임의 순열과 영상차를 이용한 영상 스테가노그래피

김찬란, *이상화, **박한훈, 박종일†
한양대학교, *서울대학교, **부경대학교
chanrankim@hanyang.ac.kr, lsh529@snu.ac.kr, hanhoon_park@pknu.ac.kr,
jipark@hanyang.ac.kr

Image Steganography Using Random Permutation and Image Difference

Chanran Kim *Sang Hwa Lee **Hanhoon Park Jong-Il Park
Hanyang University *Seoul National University **Pukyung National University

요 약

본 논문에서는 전송하고자 하는 원영상 대신에 전혀 다른 영상을 전송하여 원영상 정보를 보호하는 스테가노그래피(steganography) 기법을 제안한다. 전송할 영상의 자연스러움을 잃어버리지 않으면서 원영상을 복구할 수 있는 차영상 정보를 LSB(Least Significant Bit)에 담고, 픽셀간의 위치 관계를 무작위로 섞어 줌으로써, 원영상을 보호하는 기법을 제안한다. 본 논문에서는 우선 원영상과 전송할 영상 (cover image)의 차영상을 생성하고, 각 픽셀의 차이값을 큰 범위로 양자화하여 차영상의 데이터 크기를 줄인다. 그리고, 각 픽셀의 차이값을 전송할 영상의 4 픽셀에 걸쳐서 하위 2bit 에 나누어 담는다. 8bit 영상에서 하위 2 bit 를 다루기 때문에, 각 채널 밝기값의 최대 차이값은 3 으로 설정되어 자연스럽게 영상을 생성할 수 있다. 끝으로 신호의 보호를 위하여 차영상의 픽셀과 전송할 영상의 픽셀간의 대응위치를 무작위 순열로 변환하여 외부에서 쉽게 복원할 수 없도록 한다. 이러한 스테가노그래피 제안 기법을 통하여 원영상 대신에 커버 영상을 전송함으로써, 자연스러운 정보전송이 가능하며, 외부의 감시와 복원에 안전한 정보보호 기능이 강화될 수 있다. 여러 영상에 대한 실험을 통한 제안 기법에 의하면, 전송되는 커버 영상이 자연스럽기 때문에 외부에서 정보가 숨겨진 사실을 느끼지 못하며, 송수신 장치에 내장된 무작위 순열을 통하여 외부에서는 원영상 정보를 복구하는 것도 매우 어렵게 되어 있음을 확인하였다. 본 제안 기법은 군사통신이나 중요한 정보를 다루는 기관에서의 정보 전달 및 정보보호 시스템에서 사용될 수 있다.

1. 서론

인터넷 기술 발전으로 인해 영상을 쉽게 주고 받는 세상이 되면서, 일상 생활에서도 많은 영상 데이터를 주고 받는다. 이에 따라 영상 데이터의 중요도가 높아지고 있다. 영상 스테가노그래피는 보내고자 하는 원영상을 그대로 전송하지 않고 대신에 원영상을 복구할 수 있는 완전히 다른 영상 (cover image)을 전송하여 중요한 정보를 숨기는 기술이다[1]. 영상에 스테가노그래피 기술을 적용하면, 서로 약속된 사용자가 아닌 경우에는 전송되는 영상 자체를 자연스럽게 받아들이기 때문에, 그 속에 담긴 원영상 정보를 전혀 눈치채지 못하여 데이터 암호화 및 은닉 기술과는 다른 방식으로 원정보를 보호할 수 있다.

영상에서의 스테가노그래피는 정의와 개념이 다양하고 그만큼 여러가지 방법들이 있다. 공간 영역, 주파수 영역에서의 방법과 그 둘을 이용한 adaptive 방법 등, 다양한 방법들이 있다[2]. 또한 전송하는 영상 자체에 직접 정보를 내장하는 방식이 있는데 이는 영상 워터마킹 또는 데이터 은닉 기법과 동일한 개념이다. 그리고 실제 의도한 영상과는 전혀 다른 커버 영상을 전송한 후 수신측에서 사전에 약속한 알고리즘으로 원영상을 복원하는 기법으로 구분할 수도 있다. 이 논문에서는 커버 영상을 이용하는 후자의 방법에 기초하여 커버 영상과 원영상(original image)간의 차영상을 생성하고 공간 영역에서 LSB 를 사용하는 기술을 다룬다. 이 기술은 다른 기술에 비해 빠르며 강력하다[3]. 무작위 순열 행렬을 이용하여 차영상 정보를 교란시킴으로써, 외부에서 복원하기 어렵도록 한다.

