The Journal of the Convergence on Culture Technology (JCCT)
Vol. 6, No. 1, pp.485-488, February 29, 2020. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2020.6.1.485
JCCT 2020-2-60

공간적 암호화를 사용하는 영상 워터마킹 기법

Image Watermarking Algorithm using Spatial Encryption

정수목*

Soo-Mok Jung*

요 약 본 논문에서는 공간적 암호화를 사용하여 영상에 소유권 정보인 워터마크를 영상 픽셀의 LSB에 안전하게 은닉하는 기법을 제안하였다. 제안된 워터마킹 기법은 영상의 지적재산권 보호에 효과적으로 사용될 수 있다. 제안된 기법을 사용하여 공간적으로 암호화된 워터마크를 은닉한 영상인 스테고 이미지로부터 워터마크를 손실 없이 추출할 수 있다. 실험을 통하여 제안 기법의 우수성을 확인하였다. 제안된 기법을 적용하여 워터마킹을 수행한 결과 영상인 스테고 이미지의 화질은 51dB이상으로 사람이 육안으로 워터마크의 존재여부를 인식할 수 없으며, 워터마크가 공간적으로 암호화되어 있기 때문에 워터마크의 보안성이 우수하다.

주요어 : 커버 이미지, 워터마크, 공간적 암호화, LSB

Abstract In this paper, a technique for securely concealing the watermark, which is intellectual property information, in the image pixel LSB using spatial encryption is proposed. The proposed watermarking technique can be effectively used to protect intellectual property of images. The proposed technique can be used to extract watermark without loss from the stego-image, which is a hidden image of spatially encrypted watermark. The experimental results confirmed the superiority of the proposed technique. As a result of performing watermarking using the proposed technique, the image quality of the stego-image is higher than 51 dB, so humans cannot visually recognize the presence of a watermark. Due to the watermark is spatially encrypted, the security of the watermark is excellent.

Key words : cover image, watermark, spatial encryption, LSB

Ⅰ. 서 론

이미지의 지적재산권 보호를 위하여 이미지에 소유권 정보인 워터마크(watermark)를 은닉하는 워터마킹 기법이 사용된다. 이미지에 워터마크를 은닉하여 생성된 스테고 이미지(stego-image)로부터 워터마크를 손실 없이 추출할 수 있어야 하고, 스테고 이미지에 워터마크가 은닉되어 있는지를 사람이 인식할 수 없는 비인지성을 만족하여야 한다[1,2]. 워터마킹 결과로 생성되는 스테고 이미지의 품질을 우수하게 하여 커버 이미지(cover image)와 스테고 이미지 사이의 차이를 인식하는 것을 불가능하게 함으로써 비인지성을 만족시킬 수 있다. 따라서 커버 이미지와 차이가 거의 없도록 스테고 이미지를 생성하는 것이 중요하다.

*정회원, 교수, 삼육대학교 컴퓨터메카트로닉스공학부
접수일: 2019년 11월 15일, 수정완료일: 2019년 11월 30일
게재확정일: 2019년 12월 10일

Received: November 15, 2019 / Revised: November 30, 2019
Accepted: December 10, 2019
*Corresponding Author: jungsm@syu.ac.kr
Division of Computer Mechatronics Engineering,
Sahmyook Univ, Korea

이미지 픽셀의 LSB에 워터 마크 데이터 비트를 은닉하는 기법이 제안되었다[3]. LSB에 워터 마크 데이터 비트가 내장되어 있으면, 스테고 이미지로부터 워터 마크 데이터를 쉽게 추출 할 수 있게 되어 워터마크의 보안성이 크게 약화된다. LSB를 사용하여 워터 마크 데이터를 임베딩하는 기술들이 개발되었지만[4,5,6,7] 본 논문에서는 공간적 암호화를 사용하여 워터 마크 데이터를 LSB에 은닉하는 기법을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에서 기존의 LSB에 워터마크 데이터 비트를 은닉하는 기법을 기술하고, 3장에서 공간적 암호화 기법을 사용하는 제안기법을 기술한다. 실험결과를 4장에 기술하고, 5장에서 결론을 맺는다.

II. LSB에 워터마크를 삽입하는 기법

그레이 스케일 이미지의 각 픽셀은 8비트로 구성되기 때문에 0~255의 값을 갖는다. 8비트로 표현되는 픽셀 값의 LSB에 워터마크 데이터 비트를 은닉한다. 픽셀의 값이 238인 경우, 8비트로 표시되는 픽셀 값은 11101110 이다. 이 픽셀 값의 LSB에 워터마크 데이터 비트 1을 은닉하는 경우를 그림 1에 나타내었다. 그림 1에서 보는 바와 같이 LSB의 값이 워터마크 데이터 비트로 대체 되었으므로 은닉 결과 픽셀 값이 239가 되어 1만큼의 값이 커지게 된다. 따라서 픽셀이 조금 더 밝게 된다. 그리고 픽셀 값이 238인 경우, 워터마크 데이터 비트가 0이면 은닉 결과 픽셀 값은 변하지 않는다.

