한국정보전자통신기술학회논문지(jkiiect)'21-8, Vol.14 No.4
논문 21-14-04-269 http://dx.doi.org/10.17661/jkiiect.2021.14.4.269

수정된 화소 값 분해를 사용하여 한글 비밀 메시지를 숨기는 방법

지선수*

An Approach to Conceal Hangul Secret Message using Modified Pixel Value Decomposition

Seon-su Ji*

요 약 비밀 통신에서 스테가노그래피는 제3자에게 인지되지 않으면서 비밀 메시지를 송수신한다. 공간 영역 방법에서 비트화 된 정보가 이미지의 분해된 화소 값의 가상 비트 평면에 삽입된다. 즉 비트화 된 비밀 메시지는 커버 매체인 이미지의 최하위 비트(LSB)에 순차적으로 삽입된다. 표준 LSB는 간단하게 적용할 수 있지만 제3자에 의해 쉽게 탐지될 수 있는 단점이 있다. 보안성을 높이기 위해 상위 비트 평면을 이용할 경우 이미지 품질이 떨어질 수 있다. 이 논문에서 lo 번째 비트 평면과 수정된 화소 강도 값 분해에 기반한 이미지 스테가노그래피에 한글 비밀 메시지를 은닉하는 방법을 제시한다. 이때 은닉하려는 한글 메시지를 초성, 중성, 종성으로 분해한 후 혼합과정을 적용하여 기밀성과 견고성을 높인다. 제안된 방법의 효율성을 확인하기 위해 PSNR을 이용하였다. 제시된 기법은 상위 비트 평면에 비밀 메시지를 삽입할 경우 BCD와 Fibonacci를 적용한 방법보다 이미지 품질에서 적은 영향을 받는다는 것을 확인하였다. 기준값과 비교했을 때 제안한 방법의 PSNR 값이 적절한 것을 확인하였다.

Abstract In secret communication, steganography is the sending and receiving of secret messages without being recognized by a third party. In the spatial domain method bitwise information is inserted into the virtual bit plane of the decomposed pixel values of the image. That is, the bitwise secret message is sequentially inserted into the least significant bit(LSB) of the image, which is a cover medium. In terms of application, the LSB is simple, but has a drawback that can be easily detected by a third party. If the upper bit plane is used to increase security, the image quality may deteriorate. In this paper, I present a method for concealing Hangul secret messages in image steganography based on the lo-th bit plane and the decomposition of modified pixel intensity values. After decomposing the Hangeul message to be hidden into choseong, jungseong and jongseong, then a shuffling process is applied to increase confidentiality and robustness. PSNR was used to confirm the efficiency of the proposed method. It was confirmed that the proposed technique has a smaller effect in terms of image quality than the method applying BCD and Fibonacci when inserting a secret message in the upper bit plane. When compared with the reference value, it was confirmed that the PSNR value of the proposed method was appropriate.

Key Words : Bit plane, Decomposition, Hangul secret message, Image steganography, LSB, Lucas

1. 서론

다양한 취약점에 노출되어있는 통신 시스템에서 송수신되는 디지털 정보를 보호하기 위해 암호화와 정보 은닉 기법을 사용한다. 정보를 숨기기 위한 매개체로 디지털 정보로 변환될 수 있는 모든 도구를 사용할 수 있다. 이미지는 중복성이 높기 때문에 대부분의 커버 매체로 이미지를 사용하며, 시각적 품질을 저하시

*Department of Computer Sciences&Engineering, Gangnung-Wonju National University
Received July 17, 2021 Revised July 22, 2021 Accepted August 06, 2021

키지 않고 비밀 정보를 삽입하는 데 효과적으로 사용할 수 있다. 정보 은닉에 사용되는 기법으로 주파수 영역과 공간 영역이 있다. 주파수 영역을 이용하는 방법에서 비밀 메시지 비트는 이미지 화소의 주파수 표현 계수에 삽입된다. 공간 영역을 적용할 때 은닉하려는 정보는 이미지의 화소 값을 분해하여 삽입한다. 즉 비트화 된 비밀 메시지 정보를 최하위 비트(LSB, least significant bit)에 대체하는 접근 방식을 사용한다. 일반적으로 스테가노그래피에서 이미지 화소 값의 가상화된 비트 평면 표현은 이진화 십진 코드(BCD, binary coded decimal)를 사용하며, 표준 LSB를 적용할 경우 제3자에게 은닉된 정보가 쉽게 노출되어 공격받을 수 있는 단점이 있다[1]. 보안성과 견고성을 높이기 위해 상위 비트 평면을 이용할 경우 이미지 품질이 떨어질 수 있다. 이 논문에서 lo번째 가상 비트 평면(bit plane)과 수정된 화소 강도 값 분해(decomposition)에 기반한 이미지 스테가노그래피에 한글 비밀 메시지를 은닉하는 방법을 제시한다.