2. Proposed Steganography System

영상에서 한 픽셀이 가지는 한 채널의 값은 보통 8bit 로 표현된다. 이러한 8bit 의 최하위 2 bit 는 전체 256 중 0~3 의 값을 갖는다. 이는 단 1.5% 정도를 의미한다. 이러한 값의 차이는 인간의 눈으로는 감지할 수 없다. 이러한 인간의 눈의 한계를 이용하여 LSB 스테가노그래피를 실현한다.

본 논문에서 제안하는 스테가노그래피는 두 영상이 필요하다. 하나는 겉으로 보여질 커버 영상, 다른 하나는 전송의 목적이 되는 원영상이다. 동일한 크기의 두 영상을 가정하자. 커버 영상을 2 배로 키우면, 커버 영상과 원 영상의

†교신 저자

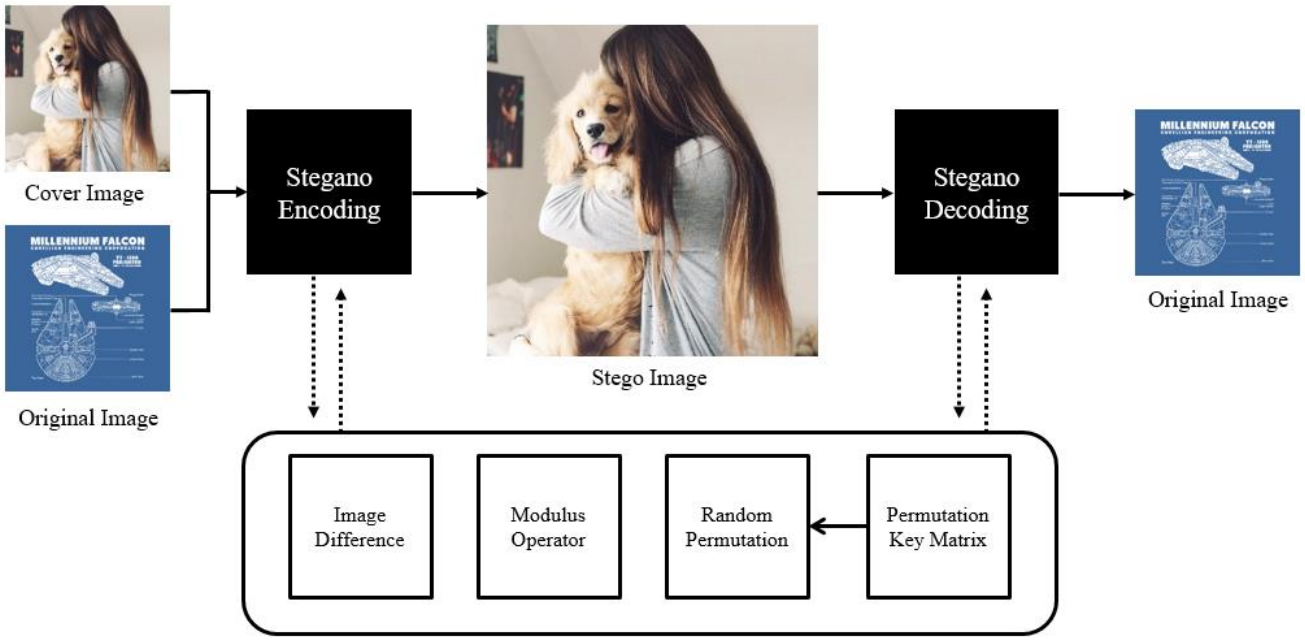

Fig. 1. Block diagram of proposed method

공간 비율이 4:1 이 된다. 이렇게 하면 원영상 4 픽셀에 원영상 1 픽셀의 데이터를 나누어 담을 수 있다. 이렇게 보이는 영상 외에 다른 정보를 가지고 있는 영상을 stego 영상이라 한다.