MSB LSB

1	1	1	0	1	1	1	1

그림 1. 픽셀 값이 238인 픽셀에 워터마크 데이터 비트 1을 은닉한 결과

Figure 1. Consequence of hiding watermark data bit 1 in a pixel with a pixel value of 238

픽셀 값의 LSB가 1인 경우, 워터마크 데이터 비트가 0이면 은닉 결과 픽셀 값이 1만큼 작아지고 워터마크 데이터 비트가 1인 경우에는 은닉 결과 픽셀 값이 동일하게 된다. 따라서 원래의 픽셀 값과 워터마크 데이터 비트를 은닉한 결과 픽셀 값과의 차의 절대치는 0이거나 1이 되어 평균은 0.5가 된다. 원래의 픽셀 값과 워터마크 데이터 비트를 은닉한 결과 픽셀 값과의 차의 절대치는 평균적으로 0.5의 값을 가지므로 사람의 시각으로는 이러한 차이를 인식할 수 없게 된다. 따라서 이 기술은 워터 마크 데이터 비트를 매우 간단하게 숨길 수 있고, 워터 마크 데이터를 은닉함으로써 생성 된 스테고 이미지의 이미지 품질이 매우 우수하다. 그러나 각 픽셀의 LSB를 사용하여 워터 마크 데이터를 쉽게 추출 할 수 있으므로 보안에 매우 취약한 단점이 있다.

III. 제안기법

공간적 암호화 기법을 사용하여 이미지에 워터마크를 은닉하기 위한 기법은 다음과 같다. 그림 2와 같이 5개의 필드로 구성된 공간적 암호화 관련 정보를 정의한다. 그림 3에 표시된 바와 같이, 그림 2의 공간적 암호화 정보는 커버 이미지의 최상위 행에 있는 픽셀들의 LSB에 좌측에서 우측으로 차례대로 저장된다.

Field name	Starting point (X)	Starting point (Y)	Normal em-bedding	Inverse em-bedding	Em-bedding pattern
bit	10	10	10	10	W-40

그림 2. 공간적 암호화 정보 레코드

Figure 2. Spatial Encryption Information record

그림 2에서 보는 바와 같이 공간적 암호화 정보는 다음과 같은 5가지의 정보로 구성된다. 공간적 암호화를 시작하는 위치 (x, y)의 값이 20비트로 표현된다. 따라서 시작위치는 (0,0)~(1023, 1023)사이의 값으로 지정될 수 있다. 그림 3에서 시작위치와 종료위치는 각각 (3, 5), (3, 4)이다.

Normal embedding은 워터마크 데이터 비트를 반전시키지 않은 그대로의 값을 LSB에 은닉하는 연속적인 워터마크 데이터 비트의 개수 이다. 이 값이 0일 때는 모든 워터마크 데이터 비트를 반전 없이 픽셀의 LSB에 은닉하는 것으로 정의한다. Normal embedding과 Inverse embedding의 값들이 모두 1023일 때는 처음 1023개의 워터마크 데이터 비트는 반전 없이 은닉하고, 다음의

1023개의 워터마크 데이터 비트는 반전시켜서 은닉하는 것으로 정의한다. 이러한 형식에 따라 반복적으로 워터마크 데이터 비트들을 픽셀의 LSB에 은닉한다.

