The Journal of the Convergence on Culture Technology (JCCT)
Vol. 7, No. 4, pp.863-867, November 30, 2021. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2021.7.4.863

JCCT 2021-11-105

인접 픽셀과 공간적 암호화 기법을 사용한 컬러 영상 워터마킹 기법

Color Image Watermarking Technique using Adjacent Pixels and Spatial Encryption Technique

정수목*

Soo-Mok Jung*

요 약 본 논문에서는 컬러 영상의 LSB에 워터마크를 은닉하기 위하여 영상의 인접 픽셀들과 공간적 암호화 기법을 사용하여 보안성이 높은 컬러 영상 워터마킹 기법을 제안하였다. 본 논문에서 제안된 기법에 따라 컬러 영상의 LSB에 워터마크를 은닉하여 생성된 스테고 이미지의 화질은 원본 영상과 차이를 인지할 수 없을 정도로 매우 우수하고, 스테고 이미지로부터 원본 워터마크를 손실 없이 추출할 수 있다. 제안 기법을 사용하여 영상에 워터마크를 은닉하면 스테고 이미지에 은닉되어있는 워터마크는 다중으로 암호화되어있기 때문에 워터마크의 보안성이 매우 우수하게 유지된다. 제안된 워터마킹 기법은 높은 보안이 요구되는 군사, 지적 재산권 보호 등의 응용에 사용될 수 있다.

주요어 : 워터마크, 스테고 이미지, 암호화, 컬러 이미지, 은닉

Abstract In this paper, in order to hide the watermark in the LSB of the color image, a color image watermarking technique with high security is proposed by using the adjacent pixels of the image and the spatial encryption technique. According to the technique proposed in this paper, the quality of the stego-image generated by hiding the watermark in the LSB of the color image is so excellent that the difference from the original image cannot be recognized, and the original watermark can be extracted from the stego-image without loss. If the watermark is hidden in the image using the proposed technique, the security of the watermark is maintained very high because the watermark hidden in the stego-image is multi-encrypted. The proposed watermarking technique can be used in applications such as military and intellectual property protection that require high security.

Key words : Watermark, Stego-image, Encryption, Color image, Hiding

Ⅰ. 서 론

컬러 영상에 소유권 정보와 같은 지적 재산권 정보인 워터마크(watermark)를 은닉하는 기법들이 사용되어 오고 있다. 워터마크를 영상에 은닉하여 생성된 스테고 이미지(stego-image)의 시각적 화질은 원본 영상과 구분 할 수 없을 정도로 우수하여야 하고, 원본 워터마크를 스테고 이미지로부터 손실 없이 추출할 수 있어야 한다. 따라서 워터마킹 기법에서는 스테고 이미지에 워터마크가 은닉되어있는지를 알 수 없는 비인지성

*정회원, 삼육대학교 컴퓨터공학부 교수 (제1저자)
접수일: 2021년 10월 31일, 수정완료일: 2021년 11월 3일
게재확정일: 2021년 11월 8일

Received: October 31, 2021 / Revised: November 3, 2021
Accepted: November 8, 2021
*Corresponding Author: jungsm@syu.ac.kr
Division of Computer Science & Engineering, Sahmyook Univ, Korea

(imperceptibility)이 매우 중요하다.[1][2] 스테고 이미지의 화질을 우수하게 유지하면, 스테고 이미지와 원본 이미지의 차이를 시각적으로 인지할 수 없게 되어 스테고 이미지에 워터마크가 은닉되어있는지를 인지할 수 없기 때문에 비인지성이 만족 된다. 따라서 워터마크를 영상에 은닉하는 기법에서는 스테고 이미지의 화질이 원본 이미지와 시각적으로 거의 차이가 없을 만큼 높은 화질을 유지하도록 하는 것이 중요하다.

워터마크를 영상 픽셀의 LSB에 은닉하는 기법들이 제안되었다.[3]-[6] 영상의 각 픽셀의 LSB에 워터마크의 데이터 비트를 은닉하면, 스테고 이미지의 화질이 우수하여 비인지성을 만족시키지만 스테고 이미지로부터 워터마크의 데이터 비트를 쉽게 추출할 수 있어 워터마크의 보안이 취약해지는 문제가 있다.

