한국정보전자통신기술학회논문지(jkiiect)'20-6, Vol.13 No.3
논문 20-13-03-177 http://dx.doi.org/10.17661/jkiiect.2020.13.3.177

혼돈 암호화 기법에 기반한 적응된 한글 스테가노그래피

지선수*

Adaptive Hangul Steganography Based on Chaotic Encryption Technique

Seon-Su Ji*

요 약 스테가노그래피는 안전하지 않은 네트워크를 통해 비밀 메시지를 전송하는데 사용하는 매개체로 디지털 이미지를 사용한다. 또한 디지털 이미지에 비밀 메시지를 포함시키는 방법 중에서 많이 사용하는 최하위 비트(LSB)가 있다. 스테가노그래피의 목표는 통신 채널을 통해 스테고 매체를 이용하여 비밀 메시지를 안전하고, 무결하게 전송하는 것이다. 제3자에게 노출의 위험성을 감소시키기 위해 저항성을 향상시키는 방법이 필요하다. 비밀 메시지를 안전하게 숨기기 위해 교차, 암호화, 혼돈, 은닉 단계를 거치는 새로운 알고리즘을 제안한다. 한글 음절을 초성, 중성, 종성으로 분리한 후 비트화된 메시지 정보를 암호화 한다. 로지스틱 맵을 적용한 후에 혼돈 시퀀스의 위치를 가지고 비트화된 정보를 재구성한다. 비밀 메시지는 임의 선택된 RGB 채널에 삽입한다. 적용된 결과의 효율성을 확인하기 위해 PSNR과 SSIM을 이용하였다. 각각 44.392(dB), 0.9884로 확인하였다.

Abstract Steganography uses digital images as a medium for sending secret messages over insecure networks. There is also a least significant bit(LSB) that is a popular method of embedding secret messages in digital images. The goal of steganography is to securely and flawlessly transmit secret messages using stego media over a communication channel. There is a need for a method to improve resistance to reduce the risk of exposure to third parties. To safely hide secret messages, I propose new algorithms that go through crossing, encryption, chaos and concealment steps. After separating Hangul syllables into choseong, jungseong and jongseong, the bitwised message information is encrypted. After applying the logistic map, bitwised information is reconstructed using the position of the chaotic sequence. The secret message is inserted into the randomly selected RGB channel. PSNR and SSIM were used to confirm the effectiveness of the applied results. It was confirmed as 44.392(dB) and 0.9884, respectively

Key Words : Chaotic Encryption, Crossover, Logistic map, RGB channel, SSIM, Steganography

1. 서론

네트워크 통신에서 암호화된 메시지임에도 반복되어 노출되면 제3자에 의해 원래의 메시지로 복원될 가능성이 높게 될 것이다. 저항성을 향상시키기 위해 암호화되고, 무결성이 훼손되지 않아야 할 필요가 있는 스테가노그래피는 커버 매체에 메시지를 숨기는 측면에서 암호화 기법과는 차이가 있다. 즉 스테가노그래피는 안전하지 않은 네트워크를 통해 비밀 메시지를 커버 매체에 은닉하여 전송하는 데 중요한 역할을 한다. 커버 매체 중에서 비밀 메시지를 전달하기 위한 매개체로 이미지가 대부분 사용된다. 스테가노그래피에서 사용되는 최하위 비트(LSB, least significant

*Department of Computer Science and Engineering, Gangneung Wonju National University
Received April 24, 2020 Revised May 20, 2020 Accepted May 26, 2020

bit) 대체 기법은 공간 영역에서 널리 사용되는 방법으로 외부 공격에 취약하고, 견고성이 떨어지지만 계산 복잡도가 낮고, 삽입 용량이 높기 때문에 폭넓게 사용되는 방법이다. 이 논문에서는 커버 매체의 무결성을 손상시키지 않으면서 저항성을 향상시키기 위해 교차(crossover)와 혼동(chaotic) 함수를 적용하여 애매 모호성이 증가된 형태의 비밀 메시지를 은닉하는 효과적인 스테가노그래피 방법을 제시한다.

