한국정보전자통신기술학회논문지(jkiiect)'21-4, Vol.14 No.2
논문 21-14-02-109 http://dx.doi.org/10.17661/jkiiect.2021.14.2.109

XNOR-XOR과 피보나치 기법을 이용하여 이미지에서 한글 비밀 메시지를 은닉하는 방법

지선수*

An Approach of Hiding Hangul Secret Message in Image using XNOR-XOR and Fibonacci Technique

Seon-su Ji*

요 약 네트워크 환경에서 다양한 사용자가 증가하면서 송수신되는 민감한 비밀 정보를 공격자로부터 보호하는 것은 어렵다. 이미지에 비트화된 비밀 자료를 LSB 기법으로 은닉하는 것은 공격에 매우 취약할 수 있다. 이를 해결하기 위해 암호화와 정보은닉이 결합하는 하이브리드 방법이 활용된다. 이용자가 비밀 메시지를 안전하게 보호하고, 비밀 통신을 구현하기 위한 효과적인 방법이 요구되고 있다. 즉, 이미지 품질을 보장하기 위해 보안성과 인식 불가능성을 향상시키기 위한 새로운 접근법이 필요하다. 이 논문에서 MSB와 LSB를 기반하여 커버 이미지에 한글 메시지를 은닉하는 LSB 스테가노그래피 기법을 제안한다. 이때 한글을 초성, 중성, 종성으로 분리한 후, 비밀 자료는 선택된 MSB에 따라 Exclusive-OR 혹은 Exclusive-NOR 연산을 적용한다. 또한 계산된 비밀 자료는 피보나치 기법에 의해 변환된 커버 이미지의 LSB n개 비트에 은닉한다. 적용된 결과의 효율성을 확인하기 위해 PSNR을 이용하였다. 허용되는 결과로서 적합한 41.517(dB)가 확인되었다.

Abstract As various users increase in a network environment, it is difficult to protect sensitive and confidential information transmitted and received from attackers. Concealing bitwise secret data in an image using the LSB technique can be very vulnerable to attack. To solve this problem, a hybrid method that combines encryption and information hiding is used. Therefore, an effective method for users to securely protect secret messages and implement secret communication is required. A new approach is needed to improve security and imperceptibility to ensure image quality. In this paper, I propose an LSB steganography technique that hides Hangul messages in a cover image based on MSB and LSB. At this time, after separating Hangul into chosung, jungsung and jongsung, the secret message is applied with Exclusive-OR or Exclusive-NOR operation depending on the selected MSB. In addition, the calculated secret data is hidden in the LSB n bits of the cover image converted by Fibonacci technique. PSNR was used to confirm the effectiveness of the applied results. It was confirmed 41.517(dB) which is suitable as an acceptable result.

Key Words : Fibonacci algorithm, Image steganography, LSB(least significant bit), MSB(most significant bit), XNOR, XOR

1. 서론

다양한 방식으로 정보를 저장하고, 안전하지 않은 통신 채널을 통해 데이터가 교환되므로 제3자의 위협으로부터 데이터의 안전성을 보호해야 한다. 네트워크를 통해 침입자가 접근하는 것을 차단하며, 통신의 신

*Department of Computer Sciences&Engineering, Gangnung-Wonju National University
Received March 31, 2021 Revised April 01, 2021 Accepted April 16, 2021

뢰성을 보장하기 위해 비밀 자료를 전송할 때 무결성과 안정성을 향상시키는 새로운 방법의 개발이 필요하다. 일반적으로 비밀 자료에 혼돈과 확산을 적용하여 권한 없는 접근자가 읽을 수 없도록 하는 암호화와 자료를 매체에 은닉하는 스테가노그래피를 결합한 하이브리드 방법을 사용한다. 인터넷에서 전송되는 모든 도구를 매체로 사용할 수 있으며, 매체로서 텍스트, 이미지, 오디오 등이 사용된다. LSB(least significant bit)는 공간 영역을 고려할 때 스테가노그래피 이미지에 폭넓게 사용되는 기술이다. 적용의 단순성과 은닉된 정보의 추출을 위한 예측 가능성이 존재함에도 불구하고, 높은 품질의 스테고 이미지가 생성될 수 있으므로 많이 사용되고 있으며, LSB를 기반으로 하는 새로운 방법이 계속 연구되어지고 있다. 스테가노그래피는 보안성(security)과 견고성(robustness), 삽입 용량(capacity), 인식 불가능성(imperceptibility)을 가지고 비밀 자료가 삽입된 스테고 매체의 효율성을 측정하고 관리한다. 특히, 인식 불가능성은 최대 신호 대 잡음비(peak signal to noise ratio, PSNR)를 사용하여 스테고 매체의 품질을 추정한다[1-3].