본 논문에서는 컬러 영상의 LSB에 워터마크 데이터 비트를 은닉하는 기법에서의 보안 문제를 해결하기 위하여, 영상의 인접 픽셀들을 사용하여 워터마크를 암호화한 뒤 공간적으로 다시 암호화를 수행하여 컬러 영상에 은닉하여 워터마크의 보안성을 매우 높게 유지하도록 하는 컬러 영상 워터마킹 기법을 제안하였다. 제안된 기법은 본 연구팀에서 제안한 기존의 기법들의 성능을 개선한 기법이다.[7]-[9]

본 논문의 구성은 다음과 같다. 2장에 영상 픽셀의 LSB에 워터마크 데이터 비트를 은닉하는 기존의 기법을 기술하고, 3장에 제안기법을 기술하였다. 실험 결과를 4장에 기술하였고 5장에 결론을 기술하였다.

II. 영상의 LSB에 워터마크를 은닉하는 기법

컬러 영상의 각 픽셀은 R, G, B 성분들로 구성된다. R, G, B 성분은 각각 1바이트로 표현되므로 각 성분은 0에서 255 사이의 값을 가지고 1픽셀은 3바이트로 구성된다. 워터마크 데이터 비트가 R, G, B 성분의 LSB에 은닉된다.

그림 1은 기밀 데이터인 워터마크 데이터 비트 1, 0, 0이 흰색(R: 255, G:255, B:255) 픽셀에 은닉된 경우를 나타낸다. 워터마크 데이터 비트가 R, G, B 성분의 LSB에 삽입됨에 따라 R, G, B 성분의 값이 미세하게 변경된다. 그림 1에서 R, G, B 성분의 값이 각각 255, 254, 254가 된 것을 확인할 수 있다. R, G, B 각 구성 요소에서 워터마크 데이터 비트가 은닉되어 발생하는 미세하게 변경되는 값의 평균은 0.5이다. R, G, B 각 구성 요소의 미세한 차이로 인해 발생하는 픽셀의 색상 변화는 시각적으로 식별할 수 없다. 따라서 원본 이미지와 워터마크가 은닉된 스테고 이미지를 시각적으로 구별하는 것은 불가능하다. 워터마크 데이터를 컬러 영상의 각 픽셀의 LSB에 은닉하는 경우 그림 1과 같이 픽셀당 최대 3비트를 은닉할 수 있다. 이 기법은 단순하여 간단하게 구현할 수 있지만, 워터마크 데이터가 픽셀의 LSB에 은닉되어 생성된 스테고 이미지로부터 원본 워터마크 데이터를 간단하게 추출할 수 있어 워터마크의 보안이 취약한 단점이 있다.

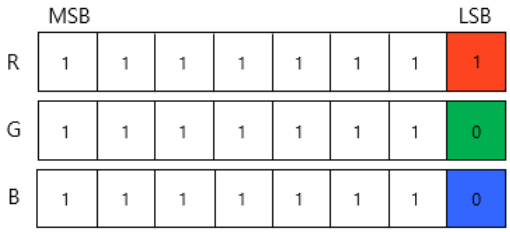

그림 1. R, G, B 성분의 LSB에 1, 0, 0 은닉
Figure 1. Hiding 1, 0, 0 in the LSB of R, G, and B components

III. 제안기법

컬러 영상의 LSB에 워터마크를 은닉하는 경우, 스테고 이미지로부터 워터마크를 추출하는 것이 용이하기 때문에 워터마크의 보안성이 취약한 단점이 있다. 이러한 단점을 극복하기 위하여 식 (1)을 사용하여 워터마크 데이터를 암호화한 후 컬러 영상의 LSB에 은닉한다. 식 (1)에서 E는 암호화된 워터마크 데이터 비트를 나타내고, i는 1부터 W·H-1의 값을 갖는다. W, H는 영상의 너비와 영상의 높이를 각각 나타낸다. $P_{(R,G,B)i-2}$, $P_{(R,G,B)i-1}$은 스테고 이미지의 위치 i-2, i-1에서 픽셀의 LSB 값을 나타낸다. i-2, i-1의 값이 음수이면 i-2, i-1의 값은 0의 값을 갖는 것으로 한다. K는 R, G, B 평면에서의 암호화 킷값을 나타내고, D는 워터마크 데이터 비트를 나타낸다. 식 (1)에 사용된 기호(⊙)는 Exclusive NOR 연산을 나타내는 기호이다.