논문의 2장에서 보안성을 높이기 위한 이미지 화소 값 분해, LSB의 적용기법 등과 관련된 문헌 연구를 제시하였다. 논문에서 제안하고자 하는 방법은 3장에서 기술하였다. 제안된 방법의 효과성을 검증하기 위한 적용 결과를 4장에서 표현하였다. 결론은 5장에서 제시하였다.

2. 관련 연구

보안성과 견고성이 보장되는 이미지 스테가노그래피를 구성하기 위해 개선된 화소 값 분해 기술, 비밀 메시지의 혼합 과정, 확률수에 의해 선택되는 삽입 비트 위치 등이 제안된다. 변형된 화소 값 분해 기법은 BCD의 비트 평면보다 더 많은 비트 평면을 활용할 수 있고, 은닉하려는 메시지 비트를 상위 비트 평면에 대체할 수 있기 때문에 이미지 품질에 미치는 영향을 줄이면서 보안성이 향상될 수 있다.

Abdulla et al.은 이미지 화소 값을 12비트 평면의 Fibonacci 이진 분해에 기반한 삽입기법이 BCD 기반 삽입에 비해 스테고 품질 왜곡이 적고, 높은 비트 평면에 삽입을 가능하게 하여 보안성을 증가시키는 특성이 있다는 것을 확인하였다. 하나 이상의 비트 스트림이 동일한 수를 나타내는 것은 Zeckendorf 정리를 적용하여 해결하므로 삽입용량의 한계성을 개선할 수 있음을 제시하였다[2]. Dey et al.은 15비트 평면으로 분해되는 Prime 분해 구조를 제안하였다. 제안된 분해 기술을 통해 더 높은 비트 평면에 비밀 메시지를 포함할 수 있을 뿐만 아니라 왜곡 없이 은닉 과정을 수행할 수 있음을 보였다. Fibonacci와 BCD 분해에 비해 향상된 스테고 품질을 제시하였으며, 모든 커버 이미지를 삽입에 사용할 수 있는 것은 아니기 때문에 삽입용량 측면에서 단점이 될 수 있다[3]. Aroukatos et al.은 Fibonacci 이진 분해를 참고하고, 삽입에 대한 효율성과 보안성을 높이기 위해 Fibonacci와 Catalan의 구조를 합친 수열을 기반으로 각 화소 값은 15비트 평면으로 분해하여 적용하는 기법을 제안하였다. 삽입 용량과 이미지 품질에서 향상되었음을 보였다[4]. Zaini는 웨이블릿 패킷 분해를 기반하여 LSB2 스테가노그래피를 제안하고, 커버 이미지의 크기를 늘리면 이미지 품질이 개선됨을 보였다[5]. Alharbi는 Lucas 수의 구조를 사용하며, 이미지의 화소 값을 분해하여 이미지의 품질을 저하시키지 않고 상위 비트 평면을 사용할 수 있음을 보였다. 실험 결과 제안된 방법이 흑백과 컬러 이미지 모두에서 표준 LSB 방법보다 PSNR(peak signal to noise ratio) 값이 높음을 보여주었다[6-7]. 삽입용량과 이미지 품질은 상충관계가 존재하며, 화소 값 분해와 비밀 메시지의 변형을 이용하여 보안성과 견고성을 향상시키기 위한 개선된 방법이 요구된다.

3. 제안된 방법

안전한 비밀 통신을 구성하기 위한 비밀 메시지의 분리와 섞음, 암호화 단계, 커버 매체의 새로운 화소 값 분해, lo번째 가상 비트 평면의 선택을 이용하여 한글 메시지를 은닉하는 이미지 스테가노그래피 방법을 제시한다. 한글의 음절 구조는 표 1과 같이 나타낼 수 있다.