논문의 2장에서 관련된 연구내용을 정리하며, 논문에서 보여주고자 하는 제안된 방법은 3장에서 보여준다. 적용방법은 4장에서 보이며, 5장에서 결론을 제시한다.

2. 관련 연구

스테가노그래피는 암호화 기법과는 다르게 메시지를 보호하기 위해 오디오, 이미지, 텍스트 매체의 특정 비트에 비밀 메시지를 대체한다. Yu 등은 혼돈 함수와 유전 알고리즘을 이용하여 비밀 메시지를 섞은 후 은닉과 추출하는 방법을 제안하였다. 제안한 혼돈 섞기 알고리즘은 스테고 이미지의 최대 신호 대 잡음 비(PSNR, peak signal to noise ratio)가 미세하게 향상되었음을 보였으며, 흑백 이미지보다는 RGB 이미지에서 향상된 이미지 품질과 높은 보안성이 유지됨을 보여 주었다[1]. Ranawat 등과 Prasad 등은 혼돈의 임의성을 주기위해 비밀 데이터의 위치를 로지스틱 맵에서 획득한 무작위 순서대로 섞는 스크램블링(scrambling) 기법을 적용하는 비선형 동적 시스템을 제안하였다. 초기 값과 모수 값에 민감하며, 암호화 알고리즘의 성능을 측정하기 위해 키 감도(key sensitivity)와 상관 계수(correlation coefficient) 사용을 제안하였다[2-3]. Talee 등은 암호화 방법 중 하나를 선택하여 비밀 메시지를 암호화 한 다음 결과를 혼돈 함수를 사용하여 RGB 채널의 특정 비트영역에 은닉한다. 최대 신호 대 잡음 비와 상관 계수 측정을 사용하여 제안된 방법의 효과를 그림으로 설명하고, 데이터의 다단계 보안을 달성할 수 있음을 보였다[4]. 일반적으로 사용되는 이미지 스테가노그래피 알고리즘은 최하위 비트(LSB, least significant bit) 기반 삽입, PRLSB(pseudo random LSB) 기반 삽입, 수량화(quantification) 기반 삽입 등이 있다. Tutuncu 등과 Elabady 등은 LSB 기반 알고리즘과 관련된 공격에 대한 저항성을 강화시키기 위해 수식(1), (2)와 같은 혼돈 함수를 이용하였다[5-6].

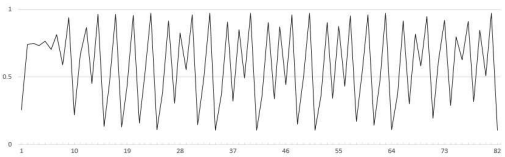

그림 1. 식(1)에서 $\alpha = 3.8889,\ x_o = 0.2555$인 로지스틱 맵 혼돈 계열의 무작위성

Fig. 1. Randomness of logistic map chaotic series $\alpha = 3.8889,\ x_o = 0.2555$ in eq(1).

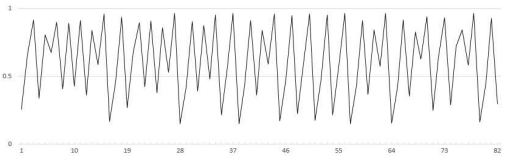

그림 2. 식(2)에서 $\alpha = 1.5333\ x_o = 0.2555$인 로지스틱 맵 혼돈 계열의 무작위성

Fig. 2. Randomness of logistic map chaotic series $\alpha = 1.5333\ x_o = 0.2555$ in eq(2).

RGB 채널 중 하나에서만 비밀 메시지를 숨기고, 혼돈 이론을 기반으로 하는 로지스틱 맵을 사용하여 은닉 채널을 무작위로 선택한다. 다른 채널의 LSB를 왜곡하여 제3자에게 스테고 이미지 내에서 비밀 메시지를 추출하는데 어려움을 겪도록 하였다. 제안된 알고리즘이 LSB와 PRLSB 보다 PSNR과 삽입 용량 모두 낮았지만 견고성을 높일 수 있음을 제시하였다[5-7].

