한국정보전자통신기술학회논문지(jkiiect)'18-10, Vol.11 No.5
논문 18-11-05-507 http://dx.doi.org/10.17661/jkiiect.2018.11.5.507

Triple-A 알고리즘과 한글자모를 기반한 안전한 스테가노그래피

지선수*

Secure Steganography Based on Triple-A Algorithm and Hangul-jamo

Seon-Su Ji*

요 약 스테가노그래피는 송신자와 신뢰하는 수신자를 제외하고, 어떤 사람도 비밀 메시지의 존재 자체를 알지 못하도록 숨겨진 메시지를 이용하는 기법이다. 이 논문에서는 24 비트 컬러 이미지를 커버 매체로 적용한다. 그리고 24 비트 컬러 이미지에는 빨강, 녹색 및 파랑에 해당하는 세 가지 구성 요소가 있다. 이 논문에서는 Triple-A 알고리즘을 사용하여 LSB 비트의 수와 사용할 컬러 채널을 임의로 선택하여 비밀 (한글) 메시지를 숨기는 이미지 스테가노그래피 방법을 제안한다. 이 논문은 비밀 문자를 초성, 중성, 종성으로 나누고, 교차, 암호화 및 임의 삽입 위치를 적용하여 견고성과 기밀성을 강화한다. 제안된 방법의 실험결과는 삽입용량과 상관성이 우수하고, 허용 이미지 품질수준임을 보였다. 또한 이미지 품질을 고려할 때 LSB의 크기를 2이하로 하는 것이 효율적임을 확인하였다.

Abstract Steganography is a technique that uses hidden messages to prevent anyone apart from knowing the existence of a secret message, except the sender and trusted recipients. This paper applies 24 bit color image as cover medium. And a 24-bit color image has three components corresponding to red, green and blue. This paper proposes an image steganography method that uses Triple-A algorithm to hide the secret (Hangul) message by arbitrarily selecting the number of LSB bits and the color channel to be used. This paper divides the secret character into the chosung, jungsung and jongsung, and applies crossover, encryption and arbitrary insertion positions to enhance robustness and confidentiality. Experimental results of the proposed method show that insertion capacity and correlation are excellent and acceptable image quality level. Also, considering the image quality, it was confirmed that the size of LSB should be less than 2.

Key Words : Hangul text-Secret Message, LSB technique, RGB channel, Secure Steganography, Triple-A Algorithm

1. 서론

지능정보사회에서 정보의 편리성과 보안성을 기반으로, 디지털 정보가 네트워크를 통해 소통되고 있으며, 사용범위는 확장되고, 고도화되고 있다. 디지털 정보를 송수신할 때 저항성을 높이고 신뢰적인 보안성 확보를 위해 암호화 기법과 정보은닉 기법을 혼합하여 사용하고 있다. 인터넷 공간에서 송수신되는 많은 매체를 이용하여 정보를 은닉할 수 있으며, 스테가노그래피에 일반적으로 사용되는 주요 방법 중 하나는 이미지 픽셀에 메시지를 숨기는 과정을 포함한다. 네트워크 환경에서 디지털 이미지는 가장 널리 사용되며, 삽입용량 및 견고성 측면에서 효과적인 커버 매체이다. 커버 매체에 비밀 메시지를 숨길 경우 저항성, 삽입용량, 비인지성이 상충관계를 이루기 때문에 어느 한 쪽 측면을

*Department of software, Gangneung Wonju National University
Received September 20, 2018 Revised October 02, 2018 Accepted October 18, 2018

집중하여 적용할 수 없다[1-2]. 여기에서는 3가지 요소인 저항성, 삽입용량, 비인지성을 모두 만족할 수 있는 Triple-A 알고리즘을 기반으로 비밀(한글) 메시지를 커버 매체에 삽입하는 방법을 제안한다.

논문의 구성은 2장에서 관련연구를 소개하며, 논문에서 제안하는 방법은 3장에서 제시한다. 4장에서 적용 및 결과를 제시하며, 5장에서 결론을 보여준다.