표 1. 한글 음절 요소
Table 1. Elements of Hangul syllables

Choseong	ㄱ, ㄲ, ㄴ, ㄷ, ㄸ, ㄹ, ㅁ, ㅂ, ㅃ, ㅅ, ㅆ, ㅇ, ㅈ, ㅉ, ㅊ, ㅋ, ㅌ, ㅍ, ㅎ
Jungseong	ㅏ, ㅐ, ㅑ, ㅒ, ㅓ, ㅔ, ㅕ, ㅖ, ㅗ, ㅘ, ㅙ, ㅚ, ㅛ, ㅜ, ㅝ, ㅞ, ㅟ, ㅠ, ㅡ, ㅢ, ㅣ
Jongseong	null, ㄱ, ㄲ, ㄳ, ㄴ, ㄵ, ㄶ, ㄷ, ㄹ, ㄺ, ㄻ, ㄼ, ㄽ, ㄾ, ㄿ, ㅀ, ㅁ, ㅂ, ㅄ, ㅅ, ㅆ, ㅇ, ㅈ, ㅊ, ㅋ, ㅌ, ㅍ, ㅎ

3.1 제안된 화소 값 분해

제안된 화소 값 분해는 이미지 품질을 저하시키지 않으면서 상위 비트 평면에 비밀 정보를 대체할 수 있는 16개의 숫자 구조를 기반으로 한다. 숫자 집합 S는 (1)식과 같이 구성할 수 있다.

$$\begin{aligned} S &= \{1,2\} \cup \{x \mid x = 2j-3,\ 3 \leqq j \leqq 9, \\ &\quad x = 2j+1,\ 10 \leqq j \leqq 16\} \\ &= \{1,2,3,5,7,9,11,13,15,21,23,25,27, \\ &\quad 29,31,33\} \end{aligned} \tag{1}$$

집합 S를 이용하여 R, G, B의 화소 값 P는 16비트 구조로 분해될 수 있으며, 비트 평면의 가중치는 (2)식으로 계산한다.

$$P = \sum_{i=1}^{16} b_i \cdot w_i \tag{2}$$

여기에서 $b_i = \{0,1\}$이며, 가중치 w_i는 $i = 1, 2$일 때 i값으로 주어지고, $3 \leqq i \leqq 9$일 경우 $2i-3$의 연산 결과로 대응되며, $10 \leqq i \leqq 16$일 때 $2i+1$ 결과로 대응시킨다.

제안된 숫자 구조에서 임의의 화소 값이 하나 이상의 표현으로 구성될 경우에 역변환 속성이 가능하도록 사전식(lexicographic rule)에 의해 상위비트 값으로 설정[6]되도록 한다.

3.2 은닉 과정

삽입을 위해 선택된 커버 이미지의 화소 값은 제안된 분해 방법을 적용하여 16비트 구조로 변환한다. 비밀 메시지를 암호화와 섞음 과정을 한 후 PRNG(pseudo random number generator)에 의해 선택된 가상 비트 평면에 다음과 같은 단계별 과정으로 삽입한다.

1단계:커버 이미지, 비밀(한글) 메시지, 암호화 키(k) 등을 입력한다.
1.1 PRNG에 의해 대체 정보에 사용할 비트 크기($n = 2,3,4$)를 결정한다.
1.2 PRNG를 사용하여 비밀 정보를 삽입할 비트 평면 위치($lo = 1,2,3,4,5,...$)를 확보한다.
2단계:비밀 메시지 글자로부터 각각의 음절 구조로 분리한다.
2.1 초성, 중성, 종성으로 분리한 후 n비트에 대응되는 정보로 대체(초성(m_1), 중성(m_2), 종성(m_3), 그림 1에서 ①~③)한다.
2.2 m_1, m_2, m_3의 특정 위치 비트를 중심으로 암호화와 섞음 과정을 진행한다. (그림 1에서 ④) $3n$비트 정보를 확보한다.
3단계:커버 이미지의 R, G, B 화소 값을 제안된 숫자 구조인 16비트 정보로 변환한다.
4단계:확보된 가상 비트 평면에 비밀 정보를 대체한다.
4.1 삽입 결과가 제안된 숫자 구조에서 유효한 표현일 경우에 대체한다.
5단계:비밀 메시지 정보가 커버 이미지에 포함될 때까지 2단계부터 4단계를 반복한다.
6단계:스테고 이미지를 완성한다. 스테고 이미지와 k 등을 송신한다.

비밀 메시지를 은닉하는 과정은 그림 1과 같이 표현할 수 있다.

