한국정보전자통신기술학회논문지(jkiiect)'23-4, Vol.16 No.2
논문 23-16-02-97 http://dx.doi.org/10.17661/jkiiect.2023.16.2.97

RS-box 은닉 모델에 기반한 한글 메시지 보안을 위한 이미지 스테가노그래피

지선수*

Image Steganography for Securing Hangul Messages based on RS-box Hiding Model

Seon-su Ji*

요 약 대부분의 정보는 네트워크를 통해 전송하기 때문에 제3자에 의한 도청, 가로채기 등이 발생할 수 있다. 네트워크에서 효과적이고, 안전한 비밀 통신을 위한 적절한 조치가 요구된다. 스테가노그래피는 비밀정보를 다른 매체에 숨기는 것을 제3자가 감지할 수 없도록 조치하는 기술이다. 구조적 취약점으로 인해 암호화와 스테가노그래피 기법에 의해 보호된 정보는 합법적이지 못한 그룹에게 쉽게 노출될 수 있다. 숨기는 방법의 단순성과 예측 가능성이 존재하는 LSB의 한계를 개선하기 위해 의사난수생성기와 재귀 함수에 기반하여 은닉하려는 메시지의 보안성을 향상시키는 기법을 제안한다. 보안성과 혼돈성을 강화하기 위해, 선택된 채널의 상위 비트에서 임의 비트를 선택한 결과와 RS-box에 의해 변형된 정보를 XOR 연산하였다. 제안된 방법의 성능을 확인하기 위해 PSNR과 SSIM을 이용하였다. 기준값에 비해 제안한 방법의 SSIM과 PSNR은 각각 0.9999, 51.366으로 정보를 숨기는데 적절함을 확인하였다.

Abstract Since most of the information is transmitted through the network, eavesdropping and interception by a third party may occur. Appropriate measures are required for effective, secure and confidential communication in the network. Steganography is a technology that prevents third parties from detecting that confidential information is hidden in other media. Due to structural vulnerabilities, information protected by encryption and steganography techniques can be easily exposed to illegitimate groups. In order to improve the limitations of LSB where the simplicity and predictability of the hiding method exist, I propose a technique to improve the security of the message to be hidden based on PRNG and recursive function. To enhance security and confusion, XOR operation was performed on the result of selecting a random bit from the upper bits of the selected channel and the information transformed by the RS-box. PSNR and SSIM were used to confirm the performance of the proposed method. Compared to the reference values, the SSIM and PSNR of the proposed method were 0.9999 and 51.366, respectively, confirming that they were appropriate for hiding information.

Key Words : Bitwise conversion, Hybrid hiding Techniques, Recursion shuffling, SSIM, Steganography

1. 서론

사이버 공간에서 디지털 통신은 필수적인 요소이며, 안전하지 않은 채널을 통해 송신 및 수신되는 정보에 대한 보안성과 신뢰성을 보장해주는 조치는 중요해지고 있다. 대부분의 디지털 정보는 네트워크를 통해 전송하기 때문에 제3자에 의한 도청, 위변조, 속이기, 가로채기 등이 발생할 수 있다. 따라서 네트워크를 통한 효과적이고, 안전한

*Department of Computer Sciences&Engineering, Gangnung-Wonju National University
Received February 28, 2023 Revised March 09, 2023 Accepted March 29, 2023