$$x_n = \alpha \cdot x_{n-1}(1 - x_{n-1}),\ 3.5699 \leqq \alpha \leqq 4,$$
$$0 < x_i < 1,\ i = 0,1,2,\ldots n, n+1,\ldots \quad (1)$$

$$x_n = \alpha \cdot x_{n-1}(1-x_{n-1})(2+x_{n-1}),$$
$$1.411 \leqq \alpha < 1.599,\ 0 < x_i < 1$$
$$i = 0,1,2,\ldots n,\ n+1,\ldots \qquad (2)$$

혼돈 함수에서 초기 값(x_o)과 모수 값(α)이 중요하며, 작은 변화에 출력 값의 편차가 높게 나타난다. 모수 값이 $3.5699 \leqq \alpha \leqq 4$와 $1.411 \leqq \alpha < 1.599$ 각각의 범위에 있고, $x_i \in [0, 1]$ 일 때 혼란스러운 시퀀스를 생성하는데 (1)식과 (2)식 모두 적절함을 보인다. 예를 들어 $\alpha = 3.8889$와 $x_o = 0.2555$를 수식(1)에 적용하여 1차원 로지스틱 맵에 의해 생성된 혼돈 그래프는 그림1에서 보여 준다. $\alpha = 1.5333$와 $x_o = 0.2555$를 수식(2)에 적용하여 1차원 로지스틱 맵에 의해 생성된 혼돈 그래프를 그림2에서 보여준다.

은닉하려는 비밀 메시지가 한글일 때 혼돈 함수와 유전 알고리즘을 이용하여 비트 순서의 위치를 섞는 방법과 암호화를 적용하여 스테가노그래피의 저항성을 향상시킬 수 있는 새로운 방법이 필요하다.

3. 제안된 방법

초성, 중성, 종성자로 분해된 한글자모의 비트화된 정보를 RGB 픽셀 값 각각의 최하위 비트에 대체하여 은닉한다. 저항성을 향상시키기 위해 교차 및 암호화, 혼돈 함수에 의한 시퀀스 위치를 이용한 비트화 된 정보의 재구성, RGB 채널의 임의 선택에 따라 재구성된 정보를 대체하는 방법을 적용한다.

표1은 한글 음절에서 초성, 중성, 종성자로 분해한 후 Kim 등이 제시한 각각의 사용 빈도수를 기초[8]로 대응시킨 코드표이다.

표 1. 한글 음절에서 대체되는 코드값
Table 1. Digit code replaced in Hangul syllables

	choseong	jungseong	jongseong
0	ㅋ	ㅟ	ㅍ
1	ㄸ	ㅑ	ㄷ
2	ㅌ	ㅚ	ㅎ ㅀ
3	ㅂ	ㅢ	ㄴㅎ ㄹㅌ
4	ㄴ	ㅐ	ㅂ ㄱㅅ
5	ㅎ	ㅜ	ㅁ ㄴㅈ
6	ㅅ	ㅓ ㅞ	ㅇ ㅃ
7	ㄱ ㅉ	ㅣ ㅖ	ㄴ ㄺ
8	ㅇ ㅆ	ㅏ ㅠ	null ㅊ
9	ㄷ ㅃ	ㅡ ㅒ	ㄹ ㄲ
10	ㅈ	ㅗ ㅕ	ㄱ ㄻ
11	ㄹ	ㅕ	ㅆ ㅀ
12	ㅁ	ㅔ	ㅅ ㅋ
13	ㅊ	ㅘ	ㅂㅅ ㄹㅍ
14	ㅍ	ㅛ	ㅌ
15	ㄲ	ㅝ	ㅈ

3.1 삽입 과정

그림3을 참고로 하여 비밀 메시지를 커버 매체에 은닉한다. 즉 커버 매체인 이미지의 선택된 RGB 픽셀 값의 최하위 영역(k)에 변형된 비밀 문자의 비트화 된 정보를 대체한다.

단계1. 커버 매체로부터 RGB 픽셀 값과 비밀(한글) 메시지의 정보를 획득한다.