2. 관련 연구

인터넷 환경에서 이미지 스캔이 손실 압축 방법을 유용하게 사용한다는 사실은 많은 스테가노그래픽 도구를 사용하여 정보 은닉을 시도할 경우 추가 정보를 숨길 수 있는 여분이 충분하다는 것을 의미한다. 이미지 스캔의 속성은 발광, 대비 및 색상을 포함하여 조정될 수 있다. 24 비트 컬러 이미지에는 빨강, 녹색 및 파랑 등의 세 가지 구성 요소가 있다. 각각의 구성 요소는 일반적으로 8 비트를 사용하여 양자화 되며, 이러한 구성 요소로 만들어진 이미지는 24 비트 컬러 이미지로 설명된다[3-4].

Prasad 등은 RGB LSB를 이용하여 비밀 메시지와 이미지 픽셀 값 사이의 동일한 비트에 대한 비교 및 검색을 기반으로 비밀 메시지를 숨기는 방법을 제안하였으며, 일반적인 LSB 기법에 비해 효율성이 좋다는 것을 보였다[5]. Jain 등의 연구에서 RGB LSB 기법은 높은 삽입용량을 유지할 수 있으며, 4-LSB까지 대체함으로 적절한 보안성을 유지할 수 있음을 보였다[6]. Manjula 등은 공간 영역에서 해시 기반 LSB(2-3-3) 기법을 제안하였으며, 기존의 해시 기반 LSB(3-3-2) 삽입 기법에 비해 최대신호잡음비(PSNR, peak signal to noise ratio) 값이 향상되었음을 보여준다. 또한 정규화된 절대오차(NAE, normalized absolute error)를 이용하여 커버 이미지의 일치성을 확인하였다[7].

Rahman 등은 LSB와 RGB의 색상 채널에서 무작위 기법을 사용하는 Triple-A 알고리즘을 적용할 경우 삽입 용량을 증가시킬 수 있음을 보였다[8]. Rahman 등과 Gutub 등은 암호화된 정보를 숨기는데 사용될 RGB 이미지의 구성 요소와 선택된 구성 요소의 최하위 비트 수를 결정하는데 표(표 1, 표 2)를 각각 사용하는 Triple-A 알고리즘을 제시하였다[8-10].

표 1. Seed1($S1$) 난수 사용법
Table 1. Seed1($S1$) random number usage

0	use R.
1	use G.
2	use B.
3	use RG.
4	use RB.
5	use GB.
6	use RGB.

표 1.의 구성 요소를 표시하는데 최대 3 비트가 필요하며, 표 2.의 구성 요소를 나타내는데 최대 2 비트가 필요하다. 비밀 정보를 숨기기 위해 선택된 픽셀마다 이용되는 비트의 수가 증가됨에도 불구하고 삽입용량이 증가됨을 보였다[8-10].

표 2. Seed2($S2$) 난수 사용법
Table 2. Seed2($S2$) random number usage

1	use 1 bit of the component(s)
2	use 2 bit of the component(s)
3	use 3 bit of the component(s)

낮은 색상 값은 픽셀 전체 색상에 작은 영향을 미치기 때문에 픽셀 강도가 낮을수록 더 많은 비트가 변경될 수 있다. 따라서 R(빨강), G(녹색), B(파랑) 사이의 낮은 값의 채널을 선택하여 LSB에 정보를 저장하는 것이 효율적이며, 픽셀의 시각적 품질을 저하시키지 않으며, 최대 4비트를 수용할 수 있음을 보였다[8-10].

3. 제안된 방법

조합형 한글을 은닉할 경우 삽입용량과 저항성 측면에서 효율성을 개선하기 위해 다음의 방법을 고려한다. 비밀 문자를 초성, 중성 종성으로 분리한 후 변환표에 의해 이진화 코드로 재정렬한 후 Triple-A 알고

리즘을 기반으로 비밀(한글) 메시지를 커버 매체에 삽입하는 방법을 제안한다.