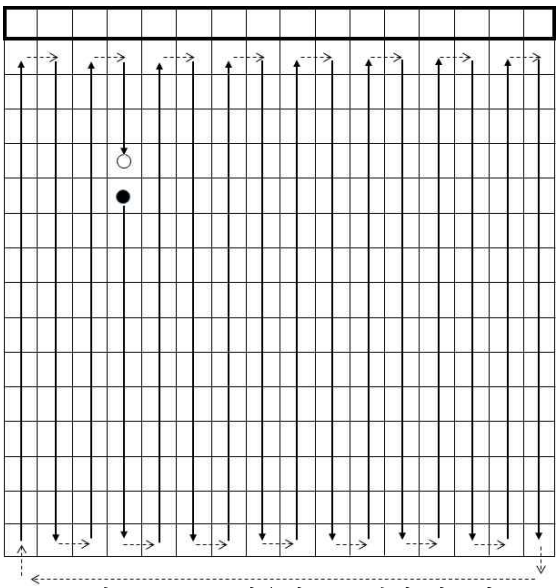

그림 3. LSB를 사용하는 공간적 암호화
Figure 3. Spatial Encryption using LSB

Embedding pattern은 워터마크 데이터를 은닉하는 패턴을 나타낸다. Embedding pattern은 이미지 폭(Width)에서 40을 뺀 값으로 표시된다. 512x512 크기를 갖는 이미지의 경우에는 Embedding pattern은 472비트로 표현된다. 따라서 Embedding pattern은 2^{472}가지로 정의 될 수 있어 무수히 많은 형태로 워터마크 데이터를 커버 이미지에 은닉할 수 있다. 실제 워터마킹에서, 그림 2에 있는 공간적 암호화 정보 레코드의 필드 순서를 다양하게 적용하여 보안성을 높일 수 있다. 또한 공간적 암호화 정보 레코드를 저장하는 위치와 임베딩 패턴을 다양하게 정의하면 보안성을 한 층 더 높일 수 있다.

Ⅳ. 실험 및 결과

실험에 사용된 커버 이미지는 그림 4와 같이 512x512 크기를 갖는 Lena, Aya_matsuura, ship, peppers, Yale 이다. 본 논문의 영문 초록을 ASCII코드로 변환한 바이너리 데이터를 워터마크 데이터로 사용하여 커버 이미지에 은닉하였다.

그림 2의 공간적 암호화 정보 필드의 크기와 순서를 다양하게 정의 할 수 있고, 그림 3에서 공간적 암호화 정보 저장 위치와 임베딩 패턴을 다양하게 지정하여 보안을 높일 수 있으나, 본 논문에서는 그림 2, 3과 같은 경우를 가정하여 실험을 수행하였다. 즉, 시작 위치와 종료위치를 각각 (3, 5), (3, 4)로 하였고, Norma embedding과 Inverse embedding을 각각 1로 설정하였다. Embedding pattern은 2(W-40) 가지로 정의 될 수 있는데, 그림 3과 같은 embedding pattern을 W-40 비트 모두가 0인 패턴으로 가정하였다. 따라서 공간적 암호화 정보 레코드에서 (0,8), (0, 9), (0, 17), (0, 19), (0, 29), (0, 39) 위치만 1이고 그 외의 위치는 모두 0이 된다. 그림 3과 같이 공간적 암호화 정보 레코드를 커버 이미지의 최상위 행의 좌측에서 우측으로 픽셀의 LSB에 차례대로 은닉하였다. 워터마크 데이터들을 공간적 암호화 정보에 정해진 방법에 따라, 워터마크 데이터들을 커버 이미지의 LSB에 은닉하였다.

그림 4는 실험에 사용된 커버 이미지와 워터마크가 은닉된 스테고 이미지를 나타내고 있다. 그림 4에서 보는 바와 같이 스테고 이미지의 품질이 높기 때문에 커버 이미지와 스테고 이미지를 시각적으로 구분하는 것은 불가능하다. 그림 4의 Lena, Aya_matsuura, ship, peppers, Yale 이미지에 워터마크를 은닉하여 생성된 각 스테고 이미지의 PSNR 값은 각각 51.154dB, 51.152dB, 51.143dB, 51.160dB, 51.137dB 이다. 스테고 이미지의 PSNR 값이 매우 높아 커버 이미지와 스테고 이미지를 시각적으로 구분 할 수 없고, 워터마크가 공간적으로 암호화 되어 있기 때문에 워터마크의 안정성과 보안성이 매우 높아진다.

(a-1) Lena
(cover image)

(a-2) Lena
(stego-image)