식 (1)을 사용하는 경우, 위치 0에 있는 픽셀에는 워터마크 데이터를 은닉하지 않기 때문에 위치 0에서는 커버 이미지의 픽셀값이 스테고 이미지의 픽셀값이 된다. 위치 1 이후부터 워터마크 데이터 비트를 암호화한

비트를 해당 위치의 스테고 이미지의 픽셀의 LSB 값으로 한다. 예를 들어 커버 이미지의 R 평면의 픽셀값이 255, 254, 253, 252, 251, 250, 249, 248이고, 킷값이 0, 워터마크 데이터 비트가 '1011001'인 경우, 스테고 이미지의 픽셀의 값은 255, 254, 252, 252, 250, 251, 248, 249가 된다. 위치 0의 커버 이미지 픽셀에는 암호화된 워터마크 데이터 비트를 은닉하지 않기 때문에 커버 이미지의 픽셀값 255가 위치 0의 스테고 이미지의 픽셀값이 된다.

위치 1의 스테고 이미지의 픽셀값 254는 다음과 같이 결정된다. $E_1=P_0\odot P_0\odot K\odot D_1=1\odot 1\odot 0\odot 1=0$이 된다. 이때 P_0는 위치 0에서의 스테고 이미지의 픽셀값 255의 LSB인 1의 값이 된다. 암호화된 비트 E_1이 커버 이미지의 픽셀값의 LSB로 대체되어 위치 1에서의 스테고 이미지의 픽셀값이 된다. 따라서 위치 1에서의 스테고 이미지의 픽셀값은 254가 된다.

위치 2에서의 스테고 이미지의 픽셀값 252는 다음과 같이 결정된다. $E_2=P_0\odot P_1\odot K\odot D_2=1\odot 0\odot 0\odot 0=0$이 된다. 이때 P_0는 스테고 이미지의 위치 0에서의 픽셀값 255의 LSB인 1의 값이 사용되고, P_1은 스테고 이미지의 위치 1에서의 픽셀값 254의 LSB인 0의 값이 사용된다. 암호화된 비트 E_2가 커버 이미지의 픽셀값의 LSB로 대체되어 위치 2에서의 스테고 이미지의 픽셀값이 된다. 따라서 위치 2에서의 스테고 이미지의 픽셀값은 252가 된다. 따라서 식 (1)을 사용하여 워터마크 데이터를 암호화하면, 암호화된 워터마크 데이터 비트는 '0000101'이 된다.

$$E_{(R,G,B)i}=P_{(R,G,B)i-2}\odot P_{(R,G,B)i-1}\odot K_{(R,G,B)}\odot D_{(R,G,B)i} \quad (1)$$

식 (1)에 의해서 암호화된 워터마크 데이터들이 컬러 영상의 LSB에 은닉될 때, 워터마크의 보안성이 보다 향상되도록 공간적으로 암호화하는 기법을 적용하여 암호화된 워터마크 데이터를 은닉한다. 그림 2는 4x4 크기의 컬러 영상에서 R, G, B 평면별로 암호화된 워터마크 데이터가 공간적으로 암호화되어 은닉되는 것을 나타내는 은닉 패턴이다. 그림 2에서 흑색 원과 흰색 원은 암호화된 워터마크 데이터 은닉 시작 위치와 은닉 종료 위치를 각각 나타낸다. 따라서 컬러 영상에 은닉되는 워터마크 데이터의 총 비트 수는 (W·H-1)·3 비트가 된다. 그림 2의 경우에는 (4·4-1)·3=45 비트의 암호화된 워터마크 데이터가 은닉된다. 식 (1)에 의해서 암호화된 워터마크 데이터를 공간적으로 암호화하여 은닉하는 패턴을 그림 2에 표시한 패턴 외에도 다양하게 변경하여 은닉되는 워터마크의 보안성을 높일 수 있다.