비밀 통신을 위한 조치가 요구된다. 데이터의 기밀성을 확보하기 위해 스테가노그래피와 암호화가 사용된다. 암호화는 실질적인 권한이 없는 사용자가 읽을 수 없도록 메시지에 혼돈(confusion)과 확산(diffusion) 기법을 적용한다. 스테가노그래피는 비밀정보를 다른 매체에 숨기는 것 자체를 제3자가 감지할 수 없도록 조치하는 기술이다. 구조적, 설계적, 관리적 문제의 취약점 등으로 인해 암호화와 스테가노그래피 기법에 의해 보호된 정보는 합법적이지 못한 그룹에게 쉽게 노출될 수 있다. 위변조로부터 보호되고, 기밀성이 보장된 정보를 전달하기 위해 암호화와 은닉기법을 함께 사용하여 은닉 매개체와 비트를 임의로 설정하여 혼돈성과 저항성을 강화하는 하이브리드 기법이 제시된다[1-2]. 스테가노그래피 과정의 주요 목표는 커버 매개체에서 비밀 메시지를 최소한으로 왜곡하거나 대체하여 은닉 정보가 매개체 내에서 비밀로 유지되도록 조치하는 것이다. 이를 위해 다양한 알고리즘을 사용하여 비밀 메시지를 암호화와 뒤섞기를 한 후 매개체의 데이터 일부에 대체 삽입한다. 매개체 중 이미지는 전송과 적용이 쉽고, 이미지의 픽셀 강도는 정보를 숨기는데 효과적으로 구현할 수 있으며, 비밀정보를 매개체 크기의 33%까지 은닉할 수 있다[3]. 또한 생성된 스테고 이미지 품질이 높기 때문에 LSB(least significant bit)를 이용한 이미지 스테가노그래피 방법은 폭넓게 사용되고 있으며, 연구와 개발이 계속되고 있다. 은닉 방법의 단순성과 예측 가능성이 존재하는 LSB의 한계를 개선하기 위해 의사난수생성기(pseudo random number generator, PRNG)와 재귀 함수에 기반하여 은닉하려는 메시지의 보안성을 향상시키는 기법을 제안한다.

논문의 2장에서 스테가노그래피 기법에 대한 관련된 자료를 제시하였다. 3장에서 제안하는 방법의 구현과정을 설명하고, 제안하는 방법의 성능 분석은 4장에서 표현하였다. 결론은 5장에서 제시하였다.

2. 관련 연구 분야

인터넷 공간에서 정보의 송수신은 중요한 기능이며, 이를 위해 스테가노그래피와 암호화 등이 사용된다. 두 기술이 결합된 하이브리드 방법이 보안성과 저항성을 높이는 안정적인 메커니즘을 달성할 수 있다.

Fateh 등은 한 번의 변경으로 비밀 메시지의 n비트에 대해 2^n개의 서로 다른 상태를 생성하는 새로운 매핑 함수를 제안하였다. 은닉단계에서 비밀 메시지를 n비트 그룹으로 나눈 다음 입력 이미지의 2^{n-1} 픽셀을 선택하여 각 그룹을 은닉하는 LSB MR(matching revised) 기반의 새로운 접근법을 보였다. 제안된 방법에서의 PSNR 값은 기존 방법에 비해 높았으며, 개선된 LSB MR은 높은 수준의 기밀성이 제공된다는 것을 보였다. 또한 ILSB(inverted LSB)의 PSNR은 기본 LSB 보다 높다는 것을 보였다[1]. Ali 등은 침입자로부터 메시지를 보호하기 위해 임의의 픽셀과 비트 선택을 위한 PRNG를 사용하여 커버 이미지에 비밀 메시지를 삽입하는 방법을 제안하였다. 24비트 컬러 이미지의 픽셀에서 비트화된 비밀정보를 숨기기 위해 3-3-2 방식을 사용하였으며, 보안성 높이고, 삽입용량을 개선할 수 있음을 보였다. 이때 임의의 픽셀 선택과 RGB 값에서의 임의의 비트 위치를 선택하기 위해 두 단계의 PRNG를 사용하였다[3]. Solak 등은 비밀성, 계산시간, 삽입용량 및 비지각성에서 효과적인 SED(shifting operation of encrypted data)-LSB를 적용하는 이중 계층 보안을 제안하였다. 키 생성기와 비트 이동 연산 과정을 추가하여 안전한 정보 은닉 알고리즘을 구현하였으며, 역연산을 수행하여 $n=4$비트 이동 작업을 진행함으로 보안성을 높일 수 있음을 제시하였다[4]. Ahmed 등은 MSB에서 추출된 비밀키와 비트화된 정보를 이중으로 XOR 연산한 후 LSB에 은닉하는 2단계 과정을 제시하였다. 이때 보안성을 강화하기 위해 이중 XOR 연산을 사용하는 일회용 패드 대칭 암호화 알고리즘을 사용하였다[5]. Özdemir 등은 암호와 스테가노그래피를 결합하

기 위해 BPS(bit plane slicing) 방법으로 얻은 MSB 조각의 비트 스트림과 메시지 스트림의 이중 XOR 연산을 수행하는 효과적인 방법을 제시하였다. 커버 이미지를 RGB 채널로 분할한 후 BPS를 R 채널에 적용하였다. 알고리즘의 시작 부분에서 처리할 비트 평면의 수와 R 색상 채널이 결정되고, 암호문 메시지는 R 채널의 LSB 비트에 은닉하는 개선된 방법을 제시하였다[6].