표 3. 한글 음절구조에서 이용되는 코드
Table 3. Code used in Hangul syllables structure

Chosung (initial)	Jungsung (medial)	Jongsung (final)	Binary code
ㅇ ㅅ ㅁ ㅆ ㅍ	ㅏ ㅗ ㅔ ㅖ ㅛ ㅓ	null ㄱ ㅅ ㅎ ㄹㄱ ㄹㅂ ㄴㅈ	00
ㄱ ㅎ ㅂ ㅉ ㄸ	ㅣ ㅜ ㅢ ㅐ ㅑ	ㄴ ㅁ ㄴㅎ ㄷ ㄲ ㄹㅌ ㅈ	01
ㄷ ㄹ ㅊ ㅃ ㅋ	ㅡ ㅕ ㅘ ㅔ ㅠ	ㄹ ㅆ ㅂㅅ ㅍ ㄹㅁ ㄹㅍ ㄱㅅ	10
ㅈ ㄴ ㅌ ㄲ	ㅓ ㅒ ㅚ ㅒ ㅟ	ㅇ ㅂ ㅌ ㄹㅎ ㄹㅅ ㅊ ㅋ	11

이때 유전 알고리즘의 교차와 $S2$-LSB를 기반으로 비트 정보를 은닉하는 과정을 적용한다. 표 3.은 한글 사용 빈도수를 기반으로 초성, 중성, 종성 문자를 재배치한 이진화 코드표이다.

3.1 삽입 과정

커버 이미지에 비밀(한글) 메시지를 삽입하기 위해 다음의 과정을 수행한다.

1. 비밀(한글) 메시지(M), 커버 매체(C), 스테고 키(k_1, k_2)를 선택한다.

2. 비밀 메시지 M의 길이를 확인한다.(l) 커버 매체의 형태와 크기를 검사하여 비밀 메시지가 커버 매체에 삽입될 수 있는지를 확인한다.

3. 키(k_1)를 가지고, 유사난수(PRNG, pseudo- random number generator)를 통해 임의의 값을 획득한다. ($0 \leqq S1 \leqq 6,\ 1 \leqq S2 \leqq 3$)

3.1 $S1$으로 커버 매체의 컴포넌트 R, G, B를 결정한다. (표 1)

3.2 $S2$는 픽셀의 R, G, B로 선택된 컴포넌트에 비밀 정보를 숨기기 위해 이용되는 LSB 수를 결정한다. (표 2)

4. 최초의 은닉시점을 확인한다. 암호화된 비밀 메시지 정보를 커버 매체의 최하위 비트($S2$)에 대체한다.

4.1 비밀 메시지로부터 한 문자씩 읽어 들여 초성, 중성, 종성으로 분리한 후 한글문자 변환표(표 3)에 의해 재정렬($m_1{:}m_2{:}m_3$)한다.

4.2 $m_1,\ m_2,\ m_3$ 정보를 교차시킨 후 암호화 한다. 여기에서 $m_2 = m_{21}m_{22}$이다.

$$stg_i = E_{k_2}(m_{22} : m_3 : m_1 : m_{21}),\ i = 1,2,...,l$$

4.3 $S1$을 사용하여 비트화된 정보(stg_i)를 커버 이미지의 오른쪽 최하위 비트에 각각 은닉한다. 이때 $S2$를 참고로 은닉 비트수를 결정한다.

4.4 비밀 메시지의 정보 끝까지 4.1부터 4.3단계를 반복한다.

5. 은닉시점(p_1)과 종점(p_2)의 위치를 확인한다.