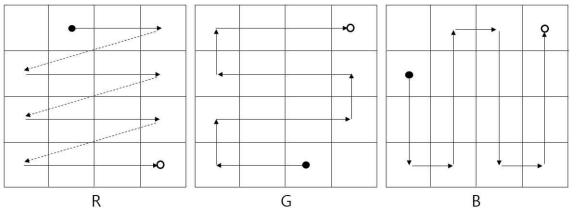

그림 2. 제안된 기법에서 공간적 암호화하는 패턴의 예
Figure 2. An Example of spatial encryption patterns in the proposed technique

다중으로 암호화된 워터마크 데이터가 은닉되어 있는 스테고 이미지로부터 식 (2)를 사용하여 원본 워터마크 데이터를 손실 없이 추출할 수 있다. 식 (2)에서 i는 1부터 W·H-1의 값을 갖는다. 암호화된 워터마크가 은닉되어 있는 스테고 이미지의 픽셀의 값이 255, 254, 252, 252, 250, 251, 248, 249인 경우, 위치 1부터 은닉되어 있는 워터마크 데이터를 추출하는 과정은 다음과 같다.

위치 1에 은닉되어있는 워터마크 데이터 비트는 $D_1=E_1\odot P_0\odot P_0\odot K=0\odot 1\odot 1\odot 0=1$이 된다. 이때 P_0는 위치 0에서의 스테고 이미지의 픽셀값의 LSB인 1의 값이 사용된다. 위치 2에 은닉되어 있는 워터 마크 데이터 비트는 $D_2=E_2\odot P_0\odot P_1\odot K=0\odot 1\odot 0\odot 0=0$이 된다. 이와 같은 과정을 거쳐 '101101'을 손실 없이 추출할 수 있다.

$$D_{(R,G,B)i}=E_{(R,G,B)i}\odot P_{(R,G,B)i-2}\odot P_{(R,G,B)i-1}\odot K_{(R,G,B)} \quad (2)$$

Ⅳ. 실험 결과

제안된 기법의 성능을 확인하기 위해 512x512 크기의 Lenna, sail-boat, Tiffany, pepper를 커버 이미지로 사용하여 실험을 수행하였다. 본 논문의 영문 초록을 기밀 데이터인 워터마크로 사용하였으며, 워터마크 데이터를 바이너리로 변환한 후, 식 (1)을 적용하여 암호화한 결과를 R, G, B 평면 순으로 그림 2와 같은 공간적 암호화 패턴에 따라 암호화된 워터마크 데이터를 반복적으로 은닉하였다.

그림 3은 실험 결과 이미지를 보여준다. 그림 a-1,

b-1, c-1, d-1은 실험에 사용된 각 커버 이미지들이다. 그림 a-2, b-2, c-2, d-2는 픽셀의 LSB에 순수 워터마크 데이터 비트들을 순차적으로 은닉하는 기존의 기법을 적용하여 생성한 스테고 이미지이다. 그림 a-3, b-3, c-3, d-3은 제안기법의 식 (1)을 적용하여 워터마크를 암호화한 다음, 그림 2와 같이 공간적으로 암호화하는 기법을 적용하여 생성된 스테고 이미지를 나타낸다.

그림 3에서 보는 바와 같이 제안된 기법을 사용하여 다중으로 암호화된 워터마크 데이터가 은닉된 스테고 이미지의 화질이 매우 우수하기 때문에 커버 이미지와 스테고 이미지를 시각적으로 구분할 수 없다. 따라서 사용자는 스테고 이미지에 워터마크가 숨겨져 있는지 여부를 인식할 수 없으며 스테고 이미지에 은닉된 워터마크를 손실 없이 추출할 수 있다. 비록 악의적인 목적으로 스테고 이미지로부터 다중으로 암호화된 워터마크를 추출하였을지라도 워터마크가 다중으로 암호화되어 있기 때문에 워터마크의 보안성이 매우 높게 유지된다.

표 1은 제안기법으로 워터마크를 각 커버 이미지에 은닉한 실험 결과 데이터이다. 표 1에서 보는 바와 같이 제안된 기법을 사용할 경우, 은닉되는 워터마크 데이터 비트 수는 최대 (W·H-1)·3에 해당하는 786,429비트이다. 제안기법에서 은닉되는 워터마크 데이터 비트 수가 기존의 LSB 기법에 비해 3비트 적지만, 제안된 기법에서는 워터마크 데이터를 다중으로 암호화하여 커버 이미지에 은닉하였기 때문에 워터마크의 보안성이 크게 향상된다.