이 논문에서 최상위 비트(MSB)와 최하위 비트(LSB)를 기반하여 커버 이미지에 한글 메시지를 은닉하는 LSB 스테가노그래피 기법을 제안한다. 이때 한글을 초성, 중성, 종성으로 분리한 후, 비트화된 자료에서 선택된 MSB에 따라 Exclusive-OR(XOR) 혹은 Exclusive-NOR(XNOR) 연산을 수행한다. 또한 계산된 비트 자료는 피보나치 기법에 의해 변환된 커버 이미지의 RGB 픽셀값 각각의 최하위 n개 비트에 은닉한다. 또한 LSB의 취약점을 보완하기위해 주기적으로 쓰레기 자료를 삽입하는 과정을 추가한다.

논문의 구성은 다음과 같다. 2장에서 보안성 강화를 위한 XNOR, 선택적 채널 선택, LSB의 적용 기법 등과 관련된 연구를 기술하였다. 논문에서 보여주고자 하는 방법은 3장에서 제시한다. 4장에서 제안된 방법을 기반으로 실효성을 검증하기 위한 적용과정과 결과를 보였다. 5장에서 결론을 제시하였다.

2. 관련연구

일반적으로 보안성은 삽입 방법에 기반을 두며, 공격자가 커버 매체에서 비밀 데이터를 추출하는 것이 어렵다고 판단하는 경우 안전한 것으로 처리된다.

Almayyahi 등은 삽입 단계를 진행하기 전에 Huffman 알고리즘으로 비밀 메시지를 압축한 후 비밀 메시지를 포함할 픽셀을 선택할 때 Exclusive-NOR 연산과 피보나치 알고리즘을 적용하는 방법을 제안하였다. 높은 보안성을 보였으며, 커버 이미지의 각 픽셀에 대해 녹색 채널만 이용할 경우, 녹색 또는 파란색 채널을 사용하고 빨간색 채널은 노이즈 자료를 삽입할 경우, 피보나치 알고리즘과 XNOR 연산을 결합하여 추출 과정을 복잡화시킬 경우에도 삽입 능력을 향상시킬 수 있음을 보였다[4-5].

Joshi 등은 LSB의 2비트와 XOR 연산의 장점만을 결합하는 방법을 제시하였다. 커버 이미지의 8번째 비트는 비밀 자료의 첫 번째 비트와 XOR 처리되고, 7번째 비트는 비밀 자료의 두 번째 비트와 XOR 처리되는 방식이다. 계산된 최종 결과의 비트는 이미지 픽셀의 마지막 두 LSB에 삽입된다. 이러한 접근 방식은 높은 삽입 용량과 보안성을 이룰 수 있음을 확인하였다[6].

Abbood 등은 암호화 키와 XNOR 연산을 사용하여 비밀 정보를 암호화한 후 LSB 알고리즘을 사용하여 암호화된 정보를 RGB 이미지에 숨기는 방법을 제안하였다. 은닉 방법은 각 픽셀에 대해 RGB 3개의 색채 채널을 추출하고, 암호화 메시지의 비트를 숨길 채널을 지정하는 방법에 따라 다르게 적용함으로 효율성과 보안성을 향상시킬 수 있음을 보였다[7].

Ahmed 등은 MSB 정보로부터 획득된 비밀키 사용하여 메시지를 암호화한 후 이진화 표현을 사용하는 이중 XOR 연산을 수행하고, 암호화된 비트 스트림을 LSB 기술을 사용하여 커버 이미지에 은닉하는 방법을 제안하였다. 제안된 방법의 품질을 확인하기 위해 MSE, PSNR, 엔트로피 및 히스토그램 분포 등을 이용하여 측정하였으며, 제안된

방법이 허용 가능한 유용한 결과임을 보였다[8]. Setyono 등은 LSB 스테가노그래피 기술과 교차(transposition) XOR 암호화 기술을 결합하여 삽입되는 메시지의 보안성을 강화하는 새로운 접근법을 제안하였다. 제안된 암호화 프로세스가 메시지 보안을 향상시키면서 인식 불가능성과 삽입용량을 유지할 수 있음을 증명하였다[9].