6. 스테고 이미지(stg)와 수신자의 공개키를 이용하여 암호화된 키(K) 정보를 전송한다.

$$E_{receiver\_public}(S1, S2, p_1, p_2, k_1, k_2, l) = K$$

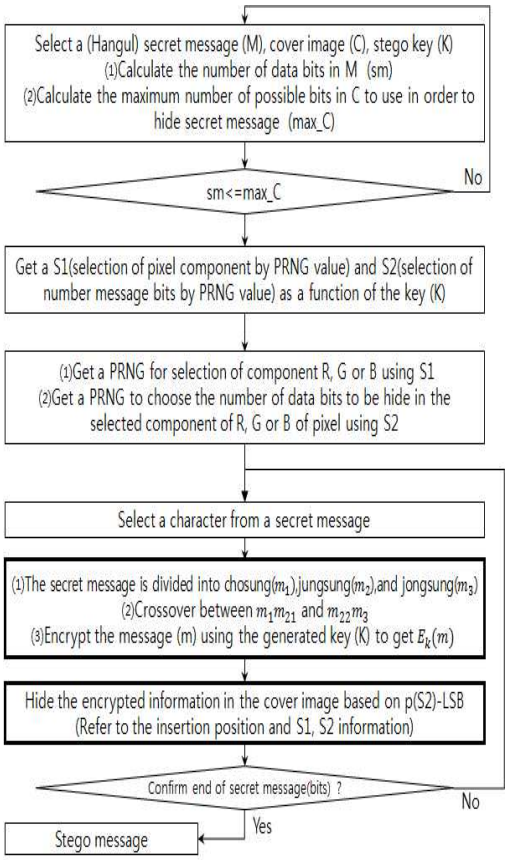


그림 1. Triple-A 알고리즘의 순서도
Fig. 1. Flow chart of Triple-A algorithm

그림 1.에서 Triple-A 알고리즘이 적용되는 과정을 보여주며, Rahman 등과 Gutub 등을 참조하였으며 [8-9], 진하게 표시된 부분은 논문에서 제안한 부분으로 삽입과정의 4단계와 추출과정의 2단계에서 각각 적용된다.

3.2 추출 과정

스테고 이미지와 키를 가지고 비밀 메시지를 추출하기 위해 다음의 과정을 수행한다.

1. 수집된 자료로부터 스테고 이미지(stg)와 수신자의 개인키를 이용하여 복호화된 키(K) 정보를 획득한다.

$$D_{receiver\_private}(K) = \{S1, S2, p_1, p_2, k_1, k_2, l\}$$

2. 스테고 이미지로부터 은닉시점(p_1)를 참고하여, 비밀 메시지를 추출한다.

2.1 $S1$, $S2$ 정보를 참고로 오른쪽 최하위 비트로부터 비트 정보를 추출한다.

2.2 추출된 정보를 정렬하여 k_2를 기반으로 복호화 한 후, 3개로 분리한 다음에 교차시킨 후 $m_1 : m_{21}m_{22} : m_3$의 결과를 재정렬($m_1 : m_2 : m_3$)한다.

2.3 2.2에서 얻은 정보를 m_1, m_2, m_3으로 분리하여 변환표(표 3)를 참고로 글자를 완성한다.

2.4 은닉종점(p_2)까지 2.1부터 2.3까지의 과정을 반복한다.

3. 추출된 글자를 확인한다.

스테고 매체의 이미지 품질을 위해 PSNR 값을 계산하여 비교하였다. 제안된 커버 매체에 대한 스테고 매체의 이미지 품질은 (1)식을 이용하여 평가한다 [9,11].

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

$$MSE = \frac{1}{h} \sum_{i=0}^{h} (\hat{x_i} - x_i)^2 \qquad (2)$$

커버 매체와 비밀 메시지가 삽입된 스테고 매체 사이의 유사성을 비교하기 위한 상관계수는 수식 (3)을 사용하여 계산할 수 있다[12].

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

여기에서 h는 이미지의 픽셀 수를 나타내며, $\hat{x_i}$는 커버 매체정보를 나타내고, x_i는 스테고 매체정보를 나타낸다. $x_i \in X$, $y_i \in Y$이다. $\bar{x}$와 $\bar{y}$는 X와 Y의 각각의 평균을 의미한다.