이 논문에서는 삽입용량과 보안성을 고려하여 비밀정보를 하나의 픽셀에 삽입하는 과정에서 한글 문자 정보에 대해 재귀 함수에 기반한 임의성과 혼동성을 강화하는 새로운 기법을 제안하였다.

3. 제안된 기법

송신 과정에서 의도하지 않은 수신자에 취약하지 않으며, 안전한 방식으로 네트워크를 통해 전달될 수 있도록 보안성과 혼돈성이 강화된 메시지 전송 기법이 필요하다. 제안하는 방법은 한글 메시지의 임의성과 저항성을 보장하기 위해 대체된 비트 정보에 기반한 순차적 이동 이중 암호화(sequential shift-double encryption)한 후 RGB에서 임의로 선택된 채널에 적용한다. 첫 번째 단계로 한글 문자에서 음절 분리를 한 후 비트화된 정보로 대치한 후 이동 과정을 적용한다, 두 번째 단계로 재귀함수에 의해 선택된 비트와 선택된 메시지 정보에 대해 exclusive-OR 연산을 수행하고, 그 결과를 임의로 선택되는 RGB 각 채널의 n-LSB에 대체한다. 이때 비밀 메시지의 보안성을 위해 의사 난수생성기를 사용한다.

커버 매개체에 은닉하려는 한글 메시지에서 글자는 초성, 중성, 종성자로 구성되어 있으며, 각각의 음절 요소는 사용 빈도에 따라 b비트 체계의 이진화 정보로 대체하고, PRNG에 의한 이동을 하였다. 예를 들어 $b=3$으로 변환될 경우 9개의 대체된 비트 정보를 얻을 수 있으며, 이동 과정은 그림 1에서처럼 표현될 수 있다. 그림 1에서 괄호의 수는 구성 요소를 의미한다.

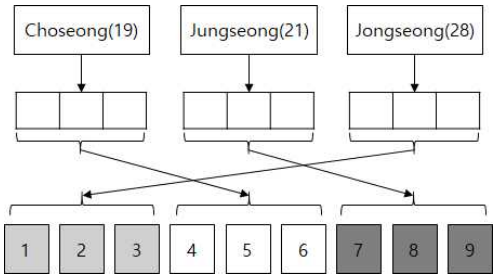

그림 1. 한글 메시지의 분해 후 비트 변환 과정
Fig. 1. Bitwise conversion process after decomposition of Hangul message

그림 1의 변환된 비트 정보에 혼돈성과 무작위성을 추가하였다. 즉 불확실성을 강화하기 위해 선형 매핑 $X_i : R \rightarrow R$, $i = 1, 2, ..., b^2$으로 대응되도록 하였다. 여기에서는 (1)식을 변형한 (3)식을 제안한다.

$$cp_j = p_i \cdot R_a \bmod q + 1 \quad (1)$$

$$p_i = (cp_j - 1) \cdot R_d \bmod q \quad (2)$$

여기에서 $q(>8)$는 임의 수이며, p_i는 i번째 비트 위치, cp_j는 변경된 j번째 비트 위치, R_a (≥ 3)는 임의 수, R_d는 모듈러 역수를 나타낸다.