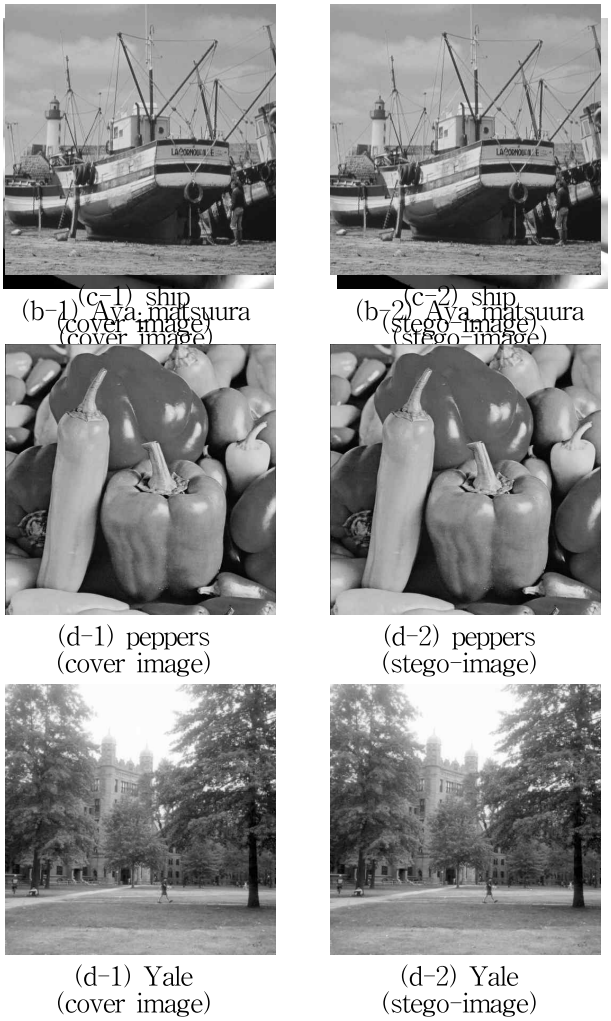

그림 4. 커버 이미지와 스테고 이미지
Figure 4. Cover images & stego images

또한 제안기법에서는 스테고 이미지의 각 픽셀의 LSB 로부터 데이터를 추출하여 공간적 워터마킹 정보에 따라 워터마크를 손실 없이 추출 할 수 있다. 따라서 제안된 기법은 영상의 소유권 정보를 공간적으로 암호화하여 커버 이미지에 안전하게 은닉할 수 있는 매우 효과적인 워터마킹 기법이다.

V. 결 론

본 논문에서 제안된 기법을 사용하여 워터마킹을 수행하면, 소유권 관련 정보인 워터마크를 공간적 암호화 방법으로 커버 이미지에 안전하게 은닉할 수 있고, 커버 이미지에 워터마크 데이터가 은닉되어 있는 스테고 이미지의 시각적 품질이 매우 우수하여 워터마크 데이터가 은닉되어 있는지 여부를 시각적으로 인식 할 수 없으며, 스테고 이미지로부터 워터마크 데이터를 손실 없이 추출 할 수 있다.

그림 2의 공간적 암호화 정보의 필드순서를 다양하게 정의 하고, 공간적 암호화 정보의 저장위치를 다양하게 지정 하고, 그림 3의 Embedding pattern을 다양하게 정의하여 워터마크 데이터를 은닉하면 워터마크 데이터의 보안성이 매우 높아지게 된다. 따라서 제안된 기법은 이미지의 지적재산권 보호에 크게 기여할 수 있다.

References

[1] Hsiang-Cheh Huang, Chi-Ming Chu, and Jeng-Shyang Pan, “The optimized copyright protection system with genetic watermarking”, Soft Computing, Vol. 13, No. 4, pp. 333-343, 2009. DIO: 10.1007/s00500-008-0333-9

[3] Zhicheng Ni, Yun-Qing Shi, N. Ansari, and Wei Su, “Reversible data hiding”, IEEE Trans. on Circuits and Systems for Video Technology, Vol. 16, No. 3, pp. 354-362, 2006. DOI: 10.1109/TCSVT.2006.869964

[3] Andrew Z. Tirkel, G.A. Rankin, Ron G. van Schyndel, W.J. Ho, N.R.A. Mee, and C.F. Osborne, “Electronic watermark”, Digital Image Computing, Technology and Applications, pp. 666-673, Macquarie University, 1994.

[4] Anum Javeed Zargar, “Digital Image Watermarking using LSB Technique”, International Journal of Scientific & Engineering Research, Vol. 5, Issue 7, pp. 202-205, 2014.

[5] Preeti Gaur, and Neeraj Manglani, “Image Watermarking Using LSB Technique”, International Journal of Engineering Research and General Science, Vol. 3, Issue 3, pp. 1424-1433, 2015.

[6] B. Chitradevi, N. Thinaharan, M. Vasanthi. “Data Hiding Using Least Significant Bit Steganography in Digital Images”, Stat. Approaches Multidiscip. Res. Vol. 1, pp. 143 - 150, 2017.

[7] Tanmoy Halder, Sunil Karforma, Rupali Mandal, “A Block-Based Adaptive Data Hiding Approach Using Pixel Value Difference and LSB Substitution to Secure E-Governance Documents“. Journal of Information Processing Systems, Vol. 15, No. 2, pp. 261 - 270, 2019. DOI: 10.3745/JIPS.03.0111