여기에서는 표준 LSB 이미지 기법을 활용하여 인식 불가능성을 향상시킴으로 이미지 품질을 보장하며, 스테고 이미지의 보안 수준을 높이는 것에 초점을 둔다.

3. 제안된 방법

비밀 통신을 수행하기 위한 비밀 자료의 분리 및 변환, 암호화 단계, 자료의 삽입 단계, 스테고 매체로부터 은닉된 자료의 추출 단계로 구성한다.

표 1. 한글 음절
Table 1. Hangul syllable

chosung (consonant)	ㄱ ㄲ ㄴ ㄷ ㄸ ㄹ ㅁ ㅂ ㅃ ㅅ ㅆ ㅇ ㅈ ㅉ ㅊ ㅋ ㅌ ㅍ ㅎ (19)
jungsung (vowel)	ㅏ ㅐ ㅑ ㅒ ㅓ ㅔ ㅕ ㅖ ㅗ ㅘ ㅙ ㅚ ㅛ ㅜ ㅝ ㅞ ㅟ ㅠ ㅡ ㅢ ㅣ (21)
jongsung (support)	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 (27)

숨기려는 한글 비밀 자료에서 각각의 글자로부터 초성(m_1), 중성(m_2), 종성(m_3)으로 분해한 후 음절의 사용 빈도수에 따라 n비트로 이루어진 이진화된 정보로 대체한다. 여기에서는 $n=3$비트를 사용하였다. 표 1과 같이 한글의 음절 구조를 분류할 수 있다.

3.1 비밀 자료의 은닉 과정

분해된 비밀 자료를 은닉하기 위해 커버 이미지를 선택한다. 선택된 이미지의 RGB 채널로부터 픽셀값과 비트화된 이진 자료를 획득한다. 그림1을 참고로 하여 비밀 메시지를 커버 매체인 이미지의 선택된 RGB 화소 값의 최하위 공간에 변형된 비트화 된 정보를 대체한다.

비밀 자료를 은닉하는 단계별 과정은 다음과 같다.

단계1 : 숨기려는 비밀(한글) 자료, 커버 이미지를 준비하고, 은닉 시작 위치와 종료 위치, 픽셀 선택값(k)을 설정한다. $p=0$으로 초기화한다.

단계2 : 커버 이미지로부터 RGB 값을 획득한 후 각각의 이진화 정보를 구성한다.

2.1 비밀 자료로부터 한 글자씩 선택한 후 초성, 중성, 종성자를 분해한 후 n(3)비트로 구성된 이진화 정보로 대체한다. ($m_1,\ m_2,\ m_3$)

2.2 R, G, B 값을 기반으로 이진화 자료를 생성한다.

2.3 R, G, B 값을 기반으로 피보나치 수열을 이용한 변환된 이진화 자료를 생성한다. (그림1의 ①) ($R^{'},\ G^{'},\ B^{'}$)

단계3 : 임의(k)로 R, G, B 채널을 선택한 후 선택된 픽셀값의 MSB를 확인한다. (그림1의 ②)

3.1 MSB가 0이면 R, G, B 채널의 이진화 값 왼쪽 n비트와 ($m_1,\ m_2,\ m_3$)를 각각 XNOR 연산한다. (그림1의 ③)

3.2 MSB가 1이면 R, G, B 채널의 이진화 값 왼쪽 n비트와 ($m_1,\ m_2,\ m_3$)를 각각 XOR 연산한다. (그림1의 ③)

3.3 $p=p+1$을 계산한다.

단계4 : 단계3의 계산된 정보를 2.3에서 구성된 최하위 n비트에 대체한다.

4.1 $p<5$이면 변형된 비밀 자료($m_1^{'},\ m_2^{'},\ m_3^{'}$)를 2.3에서 구성된 비트화된 자료의 최하위 n(3)비트에 대체한다. (그림1의 ④)

4.2 $p\geq 5$이면 비밀 정보 대신에 쓰레기 정보를 2.3에서 생성된 비트화된 자료의 최하위 n(3)비트에 대체한다. (그림1의 ④) $p=0$으로 초기화한 후 다음 단계로 간다.

단계5 : 비밀 자료의 종료 위치까지 단계3부터 단계4를 반복한다.

단계6 : 스테고 이미지를 획득한다.

비밀 자료를 은닉하는 단계별 과정은 그림1과 같이 나타낼 수 있다.