뒤섞음을 임의로 선택하고, 혼돈성을 강화하기 위해 (1)식에서 재귀함수를 적용하여 변형된 (3)식을 계산할 수 있다.

$$m_j = (p_i \cdot R_a + 1) R_a \bmod q + 1 \quad (3)$$

(1)식의 역함수인 (2)식에 (1)식을 대입하여 두 식의 관계를 (4)식에서와 같이 증명할 수 있다.

$$(p_i \cdot R_a \bmod q + 1 - 1) \cdot R_d \bmod q = p_i \cdot R_a \cdot R_d \bmod q = p_i \quad (4)$$

(3)식을 참고로 한 무작위성의 추가, 커버 매개체에서 임의로 선택된 비트와 비밀 메시지 비트에

대해 Exclusive-OR 연산, 의사난수생성기에 의한 RGB 채널의 선택 등에 기반하여 n-LSB에 정보를 은닉하는 하이브리드 과정을 제안한다. 예를 들어 $b=3$, $n=1$인 경우 임의로 선택된 RGB 값의 비트 위치를 사용하여 메시지를 삽입하는 과정을 그림 2에서 표현하였다. 여기에서 $m_j, (j=1,2,...9)$는 그림 1과 수식 (3)을 이용한 RS(recursion shuffling)-box를 통과한 변환된 비밀 자료를 의미한다.

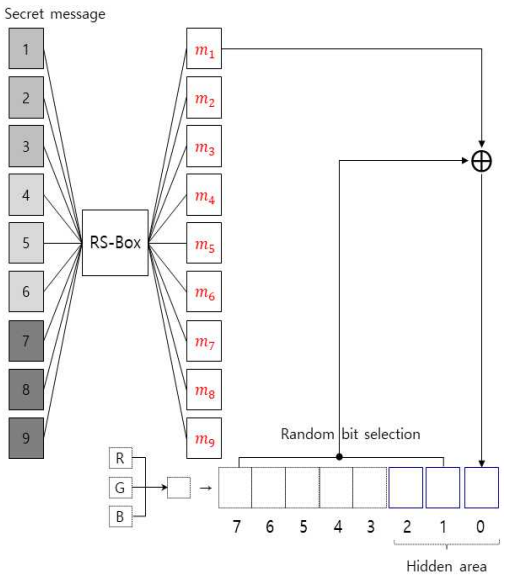

그림 2. 임의로 선택된 RGB 값의 비트 위치를 사용하여 메시지를 삽입하는 과정

Fig. 2. Embedding process of messages using random chosen bit positions of RGB value

3.1 은닉하는 과정

분해된 메시지 정보는 RS-Box, 의사난수생성기를 이용한 비트 선택, XOR 연산 과정을 거쳐 커버 매개체의 n-LSB에 대체된다.

1단계:비밀(한글) 메시지와 커버 이미지를 입력한다. 삽입위치(sp), 삽입방향(R/L), n, b, $seed$ 값을 설정한다.

2단계:한글의 글자를 초성, 중성, 종성으로 분해한 후 b비트 이진화 정보로 대체한 후 의사난수생성기에 의해 이동을 한다. (b*3) 개의 비트 정보를 준비한다.

3단계:비밀정보를 RS-box에 적용하여 변환된 정보($m_j, j=1,2,...,b$*3)를 획득한다.

4단계: (b*3) 개의 비트 정보를 RGB의 각 채널에 삽입한다. $j=1$로 설정한다.

4.1 R 채널을 선택한다.

①의사난수생성기에 의해 $(8-n)$개의 상위 비트에서 임의의 비트를 선택한다.

②if$(n \le 1)$ then ①에서 선택된 비트 정보를 m_j와 XOR 연산한 후 1-LSB에 대체한 후 $j=j+1$을 계산하고, ④로 이동한다.

$else$ ①에서 선택된 비트 정보를 m_j와 XOR 연산한 후 삽입방향이 R일 경우 n-LSB에 대체한다.

③$j=j+1$를 계산하고, ①과 ②를 반복하여 $(n-1)$-LSB, $(n-2)$-LSB 순서로 대체한다. 삽입방향이 L일 경우 ②와 ③에서 1-LSB, 2-LSB, ⋯, n-LSB 순서로 대체한다.

④①부터 ③의 과정을 반복한다.

4.2 G 채널을 선택한 후 단계 4.1 과정을 반복한다.

4.3 B 채널을 선택한 후 단계 4.1 과정을 반복한다.

4.4 if$(j \le b$*$3)$ then 단계 4.1로 이동한다.

