한국정보전자통신기술학회논문지(jkiiect)'20-6, Vol.13 No.3
논문 20-13-03-262 http://dx.doi.org/10.17661/jkiiect.2020.13.3.262

다양한 공간적 암호화 기법을 적용한 개선된 컬러 영상 워터마킹 기법

정수목*

An Advanced Color Watermarking Technique using Various Spatial Encryption Techniques

Soo-Mok Jung*

요 약 본 논문에서는 공간적 암호화 기법을 적용하여 컬러 영상의 LSB에 워터마크를 은닉하는 효과적인 기법을 제안하였다. 영상의 LSB에 은닉된 워터마크를 추출하여도 워터마크가 다양한 공간적 암호화 기법을 사용하여 암호화 되어 있기 때문에 추출된 워터마크의 정보를 해독 할 수 없다. 따라서 본 논문에서 제안된 공간적 암호화 기법을 사용하여 LSB에 워터마크를 은닉하면 기존의 LSB에 워터마크를 삽입하는 기법에 비하여 보안성이 크게 향상된다. 제안된 기법을 적용하여 워터마킹을 수행하면, 워터마크가 은닉된 영상의 화질이 매우 우수하여 원본 영상과 구별이 불가능하며 워터마크가 은닉된 영상으로부터 기밀 데이터인 워터마크를 손실 없이 추출 할 수 있다. 제안된 기법의 성능을 수학적으로 분석하고 제안된 기법의 우수성을 실험을 통하여 확인하였다. 512x512 크기를 갖는 Lenna, airplane, Tiffany, pepper 영상에 제안 기법을 적용하여 워터마크를 은닉한 경우, 워터마크가 은닉된 영상의 PSNR 값은 각각 53.91dB, 54.10dB, 54.09dB, 54.13dB 이었다.

Abstract In this paper, we proposed an effective technique for hiding the watermark in the LSB of a color image by applying spatial encryption techniques. Even if the watermark hidden in the LSB of the image is extracted, the information of the extracted watermark cannot be decrypted because the watermark is encrypted using various spatial encryption techniques. Therefore, if the watermark is concealed in the LSB using the spatial encryption techniques proposed in this paper, the security is greatly improved compared to the existing technique of embedding the watermark in the LSB. When watermarking is performed by applying the proposed technique, the image quality of the watermark-concealed image is very good, so it is impossible to distinguish it from the original image, and the watermark, which is confidential data, can be extracted from the watermarked image without loss. The performance of the proposed technique was mathematically analyzed and the superiority of the proposed technique was confirmed through experiments. When the watermark was concealed by applying the proposed technique to Lenna, airplane, Tiffany, and pepper images having a size of 512x512, the PSNR values of the watermarked images were 53.91dB, 54.10dB, 54.09dB, and 54.13dB, respectively.

Key Words : Color Image, LSB, Watermark Embedding, Spatial Encryption, PSNR

1. 서론

소유권과 관련된 기밀 정보인 워터마크를 일반 사용자가 인식할 수 없도록 영상에 은닉하는 기법이 워터마킹 기법이다. 영상 워터마킹 기법에서는 기밀 데이터를 은닉한 영상의 화질이 매우 우수하게 유지되어 원본 영상과 기밀 데이터가 은닉된 영상간의 차이를 시각적으로 인식할 수 없어야 한다. 또한 기밀 데이터가 은닉된 영상으로부터 기밀 데이터를 손실 없이 추출할

This paper was supported by the Sahmyook University Research Fund in 2019.
* Division of Computer Science & Engineering, Sahmyook University(jungsm@syu.ac.kr)
Received June 16, 2020 Revised June 22, 2020 Accepted June 23, 2020

수 있어야 한다.

이러한 영상 워터마킹 기법으로 LSB에 기밀 데이터를 은닉하는 기법들이 개발되어 왔다. [1]-[7] LSB에 기밀 데이터를 은닉하는 기법은 처리 절차가 간단한 장점이 있으나, 보안에 취약한 단점이 있다.