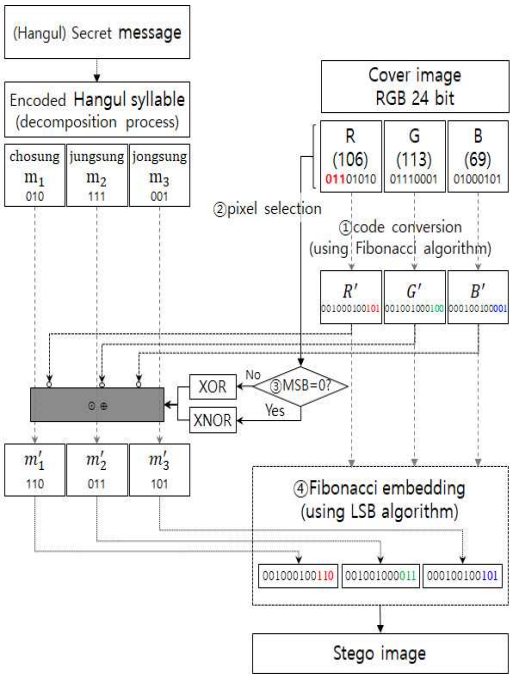

그림 1. 제안된 방법에서 삽입과정

Fig. 1. Embedding process in the proposed method

3.2 은닉된 자료의 추출 과정

스테고 매체로부터 은닉된 문자를 추출하는 단계별 과정은 다음과 같다.

단계1 : 스테고 이미지에서 피보나치 수열에 의해 변형된 비트화된 정보로부터 RGB 정보를 획득하고, 은닉 시작 위치와 종료 위치, 픽셀 선택값(k)을 확인한다. $p=0$으로 초기화한다.

단계2 : 획득된 RGB 정보를 참고하여 기본정보를 획득한다.

2.1 R, G, B 값을 기반으로 이진화 자료를 생성한다.

2.2 R, G, B 값을 기반으로 피보나치 수열을 이용한 변환된 이진화 자료에서 최하위 n비트 정보를 획득한다.

단계3 : RGB 채널 중에서 선택된(k) 픽셀값의 MSB를 확인한다.

3.1 MSB가 0이면 R, G, B 채널의 이진화 값 왼쪽 n비트와 2.2에서 구성된 정보를 XNOR 연산한다.

3.2 MSB가 1이면 R, G, B 채널의 이진화 값 왼쪽 n비트와 2.2에서 구성된 정보를 XOR 연산한다.

3.3 $p=p+1$을 계산한다.

단계4 : 단계3의 계산된 정보로부터 대체된 초성, 중성, 종성자를 획득한 후 글자를 구성한다.

4.1 $p<5$이면 획득된 (m_1, m_2, m_3)를 기반으로 은닉된 문자를 재구성한다.

4.2 $p \geq 5$이면 획득된 정보를 무시한다. $p=0$으로 초기화한 후 다음 단계로 간다.

단계5 : 은닉 자료의 종료 위치까지 단계3부터 단계4를 반복한다.

단계6 : 비밀 자료를 획득한다.

스테가노그래피는 제3자가 감지할 수 없는 안전한 통신 시스템을 구현하는 것을 목표로 한다. 스테고 이미지의 품질을 평가하기 위해 PSNR을 사용하며, 값이 클수록 커버 이미지를 손상시키거나 왜곡되지 않았음을 의미한다. PSNR 값은 (1)식에 의해 계산된다. 여기에서 l은 커버 매체의 행의 수이며, c는 열의 수를 의미한다. x와 y는 커버 이미지와 스테고 이미지의 화소 값이다.

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

$$MSE = \frac{1}{l \cdot c} \sum_{i=1}^{l} \sum_{j=1}^{c} (x_{ij} - y_{ij})^2 \quad (2)$$

4. 적용 및 결과

숨기려는 한글 문자는 표1과 같은 음절로 구성되어 있다. 초성, 중성, 종성자를 3비트 혹은 4비트로 구성된 정보에 재배치하여 m_1, m_2, m_3를 준비한다. 여기에서는 $n=3$을 사용하였다. 즉 3

비트를 적용할 경우 8가지 영역으로 배치하여 변환된 정보를 활용하였다. 재배치된 정보와 그림1을 기반으로 하였다. 임의의 수(k)를 선택하여 RGB 픽셀의 각각의 MSB에 따라 XNOR, XOR를 결정한다. RGB 픽셀 정보를 기반으로 피보나치 수열을 적용하여 최상위 3비트와 연산을 수행하여 $m_1^{'}$, $m_2^{'}$, $m_3^{'}$ 정보를 획득한다. 여기에서는 $k=1$을 적용하였다. LSB 알고리즘을 이용하여 $m_1^{'}$, $m_2^{'}$, $m_3^{'}$를 최하위 3비트에 대체시키며, 보안성을 강화하기 위해 5주기마다 쓰레기 정보를 대체한다. 여기에서는 계산의 편의성을 위해 커버 이미지 정보를 활용하였다.