5단계:2단계부터 4단계를 반복하여 숨기려는 비밀 메시지를 모두 삽입한다.

6단계:스테고 이미지를 완성한다.

단계 4에서 의사난수생성기를 이용하여 RGB 채널을 임의로 선택하는 다양성을 확보한다.

3.2 추출하는 과정

수신자에 의해 획득된 스테고 이미지로부터 비밀정보를 추출하는 과정은 정보를 은닉하는 과정

의 역순이다.

1단계:스테고 이미지와 관련 모수 정보(sp, b, $seed$, n, R/L)를 준비한다.

2단계:RGB 각 채널의 LSB에서 모수 정보를 참고하여, (b*3) 개의 비트 정보를 획득한다. $i=1$로 설정한다.

①RGB 각 채널에서 n값을 참고로 LSB의 정보($temp$)를 선택한다,

②$seed$ 값과 의사난수생성기를 참고하여 $(8-n)$개의 상위 비트에서 선택한 비트 정보와 $temp$를 XOR 연산한다.

③if(i++$\leq b$*3) then ①부터 ②의 과정을 반복한다.

④(b*3)개의 비트 정보를 inverse RS-box에 적용하여 역변환된 정보 m_j, $j=1,2,...,b*3$을 획득한다. 이때 b 비트 단위로 분리하고, 의사난수생성기에 의한 이동을 수행한 후 대체된 음절로 변환한 후 3개의 구성 요소를 조합하여 글자를 완성한다.

3단계:2단계를 반복하여 은닉된 모든 정보를 추출한다.

4단계:비밀 메시지를 완성한다.

4. 적용 결과

커버 매개체로 RGB 이미지를 사용하며, 각 채널은 의사난수생성기를 이용하여 선택한다, RS-box를 적용하여 암호화와 뒤섞기를 한다. 이때 $b=3$, $R_a=5$, $q=9$, $k_1=0.01$, $k_2=0.03$로 설정하고, n이 주어질 때 PSNR과 SSIM을 각각 계산한다. 선택된 채널의 경우 7 ($n=1$), 6($n=2$), 5($n=3$)개의 상위 비트에서 임의 비트를 선택하여 RS-box에 의해 변형된 정보와 XOR 연산한 것을 1-LSB, 2-LSB, 3-LSB에 각각 대체하였다.

비트 평면에서 $n=1,2,3$으로 주어질 때 각각의 경우에 스테고 이미지 품질을 측정하기 위해 수식 (5)를 이용하여 PSNR을 계산하였다.

$$PSNR=10\cdot\log_{10}(\frac{l^2}{MSE})\,(dB) \tag{5}$$

여기에서 MSE는 평균 제곱 오차를 의미하며, $l=\max\{cov(v,h),\,stg(v,h)\}\fallingdotseq 255$이다.

커버와 스테고 이미지의 유사도를 위해 수식 (6)을 이용하여 SSIM을 계산하였다.

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{6}$$

여기에서 커버 이미지($x\in X$)와 스테고 이미지 ($y\in Y$) 대해 μ_x와 μ_y는 각각 x와 y의 표본평균, σ_x와 σ_y는 각각 x와 y의 표본표준편차, σ_{xy}는 x와 y의 공분산이다. $c_1=(k_1 l)^2$와 $c_2=(k_2 l)^2$는 안정화 계수이다.

제안된 방법을 적용하여 n-LSB, $n=1,2,3$에 각각의 비밀 정보를 은닉할 경우 계산된 PSNR의 결과는 표 1에서 표현하였다. 저항성과 임의성을 추가한 제안된 방법은 기본 LSB 및 Hong[7]의 PSNR 값과 유사하다는 것을 확인하였다.

표 1. 제안된 방법의 성능 비교
Table 1. Performance comparison of the proposed method

n	LSB		Hong[7]		Proposed	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
1	0.493	51.199	0.248	54.181	0.473	51.366
2	2.326	44.464	1.282	47.054	1.720	45.775
3	10.192	38.048	6.118	40.264	10.151	38.966

R, G, B 각각의 채널을 선택하여 비밀정보를 삽입할 경우와 RGB 채널 모두 이용할 경우 LSB에서 n을 1, 2, 3으로 설정하여 대체할 때 PSNR과

SSIM을 계산한 결과는 표 2에서 보여주었다.