단계2. 숨기려는 문자(m)를 선택한다. 한글 음절 구조에서 초성, 중성, 종성으로 분해한 후 표1을 참고하여 각각의 정보로 대체한다.

$$m_1 = b_{11}b_{12}b_{13}b_{14}$$
$$m_2 = b_{21}b_{22}b_{23}b_{24}$$
$$m_3 = b_{31}b_{32}b_{33}b_{34}$$

단계3. 비트화된 정보를 교차시킨다.

$$d_1 = b_{23}b_{24}b_{31}b_{32}b_{33}b_{34}$$
$$d_2 = b_{11}b_{12}b_{13}b_{14}b_{21}b_{22}$$

단계4. Chaotic box를 이용하여 정보를 암호화

한 후 혼돈 시퀀스에 따라 비트화된 정보를 재배열 한다.

단계5. 임의 선택된 RGB 최하위 영역에 재구성된 정보를 은닉한다.

5.1 RGB 채널 중에서 확률수를 이용하여 두 채널을 선택한다.

5.2 선택된 채널의 최하위 영역($k=1,2,3$)에 비트화 된 정보를 대체 은닉한다. 선택되지 않은 영역에는 가짜 정보를 대체한다.

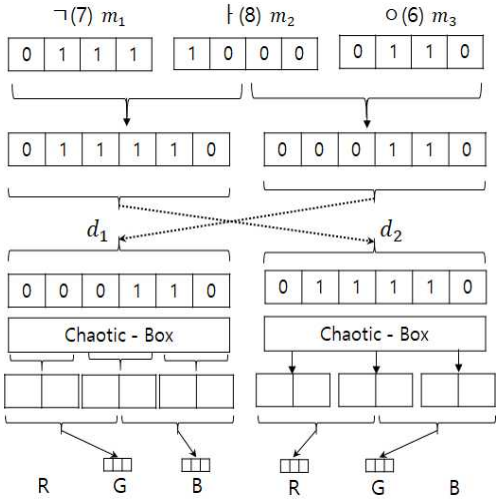

그림 3. 내림차순에 의한 요소배열과 변위과정

Fig. 3. Element arrangement and displacement process in descending order

단계6. 비밀 메시지의 끝 지점까지 단계2부터 단계5 과정을 반복한다.

단계7. 스테고 이미지와 키 값을 송신한다.

그림3은 교차, 혼돈 요소의 임의성에 따라 벡터 위치가 변경되고, RGB 픽셀 값 일부에만 비밀 메시지 정보를 삽입하는 과정을 보여준다. 그림4는 암호화와 비밀 정보의 섞음 과정을 보여준다.

3.2 혼돈을 기반한 메시지 섞음 과정

정보를 섞기 전에 암호화 과정을 적용한다. 로지스틱 맵을 사용하고, chaotic-box에 의해 혼돈 시퀀스를 가지고 비트화된 정보를 재구성한다.

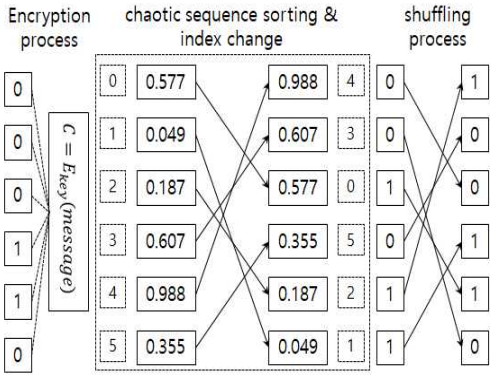

그림 4. 혼돈스러운 암호화와 픽셀 섞음 과정

Fig. 4. Chaotic encryption and pixel shuffling process

단계1. 교차된 정보는 암호 알고리즘을 적용하여 암호화 한다.

단계2. 로지스틱 맵을 이용하여 6개의 요소로 이루어지는 벡터를 생성한다. 생성된 요소 자료를 정렬한다.

단계3. 정렬된 요소의 시퀀스 위치(I)를 생성한다.

단계4. I의 위치에 따라 메시지 비트를 섞는다. I의 위치에 해당되는 메시지(m)의 비트 정보를 생성한다.

3.3 추출 과정

스테고 매체와 키로 부터 은닉된 메시지를 추출한다.