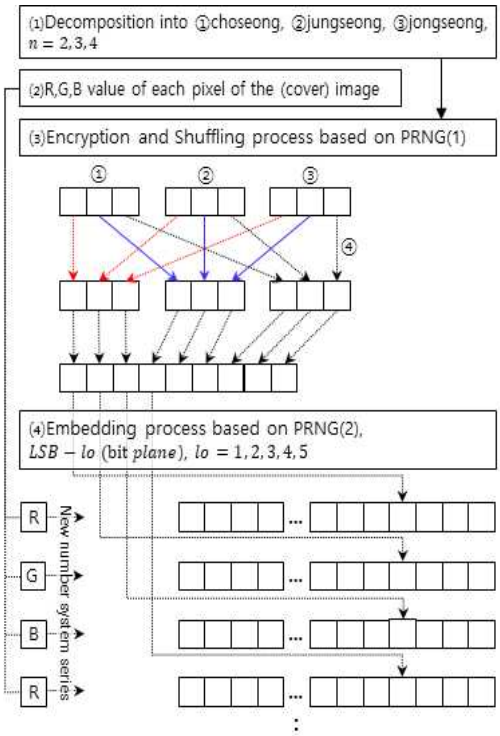

그림 1. 삽입 과정
Fig. 1. Insertion process

3.3 추출 과정

스테고 이미지의 삽입 과정에서 적용된 동일한 방법으로 PRNG를 적용하여 필요한 정보를 획득한다. 스테고 이미지에 은닉된 데이터 비트로부터 비밀 정보를 추출하는 과정은 그림 1의 삽입 과정과 반대로 적용되며, 다음과 같다.

1단계:스테고 이미지, k, PRNG에 의해 n, lo 등을 획득한다.
2단계:스테고 이미지의 은닉 위치에서 비트 정보를 추출한다.
2.1 스테고 이미지의 R, G, B 화소 값으로부터 16비트 구조 정보로 변환한다.
2.2 은닉 비트 평면 위치(lo)에 해당되는 비트 정보를 얻는다.
2.3 n비트 단위로 분류한 후 3개씩 모아서 재섞음과 복호화 과정을 적용한다.
2.4 2.3에서 획득한 n비트에 대응되는 음절을 선택한다.
2.5 $3n$씩 분류한 후 각각의 음절을 결합하여 문자를 재구성한다.
3단계:커버 이미지에 포함된 은닉 정보를 모두 추출할 때까지 2단계를 반복한다.
4단계:비밀 정보를 재구성하여 메시지를 완성한다.

4. 적용 결과

비밀 메시지의 문자를 초성, 중성, 종성으로 분류한 후 n비트로 구성된 대응 정보에 대체하였다. 여기에서 $n=3$으로 설정하였다. 또한 암호화 과정, PRNG에 의한 섞음 과정과 비트 평면 위치(lo)는 1, 2, 4, 5, 6으로 설정하여 각각의 결과를 확인하였다. 이때 사용된 커버 이미지는 lena.gif(227,335 byte)를 사용하였으며, R, G, B 화소 값을 새로운 숫자 구조의 16비트 분해 기법으로 변환하여 사용하였다. 비밀 메시지는 '대한민국청/년꿈을달성/멋있는자산' (30 byte)을 이용하였다. 제안된 방법을 검사하기 위해 MATLAB과 C를 사용하였다.

커버 매체와 스테고 매체 사이의 인식 불가능성(imperceptibility)을 측정하기 위해 PSNR을 사용하며, (3)식에 의해 계산된다. 여기에서 R은 커버 매체의 행의 수이며, C는 열의 수를 나타낸다. f는 커버 이미지, g는 스테고 이미지의 화소 값을 각각 의미한다.

$$PSNR = 20 \cdot \log_{10}\left(\frac{255}{\sqrt{MSE}}\right)\ (dB) \qquad (3)$$

$$MSE = \sum_{i=1}^{R}\sum_{j=1}^{C}\frac{(f_{ij}-g_{ij})^2}{RC} \qquad (4)$$

BCD, Fibonacci, Lucas, 제안된 방법 등을 적용한 후 MSE에 의한 PSNR, 커버와 스테고 매체의 상관성을 각각 계산하였으며, 표 2에서 결과를 제시하였다.