4. 적용 및 결과

논문에서 사용된 비밀 메시지의 크기는 2, 4, 8, 16 바이트이며, 커버 매체의 크기는 11,772 바이트이다. 3.1에서 제안된 방법으로 비밀 메시지를 은닉하며, 알고리즘을 구현하는 과정은 J2SE와 Matlab을 이용하였다. 여기에서 비밀 메시지는 "한국청년열정순수로승부하다"로 하였으며, $S1$은 6 즉, R, G, B 구성요소 모두를 선택하였다. $k_2 = 010010$(골)로 하였으며, XOR 연산을 이용하였다.

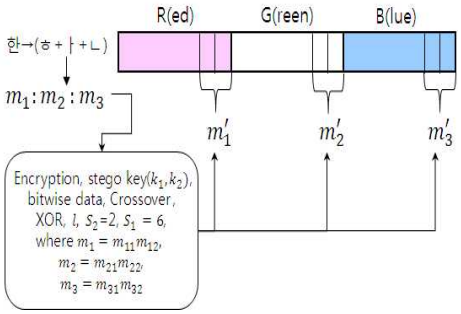
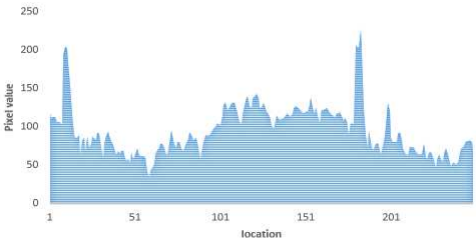
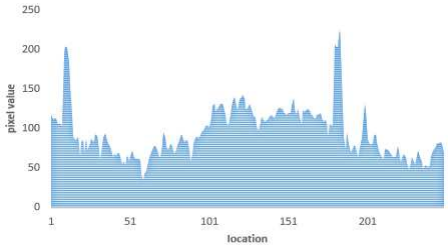


그림 2. RGB 자료에서 LSB 은닉
Fig. 2. LSB hidding in RGB data

그림 2.에서 제시한 그림을 참고로 하여 3.1절의 3과 4과정 기반으로 이진화된 비밀 메시지를 RGB 색상 채널 데이터에 삽입하였다. 그림 3.은 커버 매체(A)와 스테고 매체(B)의 픽셀 값을 그림으로 표시한 부분이며, RGB 요소 각각의 LSB에 비밀 메시지가 삽입되었음에도 픽셀 값의 변화가 미세하게 반영되어 시각적으로 판별하기가 어렵다.



(A) 커버 이미지(빨강)
(A) Cover Image(red)



(B) 스테고 이미지(빨강)
(B) Stego Image(red)

그림 3. 이미지 스테가노그래피의 히스토그램
Fig. 3. Image steganography histogram

$S2$의 값이 각각 1, 2, 3일 때 이미지 품질을 확인하였으며 커버 매체와 스테고 매체의 상관성을 보기 위해 상관계수(corr.)를 구하여 표 4.에 표시하였다. 표 4.에서 $S2$값에 따라 이미지 품질과 삽입 용량을 확인할 수 있다. 또한 비밀메시지를 다르게 하여 32회 반복 작업을 한 결과 $S2$가 1일 때 커버 매체와 스테고 매체의 유사 중복률은 48.6%이며, 2일 때 17.5%, 3일 때 11.1% 내외임을 보였으며, Chan과 Cheng이 제시한 PSNR의 최저 기준[11]과 비교할 경우 유사성 측면에서도 PSNR 값이 50.76으로 PSNR의 최저 기준을 모두 만족하였다. 또한 상관계수가 0.995로 비밀 메시지가 삽입된 전과 후 매체에 대해 픽셀 값의 상관성이 매우 높게 나타났음을 확인하였다. 삽입용량 측면에서 LSB의 크기($S2$)를 크게 하는 것이 유리하지만 이미지 품질을 고려할 때 2이하로 하는 것이 좋음을 확인하였다.

