자 정보를 대체한다.

단계1. 커버 이미지로부터 RGB 화소 값의 정보를 획득한다.

단계2. 숨기려는 비밀문자를 초성, 중성, 종성자로 분해하고, 표3을 기반으로 하는 대체값 정보로 변환한 후 각각의 정보를 RGB의 마지막 숫자에 대체한다. 이때 Hash, 암호화 기법을 적용한다.

2.1 비밀정보를 숨기기 위한 시작위치($p_1$)를 설정한다.

2.2 3개의 ($d_1$, $d_2$, $d_3$) 영역으로 변환된 숫자정보를 숨기기 위한 RGB 위치를 각각 설정한다.

2.3 변환된 정보를 은닉한다.

단계3. 비밀 메시지의 모든 정보가 커버 이미지로 은닉될 때까지 단계 2과정을 반복한다.

스테고 이미지로부터 삽입된 비밀문자를 추출한다.

단계1. 스테고 이미지의 화소 값을 계산한 RGB 각각의 정보를 획득한다.

단계2. 은닉시점을 참고하여 최하위 숫자 정보를 추출한 후 Hash, 복호화 기법을 적용한다. RGB 위치정보와 표3을 참고하며, 은닉정보를 조합하여 비밀문자를 구성한다.

단계3. 스테고 메시지로부터 은닉정보의 종료시점까지 단계 2과정을 반복한다.

### 3.2 혼합 기반 스테가노그래피

커버 이미지의 RGB 화소 값의 최하위 비트와 화소 값의 최하위 숫자에 변형된 비밀문자를 각각 삽입한다.

단계1. 커버 이미지의 화소 값을 계산한 RGB 정보를 획득한다.

단계2. 숨기려는 비밀문자를 초성, 중성, 종성자로 분해하고, 표2와 표3을 기반으로 변형된 비트화된 정보와 대체값 숫자 정보를 획득한다. 이때 암호화 기법과 무결성을 위해 Hash를 적용한다.

2.1 비밀정보를 숨기기 위한 시작위치($p_1$)를 설정한다.

2.2 정보를 숨기려는 최하위비트 수를 설정한다. ($k=1,2,3,4$)

2.3 표2를 기반으로 변환된 비트정보 혹은 표3을 기반한 대체값 숫자 정보를 숨기기 위한 RGB 위치를 설정한다.

2.4 각각 3개의 ($b_1$, $b_2$, $b_3$ : $d_1$, $d_2$, $d_3$) 영역으로 변형된 정보와 LSB와 LDR의 은닉 기법을 확률수를 이용하여 임의로 선택하여 비밀정보를 은닉한다. 즉 ①, ②, ③ 위치에 $b_i$ 혹은 $d_i$, $i=1,2,3$, 정보를 임의로 대체시킨다. 예를 들어 R영역에 초성자의 정보($b_1$), G영역에 중성자의 정보($d_2$), B영역에 종성자의 정보($b_3$)가 삽입될 경우 그림2로 표현될 수 있다. $p_2$와 LSB-LDR 경우의 수를 고려하면 은닉방법의 수는 80가지가 된다.

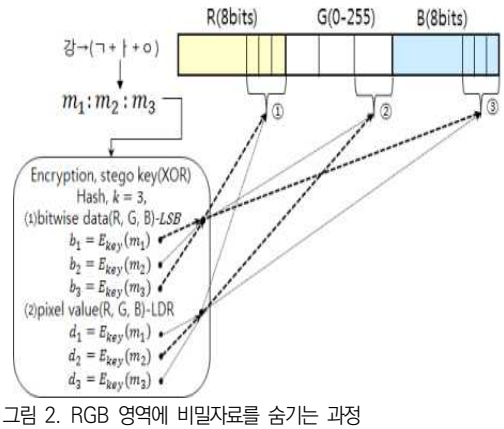

그림 2. RGB 영역에 비밀자료를 숨기는 과정
Fig 2. The hiding process of secrets in the RGB area

단계3. 비밀 메시지의 모든 정보가 커버 이미지로 은닉될 때까지 단계 2과정을 반복한다.

스테고 이미지로부터 삽입된 비밀문자를 추출한다.