단계1. 획득된 스테고 이미지와 키를 사용하여 RGB 정보로부터 필요한 정보를 수집한다.

단계2. 획득된 RGB 정보를 참고하여 LSB의 최하위 비트 값을 추출한다.

2.1 Chaotic box, 복호화, 교차를 단계별로 적용한다.

2.2 단계 2.1에서 획득한 정보와 표1을 참고하여 비트 정보를 조합한 후 문자를 재구성한다.

단계3. 스테고 매체로부터 숨겨진 정보의 종료시점까지 단계 2과정을 반복한다.

이미지 픽셀의 최대값과 두 이미지 사이의 평균 편차를 고려한 비율인 PSNR 값은 (3)식에 의해 계산된다[1,4-5,7].

$$PSNR = 10 \cdot \log_{10}\frac{255^2}{MSE}(dB) \quad (3)$$

$$MSE = \frac{1}{M \cdot N}\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j) - S(i,j))^2 \quad (4)$$

여기에서 M은 커버 이미지의 행의 수이며, N는 열의 수를 의미한다. $C(i,j)$와 $S(i,j)$는 커버 이미지와 스테고 이미지의 각각의 픽셀 값을 의미한다.

이미지 품질을 측정하기 위해 사용되는 구조 유사성(SSIM, structural similarity) 지수는 3가지 이미지 손실 요소인 휘도 왜곡(luminance distortion), 대비 왜곡(contrast distortion), 상관 손실(loss of correlation)을 조합하여 구성하며, (5)식에 의해 계산된다[9].

$$SSIM(c,s) = [ld(c,s))]^{\alpha} \cdot [cd(c,s)]^{\beta} \cdot [lc(c,s)]^{\gamma}$$
$$SSIM(c,s) \in [0,1] \quad (5)$$

여기에서 두 매체 간 평균 휘도의 근접도를 측정하는 휘도 비교 수식은 $ld(c,s) = \frac{2\mu_c \cdot \mu_s + c_1}{\mu_c^2 + \mu_s^2 + c_1}$이며, u_c는 커버 매체(c)의 평균, u_s는 스테고 매체(s)의 평균을 나타낸다. 두 매체 간 대비의 근접성을 측정하는 대비 비교 함수는 $cd(c,s) = \frac{2\sigma_c \cdot \sigma_s + c_2}{\sigma_c^2 + \sigma_s^2 + c_2}$이며, σ_c는 커버 매체의 표준편차, σ_s는 스테고 매체의 표준편차를 나타낸다. 두 매체 간 상관 계수를 측정하는 구조 비교 수식은 $lc(c,s) = \frac{\sigma_{cs} + c_3}{\sigma_c \cdot \sigma_s + c_3}$를 사용한다. 이때 σ_{cs}는 커버 매체와 스테고 매체 사이의 공분산을 나타낸다.

4. 적용 및 결과

논문에서 사용된 비밀 메시지는 '꿈과도전을멈추지않는대한민국청년'(32바이트) 이다. 커버 매체의 크기는 26,277 바이트이다. 유전알고리즘의 교차를 이용하며, 암호화 할 때 스트림 암호를 사용하며, 키는 '001101'을 이용하였다. 로지스틱 맵의 1차 다항식인 (1)식에서 $\alpha = 3.9998$, $x_o = 0.2555$를 각각 사용하였다. 로지스틱 맵에서 6개의 요소로 이루어지는 벡터를 이용하므로 숨기려는 비밀 문자의 1/2 정보씩 처리하였다. 예를 들어 비밀 문자가 '강'일 경우 m_1은 7(0111), m_2는 8(1000), m_3는 6(0110)이며, d_1은 000110, d_2는 011110이다. 여기에서 비트화된 비밀 문자는 내림차순으로 정렬된 시퀀스의 위치를 참고로 섞기 작업을 하였다. 이때 생성된 $I = 430521$을 사용하였다.