stego 영상을 만드는 과정을 stegano encoding, 복호화하는 과정을 stegano decoding 이라 한다 (Fig. 1). stegano encoding 과정에서 커버 영상과 원영상의 영상차 값을 이용하여 차영상을 만든다. 이 차영상은 음의 부호도 고려하여야 하기 때문에 modulus 연산을 통하여 값을 8bit 내로 적절하게 분배한다. 마지막으로 임의 순열 과정을 거쳐 차영상과 stego 영상의 픽셀간에 대응되는 위치를 섞은 뒤 최종적인 stego 영상을 완성한다. 이때 사용되는 임의 순열 행렬은 복호화에 쓰일 key 행렬로 수신측과 송신측 모두 가지고 있어야 한다. 복호화 과정은 위 과정의 역순으로 이루어진다

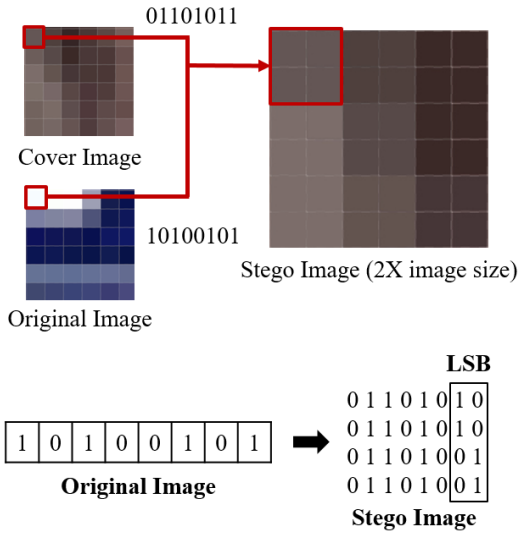

Fig. 2. An example of creating a stego image using the LSB.

가장 먼저 LSB 를 다루기 위하여 커버 영상을 2 배로 키워 원영상의 데이터에 대응시킬 위치를 잡는다. 2 배의 영상으로 변환하였기 때문에, stego 영상 한 픽셀당 2 개의 LSB 를 이용하면 충분히 숨길 수 있다. 커버 영상의 한 픽셀 데이터를 동등하게 stego 영상의 이웃하는 4 픽셀에 대응시킨다. 그 4 픽셀의 하위 2 비트를 각각 원영상의 8 비트 데이터를 4 등분한 것으로 대체한다. (Fig. 2)에서 한 픽셀에 대한 예를 보여준다. 커버 영상의 한 픽셀이 01101011 의 8bit 데이터를 가지고 있고, 대응 대는 위치에 있는 원영상의 한 픽셀이 10100101 의 데이터를 가지고 있다. 이러한 경우 stego 영상을 만들 때, 대응 되는 stego 영상 픽셀은 커버 영상과 동일한 값을 가지는 4 픽셀이 된다. 원영상의 8 비트 데이터를 2 개씩 나눈 10, 10, 01, 01 을 stego 영상의 4 개의 픽셀의 2 LSB 에 대입한다. 위에서 설명했던 것처럼, 원영상에서 최대 3 의 차이밖에 나지 않기 때문에, 인간의 눈으로는 느낄 수 없다.

2.1. Difference Encoding

LSB 를 다루는 것만으로도 다른 정보가 있는지 눈으로 확인할 수 없지만, 정직하게 원영상을 그대로 부호화하는 것보다 변형시켜 표현하는 것이 데이터를 복원하기 힘들게 한다[4]. 차영상은 cover image – original image 로 만든다(식 (1)).

$$D_{x,y} = C_{x,y} - O_{x,y}. \quad (1)$$

이렇게 차영상을 만들면, 기존의 8bit 에 없는 음의 부호를 추가로 고려해야한다. 이 문제점을 해결하기 위해 modulus 2, 5 연산, 또는 XOR 연산을 이용하여 해결할 수 있다 (Fig. 3).

가장 단순하게 modulus 2 연산을 취하는 것은 차영상이 가질 수 있는 데이터에 1 을 더하여 -254~256 의 범위로 만든다. 그리고 2 로 나누어 -127~128 로 만든다 (식 (2)).

Fig. 3. (a) Original Image and Difference Image with (b) module 2 (c) module 5 (d) XOR

$$D_{x,y} = (D_{x,y} + 1)/2, \quad (2)$$

$$D_{x,y} = (D_{x,y} + 2)/5, \quad (3)$$

$$D_{x,y} = C_{x,y} \oplus O_{x,y}. \quad (4)$$

그리고 거기에 127을 더하면, 0~255의 데이터가 되어 1픽셀의 1 채널 8bit 에 담을 수 있다. 이는, 2 개의 값이 1 개의 값으로 양자화 되는 것으로 볼 수 있다.