본 논문에서는 LSB에 기밀 데이터를 은닉하는 일반적인 기법의 단점을 보완하기 위하여 다양한 공간적인 암호화 기법을 적용하여 기밀 데이터인 워터마크를 LSB에 은닉하여 보안성을 획기적으로 향상시키는 워터마킹 기법을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에 기밀 데이터를 LSB에 은닉하는 기법에 대하여 기술하였고, 3장에 공간적 암호화 기법을 적용하여 LSB에 기밀 데이터를 은닉하는 제안 기법을 기술하였다. 4장에 실험 결과를 기술하였다고, 5장에 결론을 기술하였다.

2. LSB에 기밀 데이터를 은닉하는 기법

컬러 영상의 각 픽셀은 R, G, B 성분 값을 갖는다. R, G, B 성분 값은 각각 1Byte로 표시되기 때문에 0~255사이의 값을 갖는다. LSB에 정보를 은닉하는 경우에는 R, G, B 각 성분의 LSB에 기밀 데이터의 비트들을 삽입한다. 그림 1은 흰색(R: 255, G:255, B:255)인 픽셀에 기밀 데이터 비트 101을 은닉한 경우를 보여주고 있다. 기밀 데이터의 비트가 R, G, B 성분의 LSB에 삽입됨으로 R, G, B 성분의 값이 변하게 되는데 각 성분은 평균 0.5의 차이를 갖게 된다. 이러한 차이는 시각적으로 거의 인식할 수 없기 때문에 원본 영상과 워터마크가 삽입된 영상을 시각적으로 구분하기가 거의 불가능하다. 컬러 영상에서 각 픽셀의 LSB에 기밀 데이터를 은닉하는 경우에는 그림 1에서 보는 바와 같이 각 픽셀 당 최대 3비트를 은닉시킬 수 있다. 이러한 기법은 단순하여 구현이 간단하고 기밀 데이터를 은닉하는 시간이 짧게 된다. 그러나 LSB에 기밀 데이터를 은닉하면, 기밀 데이터가 삽입 된 이미지로부터 간단히 기밀 데이터를 추출할 수 있어 기밀 데이터 보안에 문제가 발생하게 된다.

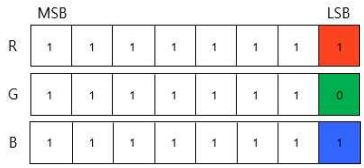


그림 1. R, G, B 성분의 LSB에 기밀 데이터 은닉
Fig. 1. Confidential data concealment in LSB of R, G, B components

3. 제안 기법

컬러 영상은 R, G, B 성분을 갖기 때문에 영상을 R, G, B 평면(plane)으로 분리할 수 있다. 각 평면에서, 워터마크 데이터 비트들이 각 픽셀의 LSB에 공간적으로 암호화 되어 저장되도록 하는 방법과 관련된 정보인 임베딩 정보를 그림 2와 같이 정의한다. 임베딩 정보는 R, G, B 평면의 최상위 행(row)에 저장되도록 한다.

Field (R plane)	Starting point		Pattern	Normal, Inverse, Skip	RGB order
	X_R	Y_R	R	R	
bits	A	B	K	3,3,3	3

Field (G plane)	Starting point		Pattern	Normal, Inverse, Skip	RGB order
	X_G	Y_G	G	G	
bits	A	B	K	3,3,3	3

Field (B plane)	Starting point		Pattern	Normal, Inverse, Skip	RGB order
	X_B	Y_B	B	B	
bits	A	B	K	3,3,3	3

그림 2 R, G, B 평면의 최상위 행에 저장되는 임베딩 정보
Fig. 2. Embedding information stored in the top row of the R, G, and B planes

그림 2의 각 필드의 의미는 다음과 같다. Starting point는 R, G, B 평면에서 워터마크 임베딩이 시작되는 X, Y 좌표를 나타낸다. X, Y 좌표를 나타내는 비트수 A, B는 식 (1), (2) 와 같이 계산된다. 식 (1), (2)에

서 사용된 W와 H는 원본 영상의 폭(W)과 높이(H)를 각각 나타낸다. 따라서 Starting point의 X 좌표는 0~(2^A-1), Y 좌표는 0~(2^B-1) 사이의 값 중에서 각각 W-1, H-1 이하의 값만을 가질 수 있다. R, G, B 평면에서 Starting point를 다르게 설정하여 각 평면에서 기밀 데이터 임베딩 시작 위치를 다르게 할 수 있다.