RGB 채널 중에서 확률수에 의해 선택된 2개는 실제 메시지 정보가 최하위 비트에 대체되며, 나머지 1개에는 가짜 정보를 은닉하였다. 여기에서 가짜 정보는 계산의 편의성을 위해 현 위치에서 커버 매체의 해당 비트 정보를 사용한다. 구조 유사성 지수를 계산할 때 지수의 기본 값인 가중치 $\alpha = 1$, $\beta = 1$, $\gamma = 1$과 안정화 지수인 $c_1 = (0.01L)^2$, $c_2 = (0.03L)^2$, $c_3 = c_2/2$를 각각 적용하였다. 또한 픽셀 값의 생성 범위는 $L = (2^{bits\ per\ pixel} - 1)$를 이용하여 계산하였다.

표 2. 제안된 방법의 결과
Table 2. Results of the proposed method

Type	Secret data (byte)	MSE	PSNR > 35.0	SSIM > 0.97
Image A	16	2.823	43.623	0.9787
	32	2.569	44.032	0.9889
Image B	16	2.211	44.686	0.9775
	32	2.397	44.334	0.9879
Image C	16	1.962	45.203	0.9884
	32	2.317	44.480	0.9786

제안된 방법을 적용한 결과는 표2에서 보여준다. 커버 매체에 따라 약간의 차이가 있지만 MSE는 2.380, PSNR 값이 44.392(dB)이다. 구조 유사성(SSIM) 지수는 0.9884, 상관 계수가 0.9989로 각각 나타났으며, 커버 매체와 스테고 매체 사이의 차이를 감지하기가 매우 어렵다는 것을 확인하였다. 또한 삽입 전과 후 동일 정보가 대체되는 것은 11.7%임을 확인하였다.

5. 결론

저항성이 부족한 LSB 은닉 방법을 개선하기 위해 교차 및 암호화, 로지스틱 맵에 의한 정보의 재구성 방법, 즉 혼돈 요소의 임의성에 따라 메시지 정보 위치가 섞여지고, 확률 수에 의해 RGB 채널을 선택하여 일부 채널의 최하위 비트에 가짜 정보를 입력하는 과정을 적용하였다. 삽입 용량과 PSNR은 낮아지지만 보안성은 증가되며, 구조 유사성 지수는 1.0에 근접함을 확인하였다. 즉 지각 투명성을 유지하면서 교차와 로지스틱 맵의 임의성이 적용된 제안된 방법이 다단계 보안성을 이룰 수 있음을 확인하였다.

REFERENCES

[1] L. Yu, Y. Zhao, R. Ni and T. Li, "Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm", EURASIP Journal on Advances in Signal Processing, Vol. 2010, pp. 1-6, 2010.

[2] P. Ranawat and S. Khandelwal, "Chaos Image Encryption using Transposition and Pixel Shuffling", International Journal of Innovations in Engineering and Technology, Vol. 4, Issue 4, pp. 259-265, 2014.

[3] M. Prasad and K. L. Sudha, "Chaos Image Encryption using Pixel shuffling", CCSEA 2011, CS & IT 02, pp. 169-179, 2011.

[4] G. T. Talee, M. J. Jelmeran and S. J. Mohammed, "A New Approach for Chaotic Encrypted Data Hiding in Color Image", International Journal of Computer Applications, Vol. 86, No. 8, pp. 23-26, January 2014.

[5] K. Tutuncu and B. Demirci, "Adaptive LSB Steganography Based on Chaos Theory and Random Distortion", Advances in Electrical and Computer Engineering, Vol. 18, No. 3, pp. 15-22, 2018.

[6] N. F. Elabady, H. M. Abdalkader, M. I. Moussa and S. F. Sabbeh, "Image Encryption Based on New One-Dimensional Chaotic Map", International Conference on Engineering and Technology(ICET), 2014.

[7] S. Rajendran and M. Doraipandian, "Chaotic Map Based Random Image Steganography using LSB Technique", International Journal of Network Security, Vol. 19, No. 4, pp. 593-598, July 2017.

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

[9] Y. A. Y. Al-Najjar and D. C. Soong, "Comparison of Image Quality Assessment : PSNR, HVS, SSIM, UIQI", International Journal of Scientific & Engineering Research, Vol. 3, Issue 8, pp. 1-5, 2012.

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(암호키, 정보은닉), 스테가노그래피