표 4. 커버 이미지에 비밀 메시지를 삽입한 결과
Table 4. The result of inserting a secret message into the cover image

secret messages	$S2$	PSNR	Worst PSNR[11]	Capacity	Corr.
2	1	59.760	48.13	12.5	0.9995
	2	51.396	42.11	25.1	–
	3	51.124	36.09	37.5	–
4	1	50.384	48.13	12.5	0.9996
	2	45.646	42.11	25.1	0.9974
	3	44.483	36.09	37.5	–
8	1	49.635	48.13	12.5	0.9994
	2	45.806	42.11	25.1	0.9971
	3	43.326	36.09	37.5	0.9898
16	1	49.395	48.13	12.5	0.9998
	2	45.881	42.11	25.1	0.9968
	3	42.863	36.09	37.5	0.9897

5. 결론

R, G, B 영역 각각의 최하위 비트에서 1비트 혹은 2비트에 비밀 메시지를 삽입하는 것은 PSNR과 상관성 측면에서 매우 효율적임을 확인하였다. 또한 스테고 매체의 이미지 품질이 PSNR의 최저 수준을 모두 만족함을 확인하였다. Triple-A 알고리즘을 기반으로 비밀(한글) 메시지를 커버 매체에 삽입할 경우 저항성, 삽입용량, 비인지성을 모두 만족하는 결과를 확인하였다. 그리고 교차와 암호화, $S2-LSB$를 적용함으로 저항성과 기밀성 측면에서 한글의 초성, 중성, 종성의 변형된 정보를 은닉하는 효율적인 방법임을 확인하였다.

REFERENCES

[1]S. S. Ji, "A Study of Hangul Text Steganography based on Genetic Algorithm", KIISC, Vol. 21, No. 3, pp. 7-12, 2016.
[2]S. Alam1, S M Zakariya and N. Akhta, "Analysis of Modified Triple-A Steganography Technique using Fisher Yates Algorithm", International Conference on Hybrid Intelligent Systems, pp. 207-212, 2014.
[3]N. Tiwari1 and M. Shandilya, "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth", International Journal of Security and Its Applications, Vol. 4, No. 4, pp. 53-62, 2010.
[4]Shahin Shabnam and K Hemachandran, "LSB based Steganography using Bit masking method on RGB planes", International Journal of Computer Science and Information Technologies, Vol. 7, No. 3, pp. 1169-1173, 2016.
[5]K. L. Prasad and T. Ch. Malleswara Rao, "A Novel Secured RGB LSB Steganography with Enhanced Stego-Image Quality", Int. Journal of Engineering Research and Applications, Vol. 3, Issue 6, pp. 1299-1303, 2013.
[6]Mamta Jain and Pallavi Kumari, "A Survey on Digital Image Steganography using RGB Color Channel", Suresh Gyan Vihar University International Journal of Environment, Science and Technology, Vol. 3, Issue 1, pp. 21-25, 2017.
[7]G. R. Manjula and Ajit Danti, "A Novel Hash based Least Significant Bit(2-3-3) Image Steganography in Spatial Domain", International Journal of Security, Privacy and Trust Management, Vol. 4, No. 1, pp. 11-20, 2015.
[8]Md. M. Rahman, P. K. Mondal, I. Mandal and H Sultana, "Secure RGB Image Steganography Based on Triple-A Algorithm and Pixel Intensity", IJSER, Vol. 7, Issue 3, pp. 864-869, 2016.
[9]A. Gutub, A. Al-Qahtani and A. Tabakh, "Triple-A: Secure RGB Image Steganography Based on Randomization", ACS/IEEE International Conference on Computer Systems and Applications, pp. 400-403, 2009.
[10]Marwa M. Emamm, Abdelmgeid A. Aly and Fatma A. Omara, "A Modified Image Steganography Method based on LSB Technique", International Journal of Computer Applications, Vol. 125, No. 5, pp. 12-17, 2015.
[11]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.
[12]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> 정보보호(암호키, 정보은닉), 스테가노그래피