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

Application method	Hidden data (byte)	MSE	PSNR	Correlation
General	22	7.821	39.198	0.9984
	46	7.234	39.536	0.9982
Proposed	22	4.102	42.001	0.9992
	46	5.123	41.035	0.9989

한글 입력 자료는 11글자(22byte)와 23글자(46byte)를 각각 사용하였다. 커버 이미지로 A(31,791byte), B(27,772byte)를 사용하였다.

적용된 결과는 표2에 제시하였다. 커버 매체에 따라 다소간의 차이가 있지만 MSE는 4.613, PSNR 값이 41.517(dB)이다. 또한 비트화된 은닉자료와 커버 매체 LSB 3비트와의 일치율은 17.39%였으며, 상관계수는 0.9991로 커버 매체와 스테고 매체 사이의 차이를 감지하기가 어렵다는 것을 확인하였다.

5. 결론

제안된 방법은 RGB 픽셀을 선택하고, MSB를 이용하여 은닉하려는 한글 메시지를 XOR 혹은 XNOR 연산을 진행하며, 피보나치 알고리즘에 의해 재구성된 영역의 최하위 비트 영역에 정보를 은닉하게 하여 비합법적인 추출 과정을 매우 어렵게 한다. 즉 XOR-XNOR 연산, 주기적인 가짜자료의 대체, 피보나치 알고리즘의 특성을 활용함으로 보안성을 확보할 수 있음을 보였다. 제안한 방법은 PSNR을 사용하여 평가되었으며, 허용 기준치[10]보다 32.94% 높게 나타나는 결과를 보였다.

REFERENCES

[1] F. Akhter and M. Selim, "A New Approach of Graph Realization for Data Hiding using Human Encoding", *International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 12, pp. 436-442, 2016.

[2] A. Rehman, T. Saba, T. Mahmood, Z. Mehmood, M. Shah, and A. Anjum, "Data Hiding Technique in Steganography for Information Security using Number Theory", *Journal of Information Science*, Vol. 45, No. 6, pp. 767-778, 2019.

[3] M. N. Abdulwahed, "An Effective and Secure Digital image Steganography Scheme using Two Random Function and Chaotic Map", *Journal of Theoretical and Applied Information Technology*, Vol. 98, No. 1, pp. 78-91, 2020.

[4] A. A. Almayyahi, R. Sulaiman, F. Qamar and A. E. Hamzah, "High-Security Image Steganography Technique using XNOR Operation and Fibonacci Algorithm", *International Journal of Advanced Computer Science and Applications*, Vol. 11, No. 10, pp. 511-522, 2020.

[5] U. A. Md. Ehasn Ali, Md. Sohrawordi and Md. Palash Uddin, "A Robust and Secured Image Steganography using LSB and Random Bit Substitution", *American Journal of Engineering Research,* Vol. 8, Issue 2,

pp. 39-44, 2020.

[6] K. Joshi, R. Yadav, and G. Chawla, "An Enh anced Method for Data Hiding using 2-bit XOR in Image Steganography", *International Journal of Engineering and Technology*, Vol. 8, No. 6, pp. 3043-3055, 2017.

[7] R. M. Neamah, J. A. Abed, and E. A. Abbood, "Hide Text Depending on the Three Channels of Pixels in Colour Images using the Modified LSB Algorithm", *International Journal of Electrical and Computer Engineering*, Vol. 10, No. 1, pp. 809-815, 2020.

[8] A. Ahmed and A. Ahmed, "A Secure Image Steganography using LSB and Double XOR Operations", *International Journal of Computer Science and Network Security*, Vol. 20, No. 5, pp. 139-144, May 2020.

[9] A. Setyono and D. R. I. M. Setiadi, "Securing and Hiding Secret Message in Image using XOR Transposition Encryption and LSB Method", *Journal of Physics: Conference Series 1196*, pp. 1-6, 2019.

[10] 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.

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