단계1. 스테고 이미지의 RGB 화소 값으로부터 필요한 정보를 획득한다.

단계2. 은닉시점을 참고하여 LSB의 정보와 RGB 화소 값에서 최하위 숫자값을 추출한 후 Hash, 복호화 기법을 적용한다. RGB 위치정보와 표2, 표3을 참고하며, 은닉정보를 조합하여 비밀문자를 구성한다.

단계3. 스테고 메시지로부터 은닉정보의 종료시점까지 단계 2과정을 반복한다.

피크신호대 잡음비율은 이미지 화소의 최대값과 두 이미지의 평균 오차 차이를 고려한 비율을 나타내며, 이 비율은 화소 값을 기준으로 이미지를 구별하는 데 도움이 된다. PSNR 값은 (1) 식에 의해 계산된다[9]. 여기에서 $r$은 커버 매체의 행의 수이며, $c$는 행의 수를 의미한다. $Cov(i,j)$와 $Steg(i,j)$는 커버 매체와 스테고 매체의 각각의 화소 값을 의미한다.

$$PSNR=10\cdot\log_{10}\frac{255^2}{MSE} \quad (1)$$

$$MSE=\frac{1}{r\cdot c}\sum_{i=1}^{r-1}\sum_{j=1}^{c-1}(Cov(i,j)-Steg(i,j))^2 \quad (2)$$

커버 이미지와 비밀 메시지가 삽입된 스테고 이미지 사이의 유사점을 비교하기 위한 상관계수는 수식 (3)을 사용하여 계산할 수 있다.

$$Corr=\frac{\sum_{i=1}^{p}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{p}(x_i-\bar{x})^2}\cdot\sqrt{\sum_{i=1}^{p}(y_i-\bar{y})^2}} \quad (3)$$

여기에서 $p$는 이미지의 화소 수를 나타내며, $x_i$는 커버 매체정보를 나타내고, $y_i$는 스테고 매체정보를 나타낸다. $x_i\in X$, $y_i\in Y$이다. $\bar{x}$와 $\bar{y}$는 $X$와 $Y$의 각각의 평균을 의미한다.

## 4. 적용 및 결과

논문에서 사용된 비밀 메시지의 크기는 2, 4, 8, 16 바이트이며, 커버 매체의 크기는 442,174 바이트이다. 3.1, 3.2에서 제안된 방법으로 비밀 메시지를 숨기며, 알고리즘을 구현하는 과정은 J2SE를 이용하였다. 여기에서 비밀 메시지는 "대한민국개인정보철통방어수립하다암호구성"으로 하였다. 보안성을 향상시키기 위해 정보를 숨기기 위한 비트수($k$)를 임의로 설정하여 사용하며, Red, Green, Blue 요소를 선택하였다.

표 4. LSB, LDR, 혼합(LSB-LDR) 기법을 적용한 결과
Table 4. Result of applying LSB, LDR and mixture(LSB-LDR) respectively

| secret messages | Type | MSE | PSNR | Corr. |
|---|---|---|---|---|
| 2 | LDR | 1.326 | 46.903 | 0.9997 |
| | LSB | 1.187 | 47.384 | 0.9997 |
| | Mixture | 1.229 | 47.234 | 0.9997 |
| 4 | LDR | 2.291 | 44.129 | 0.9998 |
| | LSB | 2.125 | 44.857 | 0.9998 |
| | Mixture | 2.458 | 44.224 | 0.9994 |
| 8 | LDR | 4.645 | 41.460 | 0.9996 |
| | LSB | 3.520 | 42.664 | 0.9997 |
| | Mixture | 3.666 | 42.488 | 0.9992 |
| 16 | LDR | 9.448 | 38.376 | 0.9875 |
| | LSB | 6.854 | 39.771 | 0.9938 |
| | Mixture | 8.270 | 38.955 | 0.9981 |

LSB를 사용하기 위해 $k=3$(비트)을 이용하였으며, $key=011$로 하였으며, XOR 연산을 적용하였다. 제시된 그림2를 참고로 하며, 3.2절의 단계2 과정을 기반으로 적용하였다. 이진화된 비트정보와 화소 값의 최하위 숫자를 참고로 LSB와 LDR을 혼합하여 RGB 색상 채널에 대체 삽입하는 방법을 사용하였다.