Modulus 5 연산은 차영상이 가질 수 있는 -255~255 의 데이터 값을 5 로 나누어 1 개의 값에 5 개의 값이 대응되게 한다 (식 (3)). 값에 대응되는 값의 수가 동일하게 하기 위하여 2 를 더해준다. 이 경우 차영상의 데이터 값은 7 bit 로 표현이 가능하다.

마지막으로 XOR 연산을 이용하여 차영상을 만드는 방법이다. XOR 연산은 부호 비트를 필요로 하지 않기 때문에 단순하다 (식 (4)).

2.2. Random Permutation

원영상에 커버 영상의 데이터를 대입할 때 대응되는 위치가 복잡하면 복원하기 힘들어진다[5]. 본 논문에서는 random permutation matrix 를 이용하여 변형된 LSB 데이터의 위치를 섞는다. 이 permutation matrix 는 보안성을 높이는 이중 장치의 역할을 하는 Key 값이다. 송신 측과 수신 측이 초기에 생성하여 서로 갖고 있어서, encoding, decoding 시에 각각 필요하다. OTP(One Time Pad)와 같은 다양한 방식으로 Key 의 보안성을 높이는 것도 가능하다[6].

$$(P_c(P_r I)^T)^T = P_r I P_c^T = \mathrm{X} \quad (5)$$

$$P_r(P_c X^T)^T = P_r X P_c^T = I \quad (6)$$

Where $P_r \cdot P_r = E$, $P_c \cdot P_c = E$. I 는 기존 영상, X 는 임의 순열로 바꾼 영상이다. P_r 은 행에 대한 임의 순열 행렬이고, P_C 는 열에 대한 임의 순열 행렬이다. I 가 $(\mathrm{m} \times \mathrm{n})$ 행렬이라면, P_r 은 $(\mathrm{m} \times \mathrm{m})$ 행렬로, P_C 는 $(\mathrm{n} \times \mathrm{n})$ 행렬로 만들어야 한다. 그러면, 연산의 결과인 X 는 I 와 같은 크기인 $(\mathrm{m} \times \mathrm{n})$ 행렬이 된다.

임의 순열 행렬은 각 행과 열의 단 하나의 원소만 1 이고 다른 모든 원소가 0 인 정방 행렬이다. 이것을 어떤 행렬에 곱하면 그 행렬의 행의 순서를 바꿔준다. P_C 를 전치행렬로 이용하는 것은 열의 순서를 바꿔주기 위함이다.

3. 실험 결과

본 논문의 실험에서는 일상적인 사진을 커버 영상으로, 정보를 담고 있는 도면 영상을 원영상으로 설정하였다. 두 영상은 채널당 8bit 를 가지는 RGB 3 채널 영상이다. 한 채널에서, 1 픽셀의 8 bit 데이터를 온전히 숨기기 위해서는 4 픽셀의 최하위 2bit 가 필요하다. 따라서 2 배 이상의 크기를 가진 영상이라면, 영상의 데이터를 충분히 숨길 수 있다. 이 실험의 stegano encoder 는 동일한 크기의 커버 영상과 원영상을 입력 받아 커버 영상의 크기를 2 배로 늘려 원영상의 정보를 담는다. 담을 정보를 처리하기 위해 가장 먼저 영상차를 구하고, 경우에 따라 modulus 연산을 취해 부호화시킨다. 마지막으로 영상의 수신측과 송신측이 갖고 있는 permutation key matrix 를 이용하여 random permutation 를 수행하여 배열을 섞는다. Decoding 과정은 이에 역으로 수행된다.

Table 1. PSNR of Cover and Original Image in each case

	Cover Image's PSNR	Original Image's PSNR
Without Difference	44.16581	-
With XOR	44.44984	43.12914
With modulus 5	44.08357	38.51187
With modulus 2	43.92628	43.37532

본 논문에서 소개한 방법을 여러 영상에 적용하고, stego 영상과 커버 영상 간의 PSNR 을 비교하였다. (Table 1). 커버 영상의 PSNR 은 stego 영상을 nearest neighbour interpolation 로 축소한 영상과 비교를 하여 얻었다. XOR 의 경우 가장 좋은 결과를 얻었고, 오히려 차영상을 이용하지 않았을 때 보다 좋은 결과를 얻었다. 원영상의 PSNR 의 경우 차영상을 이용하지 않는 방법은 온전한 8bit 데이터를 가지고 있기 때문에 stego 영상에서 원영상을 완벽하게 복원할 수 있었다.