표 1에서 보는 바와 같이 제안된 기법을 사용하여 생성된 스테고 이미지의 PSNR 값은 각각 51.145dB, 51.143dB, 51.148dB, 51.137dB이다. 일반적으로 PSNR 값이 40dB 이상이면 사람의 시각으로는 원본 영상과 스테고 이미지의 차이를 구분할 수 없다. 따라서 제안기법은 비인지성을 만족하여, 제안된 기법으로 워터마크를 은닉하면 스테고 이미지가 원본 커버 이미지와 시각적으로 차이가 없어 워터마크가 스테고 이미지에 은닉되어 있는지 여부를 인식할 수 없다. 또한 은닉되어 있는 워터마크는 다중으로 암호화되어 있기 때문에 보안성이 높게 유지된다. 그리고 스테고 이미지로부터 암호화 킷값과 공간적 암호화 패턴과 암호화 수식을 알아야만 기밀 데이터인 워터마크를 추출할 수 있다. 따라서 제안된 기법은 매우 효과적인 워터마킹 기법이다.

그림 3. 커버 이미지 및 스테고 이미지
Figure 3. Cover image and stego-image

표 1. 실험 결과
Table 1. Experimental results

Image	Technique	PSNR	Hidden bits
Lenna	LSB	51.178	786,432
	Proposed	51.145	786,429
sail-boat	LSB	51.148	786,432
	Proposed	51.143	786,429
Tiffany	LSB	51.069	786,432
	Proposed	51.148	786,429
pepper	LSB	51.148	786,432
	Proposed	51.137	786,429

V. 결 론

본 논문에서는 LSB에 워터마크를 은닉하는 경우 발생하는 보안이 취약한 문제를 해결하기 위하여, 워터마크를 암호화한 다음 공간적으로 다시 암호화하여 컬러 영상의 R, G, B 평면별로 각 픽셀의 LSB에 은닉하는 보안이 매우 우수한 기법을 제안하였다. 제안된 기법을 적용하여 워터마크를 영상에 은닉하면, 스테고 이미지

에 은닉된 워터마크의 보안이 매우 높게 유지되며, 스테고 이미지로부터 원본 워터마크를 손실 없이 복원할 수 있다.

영상에 은닉할 수 있는 워터마크의 최대 비트 수는 (W·H-1)x3 비트이며, 스테고 이미지의 PSNR 값은 51.137dB 이상이었다. 따라서 스테고 이미지에 워터마크가 은닉되어 있는지 여부를 식별할 수 없다. 제안된 기법은 중요 기밀 데이터를 은닉하여야 하는 군사, 지적 재산권 보호 등의 응용에 사용될 수 있는 효과적인 워터마킹 기법이다.

References

[1] H. C. Huang, C. M. Chu, and J. S. Pan, “The optimized copyright protection system with genetic watermarking,” Soft Computing, Vol. 13, No. 4, pp. 333-343, Feb. 2009. DOI: https://doi.org/10.1007/s00500-008-0333-9

[2] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. on Circuits and Systems for Video Technology, Vol. 16, No. 3, pp. 354-362, March 2006. DOI: https://doi.org/10.1109/TCSVT.2006.869964

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

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

[5] P. Gaur, and N. Manglani, “Image Watermarking Using LSB Technique”, International Journal of Engineering Research and General Science, Vol. 3, Issue 3, pp. 1424-1433, June, 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, January, 2017. https://doi.org/10.5281/zenodo.262996

[7] S. M. Jung, “An Advanced Color Watermarking Technique using Various Spatial Encryption Techniques”, The Journal of Korea Institute of Information, Electronics, and Communication Technology, Vol. 13, No. 3, pp.262-266, June, 2020. https://doi.org/10.17661/jkiiect.2020.13.3.262

[8] S. M. Jung, “Data hiding technique using image pixel value and spatial encryption technique”, International Journal of Internet, Broadcasting, and Communication, Vol. 13, No. 3, pp.50-55, August, 2021. https://doi.org/10.7236/IJIBC.2021.13.3.50

[9] S. M. Jung, “An Effective Technique to Conceal Confidential Data in the LSB of Image”, Autumn Annual Conference of KIIECT, October, 2021.