$$A=(int)(\log_2{}^W+0.5) \quad (1)$$

$$B=(int)(\log_2{}^H+0.5) \quad (2)$$

Normal, Inverse, Skip은 R, G, B 각 평면에 기밀 데이터 은닉 시, 기밀 데이터 비트를 반전시키지 않고 연속적으로 은닉하는 비트수와 반전하여 연속적으로 은닉하는 비트수, 기밀 데이터 비트를 은닉하지 않고 건너뛰는 픽셀 수를 각각 나타낸다. Norma, Inverse, Skip을 나타내는 비트수를 각각 3, 3, 3으로 하였기 때문에 0~7사이의 값을 갖는다. R평면에서 Normal, Inverse, Skip의 값이 2(010), 1(001), 1(001)인 경우에는 R 평면에서 임베딩 패턴을 따라 기밀 데이터 비트들을 은닉할 때 2비트는 반전시키지 않고 연속적으로 은닉하고, 1비트는 반전시켜서 은닉하고, 그 다음 위치에 있는 픽셀의 LSB에는 은닉하지 않는 형태를 반복하는 것으로 정의한다. R평면에서 Normal, Inverse 의 값이 0, 0인 경우에는 R 평면에서 기밀 데이터 비트를 반전 없이 삽입하는 것으로 정의한다.

임베딩 정보는 R, G, B 평면의 최상위 행에 저장되기 때문에 임베딩 정보가 저장되는 영역의 길이는 영상의 폭(W)과 같다. Pattern은 기밀 데이터를 임베딩하는 패턴을 나타낸다. 이 필드의 비트수 K는 식 (3)과 같이 정의된다. 따라서 임베딩 패턴은 2^K 가지를 정의할 수 있다.

$$K=(W-(A+B+12) \quad (3)$$

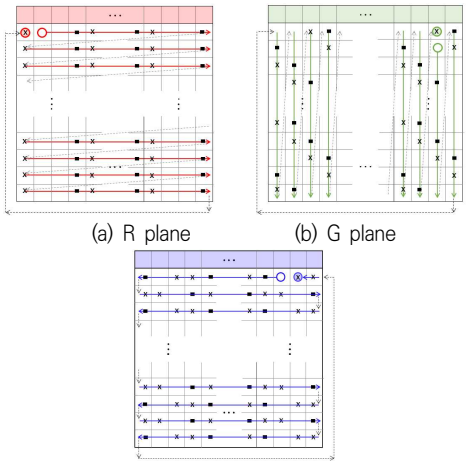
RGB order 필드는 기밀 데이터가 임베딩 되는 R, G, B 평면의 순서를 나타낸다. 0(000), 1(001), 2(010), 3(011), … , 7(111) 은 임베딩 되는 순서가 RGB, RBG, GRB, GBR, … , BGR을 나타내는 것으로 정의한다. RGB order 필드의 3비트 값은 모든 평면에 동일하게 적용된다.

임베딩 정보가 저장되는 영역은 R, G, B 평면의 최상위 행에 저장되기 때문에 나머지 영역에 기밀 데이터가 임베딩 된다. 512x512 크기의 영상인 경우에는 R, G, B 평면에서의 A, B, K는 각각 9, 9, 482가 된다.

그림 3은 R, G, B 평면에서 기밀 데이터가 임베딩 되는 패턴 3가지를 보여주고 있다. 빈 원이 임베딩이 시작되는 픽셀 위치를 나타내고, 색으로 채워진 원이 임베딩 마지막 픽셀 위치를 나타낸다. 그림 3에서 검은 사각형은 기밀 데이터 비트가 반전되어 LSB에 삽입되는 위치를 나타내고, X는 LSB에 기밀 데이터 비트를 삽입하지 않고 skip하는 픽셀 위치를 나타낸다. 아무런 표시가 없는 위치는 비 반전 상태, 즉 기밀 데이터의 비트가 그대로 해당 픽셀의 LSB에 은닉되는 위치를 나타낸다.