커버 영상의 PSNR 의 수치가 상당이 높기 때문에 인간의 눈으로는 인지할 수 없다. 또한 숨겨진 영상, 원영상의 PSNR 도 방법에 따라 높은 결과가 나타나 스테가노그래피를 효과적으로 수행하였다고 볼 수 있다.

본 논문에서는 stego 영상을 무손실 압축하여 전송하는 경우로 가정하였지만, 실제에서는 전송하는 과정에서 압축이 되는 경우가 많다. 따라서 향후 jpeg encoding 과 같은 환경에서 LSB 변형에 강인한 구조 설계가 필요하다[7].

4. 결론

본 논문에서는 정보를 담고 있는 원영상 대신에 전혀 다른 커버 영상을 전송하여 원영상 정보를 외부로부터 보호하는 스테가노그래피(steganography) 기법을 제안하였다. 본 논문에서는 원영상과 커버 영상의 차영상을 생성하고, 각 픽셀의 차이값을 큰 범위로 양자화하여 차영상의 데이터 크기를 줄였다. 그리고 각 픽셀의 차이값을 전송할 커버 영상의 4 픽셀에 걸쳐서 하위 2bit 에 나누어 담았다. 끝으로 신호의 보호를 위하여 차영상의 픽셀과 전송할 영상의 픽셀간의 대응위치를 무작위 순열로 변환하여 외부에서 쉽게 복원할 수 없도록 하였다. 스테가노그래피 제안 기법을 통하여 원영상 대신에 커버 영상을 전송함으로써, 자연스러운 정보전송이 가능하며, 외부의 감시와 복원에 안전한 정보보호 기능이 강화될 수 있다. 여러 영상에 대한 실험을 통하여 제안 기법에 의하면, 전송되는 커버 영상이 왜곡없이 자연스럽기 때문에 외부에서 정보가 숨겨진 사실을 느끼지 못하며, 송수신 장치에 내장된 무작위 순열을 통하여 외부에서는 원영상 정보를 복구하는 것도 매우 어렵게 되어 있음을 확인하였다. 본 제안 기법은 군사통신이나 중요한 정보를 다루는 기관에서의 정보 전달 및 정보보호 시스템에서 사용될 수 있다[3]. 향후 연구 방향으로는 JPEG 등의 압축 환경에서 LSB 이 왜곡되는 문제를 해결하는데 집중할 필요가 있다[8].

감사의 글

본 연구는 방위사업청 및 국방과학연구소에 의해 설립된 신호정보 특화연구센터의 지원을 받아 수행되었음.

참고문헌

[1] Neil F. Johnson and Sushil Jajodia, "Exploring steganography: Seeing the unseen." Computer., vol. 31, no. 2, pp. 26-34, 1998.

[2] Abbas Cheddad, Joan Condell, Kevin Curran, and, Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods." Signal processing., vol. 90, no. 3, pp. 727-752, 2010.

[3] Paul Alvarez, "Using extended file information (EXIF) file headers in digital evidence analysis." International Journal of Digital Evidence., vol. 2, no. 3, pp. 1-5, 2004.

[4] Da-Chun Wu and Wen-Hsiang Tsai, “A steganographic method for images by pixel-value differencing” Pattern Recognition Letters., vol. 24, no. 9, pp.1613-1626, 2003.

[5] Chin-Chen Chang and Hsien-Wen Tseng, "A steganographic method for digital images using side match." Pattern Recognition Letters., vol. 25, no. 12, pp. 1431-1437, 2004.

[6] Adam Shefi, "System and method for synchronizing one time pad encryption keys for secure communication and access control." U.S. Patent., No. 6,445,794. 2002.

[7] Pennebaker, William B., and Joan L. Mitchell, “JPEG: Still image data compression standard.” Springer Science & Business Media., 1992.

[8] Ross J. Anderson and Fabien A. P. Petitcolas, "On the limits of steganography." IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS., vol. 16, no. 4, pp. 474-481, 1998.