표 2. 은닉 기법의 결과
Table 2. Results of embedding techniques

Applied method	hidden location	PSNR (dB)	Correlation
BCD	1st	52.378	0.9998
	2nd	44.938	0.9994
	4th	32.299	0.9892
	5th	26.469	0.9576
Fibonacci	1st	51.330	0.9998
	2nd	45.310	0.9994
	4th	36.934	0.9963
	5th	32.969	0.9913
	6th	28.752	0.9775
Lucas	1st	45.794	0.9989
	2nd	52.428	0.9997
	4th	39.011	0.9984
	5th	34.534	0.9952
	6th	30.062	0.9831
Proposed	1st	51.031	0.9998
	2nd	45.611	0.9996
	4th	38.239	0.9978
	5th	34.607	0.9956
	6th	32.324	0.9932

제안된 방법이 최소한의 비밀 비트 수를 전달할 수 있기 때문에 PSNR이 높다는 것을 확인할 수 있다. 또한 섞음 과정, PRNG에 의한 lo번째 비트 평면 위치를 선택하여 비밀 정보를 대체함으로 보안성이 향상될 수 있음을 확인하였다. 최하위 비트에 비밀 정보를 삽입할 경우 표준 BCD, Fibonacci, 제안된 방법은 이미지 품질 면에서 비슷한 결과를 보였으며, Lucas 기법을 적용할 경우 PSNR이 낮게 나타남을 확인하였다. 제안된 화소 값 분해 시스템을 기반으로 한 삽입은 비밀 정보가 2번째 혹은 4번째 비트 평면에 삽입될 경우 표준 BCD, Fibonacci 등의 방법보다 PSNR이 1.9% 이상 높게 나타났다. 또한 4번째와 5번째 비트 평면을 이용할 때 Lucas와 비슷하게 나타났음을 확인하였다. 6번째 이상의 비트 평면을 이용할 경우 표준 BCD, Fibonacci, Lucas 방법에 비해 PSNR이 높게 나타남을 확인하였다. 상관계수가 0.9991이며, 커버와 스테고 이미지 간의 유사도가 높음을 확인하였다. 또한 PSNR은 기준치[8]보다 35.82% 높게 나타나는 결과를 보였다.

5. 결론

제안된 방법은 16개의 숫자 구조를 기반으로 R, G, B 화소 값의 새로운 분해 기법을 사용하고, 암호화와 섞음 과정을 포함하여 비밀 자료 숨김 기법을 적용하였다. 확률 수에 의해 상위 비트 평면에 비밀 정보를 삽입하기 때문에 보안성을 보장할 수 있으며, 은닉 위치가 위쪽에 있을 때 이미지 품질 면에서 효과적이며, 표준 BCD, Fibonacci, Lucas를 적용할 때 보다 왜곡을 감지하기 어렵다는 것을 확인하였다.

REFERENCES

[1] P. Das, S. Ray and A. Das, “An Efficient Embedding Technique in Image Steganography using Lucas Sequence”, *Mathematics International Journal of Image, Graphics and Signal Processing 9*, pp. 51-58, 2017.

[2] A. A. Abdulla, H. Sellahewa and S. A. Jassim, “Steganography based on Pixel Intensity Value Decomposition”, *Mobile Multimedia /Image Processing, Security, and Applications*, Volume 9120, 2014.

[3] S. Dey, A. Abraham and S. Sanyal, “An LSB Data Hiding Technique Using Natural Number Decomposition”, *Proc. IIHMSP, IEEE*, pp. 473-476, 2007.

[4] N. Aroukatos, K. Manes, S. Zimeras and F. Georgiakodis, “Techniques in Image Steganography using Famous Number Sequences”, *International Journal of Computers & Technology*, Vol. 11, No. 3, pp. 2321-2329, 2013.

[5] H. G. Zaini, “Image Segmentation to Secure LSB2 Data Steganography”, *Engineering, Technology & Applied Science Research*, Vol.

11, No. 1, pp. 6632-6636, 2021.
[6] F. Alharbi, "Novel Steganography System using Lucas Sequence", *International Journal of Advanced Computer Science and Applications*, Vol. 4, No. 4, pp. 51-78, 2013.
[7] F. Battisti, M. Carli, A. Neri, and K. Egiaziarian, "A Generalized Fibonacci LSB Data Hiding Technique", *Proc. CODEC*, 2006.
[8] Chi-Kwong Chan and L. M. Cheng, "Hiding Data in Images by Simple LSB Substitution", *The Journal of the Pattern the Recognition Society 37*, pp. 469-474, 2004.

저자약력

지 선 수(Seon-Su Ji) **[종신회원]**

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

〈관심분야〉 정보보안(정보은닉), 스테가노그래피