표4에서 적용형태에 따라 이미지 품질을 확인할 수 있다. $k=3$이고, 16글자를 삽입할 경우 PSNR 값이 LSB(39.771dB), LDR(38.376dB), 혼합 방법일 때 38.955dB으로 PSNR의 최저 기준을 모두 만족하였다. LSB만을 적용할 때 PSNR 값 약간 높게 나타났지만 적용한 방법 모두 유사하였다. 또한 적용한 모든 방법에서 비밀 메시지가 삽입된 전과 후 매체에 대해 화소 값의 유사성이 매우 높게 나타났음을 확인하였다. 커버 매체와 스테고 매체의 중복률은 LSB(16.6%), LDR(8.3%), 혼합 방법을 적용할 경우 10.5%임을 확인하였다. 삽입용량은 LDR 방법을 적용할 때 LSB 및 혼합 방법보다 크다는 것을 확인하였다.

## 5. 결론

비밀 메시지를 완성형 문자의 유니코드를 이용하는 것보다 초성, 중성, 종성으로 분리하여 삽입하면 $k=3$일 경우 LSB(62.5%), LDR(66.6%), 혼합 방법일 때 54.1%의 메모리를 절약할 수 있다. 혼합 알고리즘을 사용할 경우 PSNR은 LSB 및 LDR을 단독으로 이용하는 방법에 비해 1.2% 내외의 차이가 발생하였으며, 상관성은 3가지 방법 모두 유사하였다. 또한 정보를 숨기는 방법의

수가 80가지로 다양한 은닉방법과 Hash 등을 적용하는 혼합 스테가노그래피 기법은 저항성과 기밀성을 높일 수 있음을 확인하였다.

## References


[1] Susmita Soni and Sunita Chaudhary, "A Hybrid Approach of Steganography and Cryptography to improve Data Security", IJLTEMAS, Vol. 3, Issue 4, pp. 163-166, 2014.

[2] R. Halder, S. Sengupta, S. Ghosh and D. Kundu, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", IOSR Journal of Computer Engineering, Vol. 18, Issue 1, pp. 39-43, 2016.

[3] C. K. Chan and L. M. Cheng, "Hiding Data in Images by Simple LSB Substitution", Pattern Recognition, Vol. 37, No. 3, pp. 469-474, 2004.

[4] A. G. Meshram and Rahul Patil, "Secure Secret Key Transfer Using Modified Hash Based LSB method", International Journal of Computer Science and Information Technologies, Vol. 5, No. 6, pp. 7683-7685, 2014.

[5] A. Fatnassi, H. Gharsellaoui and S. Bouamama, "A New Hybrid Steganalysis Based Approach for Embedding Image in Audio and Image Cover Media", IFAC-PapersOnLine Vol. 49, No. 12, pp. 1809-1814, 2016.

[6] V. Parihar, D. Gehlot and A. Choudhary, "A Steganography Implementation based on LSB & LDR Algorithm", 3rd Security and Privacy Symposium, 2015.

[7] Y. Yu Wai and E. Ei Myat, "Comparison of LSB, MSB and New Hybrid(NHB) of Steganography in Digital Image", International Journal of Engineering Trends and Applications, Vol. 5, Issue 4, pp. 16-19, 2018.

[8] H. G. Kim and B. M. Kang, "Frequency Analysis of Hangul Usage", Korea Cultural Research Center, Korea university, 1997.

[9] G. Swain and S. K. Lenka, "Classification of Image Steganography Techniques in Spatial Domain: A Study", International Journal of Computer Science&Engineering Technology, Vol. 5, No. 3, pp. 219-232, 2014.


## 저자약력


**지 선 수(Seon-Su Ji)** **[종신회원]**

- 충남대학교 계산통계학과(학사)
- 중앙대학교 응용통계학과(석사)
- 중앙대학교 응용통계학과(박사)
- 명지대학교 컴퓨터공학과(박사수료)
- (현)강릉원주대학교 소프트웨어학과 교수

〈관심분야〉 정보보안(암호키, 정보은닉), 스테가노그래피