표 2. RGB 채널과 비트 평면에 따른 PSNR과 SSIM 값
Table 2. PSNR and SSIM values according to RGB channels and bit planes

channel		n	simple LSB	random LSB[7]	Proposed
PSNR	R	1	51.097	51.094	51.011
		2	44.706	45.291	45.877
		3	39.706	39.132	38.559
	G	1	50.550	50.556	50.562
		2	43.867	44.061	44.256
		3	37.970	37.431	36.892
	B	1	52.066	52.121	52.176
		2	44.950	45.101	45.252
		3	39.319	39.072	38.825
	RGB	1	51.652	52.171	51.366
		2	44.297	44.154	45.775
		3	37.963	39.126	38.065
SSIM		1	0.9999	0.9999	0.9999
		2	0.9971	0.9970	0.9973
		3	0.9911	0.9921	0.9917

제안된 방법은 기본 LSB 및 Hong[7]의 PSNR, SSIM과 유사함을 확인하였다. 또한 PSNR 값은 기준치[8]보다 $n=1$일 경우 6.7%, $n=2$일 경우 18.6%, $n=3$일 경우 21.9% 향상할 수 있음을 확인하였다. Solak[4] 등이 제시한 것과 같이 B 채널의 PSNR 값은 B 채널에 숨겨지는 여유 비트 때문에 R 및 G 채널보다 높음을 확인하였다. 또한 SSIM 값은 1.0에 근접하며, 커버 이미지와 스테고 이미지의 유사도가 높다는 것을 확인하였다. RGB 각각의 채널만을 이용하는 것과 모든 채널을 이용할 경우 이미지 품질이 우수하고 유사도 면에서 차이는 없으며, 임의 선택에 의한 각각을 적용하는 것은 추가적으로 혼돈성을 높이는 효과적인 방법임을 확인하였다.

5. 결론

3가지 구성 요소로 이루어지는 특성을 가진 한글의 글자 정보를 분리한 후 각각의 요소에 대체한 정보를 암호화와 뒤섞기를 위한 RS-box를 적용하고, 은닉 비트를 제외한 상위비트를 임의로 선택하여 XOR 연산한 정보를 n-LSB에 대체함으로 보안성과 저항성을 강화하였다. n이 클수록 이미지 품질과 유사도 측면에서도 효율적임을 확인하였다.

REFERENCES

[1] M. Fateh, M. Rezvani, Y. IraniA, "New Method of Coding for Steganography Based on LSB Matching Revisited", Security and Communication Networks, Vol. 2021, pp. 1-15, 2021.

[2] S. Kaur, S. Bansal, R. K. Bansa, "Image Steganography for Securing Secret Data using Hybrid Hiding Model", Multimedia Tools and Applications, Vol. 80, No. 13, pp. 1-21, 2021.

[3] U. A. Md. Ehsan Ali, Emran Ali, Md. Sohrawordi, Md. Nahid Sultan, "A LSB Based Image Steganography using Random Pixel and Bit Selection for High Payload", International Journal of Mathematical Sciences and Computing, Vol. 7, No. 3, pp. 24-31, 2021.

[4] S. Solak, U. Altinisik, "A new Approach for Steganography:Bit Shifting Operation of Encrypted Data in LSB (SED-LSB)", Bilişim Teknolojileri Dergisi, Vol. 12, No. 1, pp. 75-81, 2019.

[5] A. Ahmed, A. Ahmed, "A Secure Image Steganography using LSB and Double XOR Operations", International Journal of Computer Science and Network Security, Vol. 20, No. 4, pp. 139-144, 2020.

[6] B. Özdemir, N. Doğan, "Data Hiding to the Image with Bit Plane Slicing and Double XOR", Manas Journal of Engineering, Vol. 10, Issue 1, pp. 66- 72, 2022.

[7] W. Hong, "Adaptive Reversible Data Hiding

Method based on Error Energy Control and Histogram Shifting", Optics Communications, Vol. 285, No. 2, pp. 101-108, 2012.

[8] C. K. Chan, 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