그림 3의 (a)와 (b)는 Normal, Inverse, Skip 값으로 2(010), 1(001), 1(001)이 적용된 경우를 보여주고 있고, (c)는 Normal, Inverse, Skip 값으로 1(001), 2(010), 2(010)가 적용된 경우를 보여주고 있다. 그림 3 (a)와 (b)에서 보는 바와 같이 임베딩 패턴을 따라 기밀 데이터의 2비트는 비 반전상태로 LSB에 은닉되고, 1비트는 반전되어 다음 위치에 은닉되고, 패턴상의 다음 1개의 픽셀에는 임베딩을 하지 않고 skip하는 형태를 반복하게 되는 것을 볼 수 있다. 임베딩 정보의 RGB order는 0의 값을 갖도록 하였다.

그림 3의 (a)에 나타낸 임베딩 패턴을 0, (b)에 나타낸 임베딩 패턴을 1, (c)에 나타낸 임베딩 패턴을 2라고 가정하면, R평면에 저장되는 임베딩 정보는 0X008040…00448이고, G평면에 저장되는 임베딩 정보는 0xFF0080…01448 이다. 그리고 B평면에 저장되는 임베딩 정보는 0xFE8040…02290이다. 이때 0X는 16진수를 나타내는 표기이며 0…0은 0이 119개 반복되는 것을 나타낸다.



(a) R plane (b) G plane

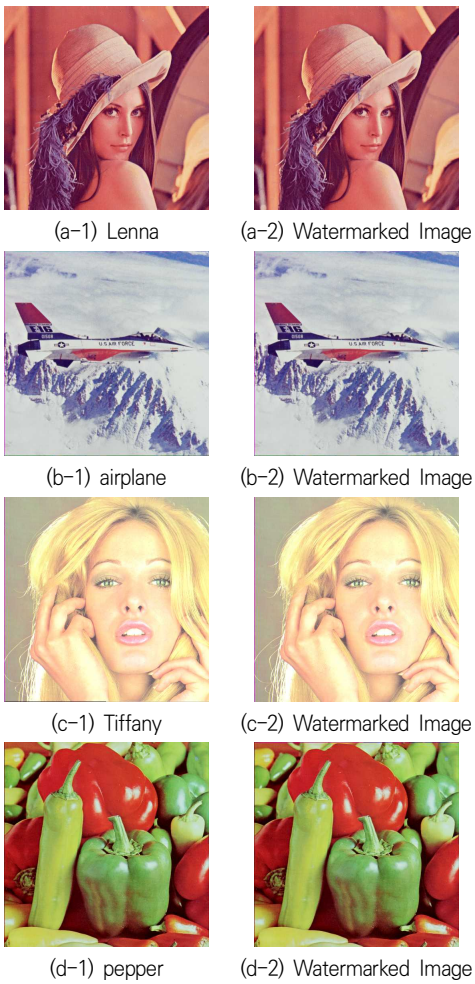
(c) B plane

그림 3 R, G, B 평면에서 기밀 데이터 임베딩의 예
Fig. 3. Examples of embedding confidential data in R, G and B planes

4. 실험 결과

512x512 크기를 갖는 Lenna, airplane, Tiffany, pepper 영상에 대하여 실험을 수행하여 제안된 기법의 성능을 확인하였다. 영상의 R,G,B 평면의 최상위 행(row)에 그림 2와 같은 임베딩 정보를 삽입하고, 임베딩 정보에 따라 나머지 영역에 기밀 데이터를 은닉하였다. R, G, B 평면의 임베딩 정보는 그림 3의 (a), (b), (c)와 동일하게 하여 실험을 수행하였다.

실험에 사용된 기밀 데이터는 본 논문의 Abstract 이며, 이를 2진 파일로 변환한 결과를 임베딩 정보에 따라 영상의 LSB에 반복적으로 은닉하였다. 그림 4는 실험에 사용된 원본 영상과 기밀 데이터가 은닉된 결과 영상을 보여주고 있다. 제안된 기법에 따라 Lenna, airplane, Tiffany, pepper 영상에 대하여 워터마킹을 수행한 결과 영상인 기밀 데이터가 은닉된 영상의 PSNR 값은 각각 53.91dB, 54.10dB, 54.09dB, 54.13dB 이었다. 그림 4에서 보는 바와 같이 각 원본 영상에 기밀 데이터를 은닉하면, 기밀 데이터가 은닉된 영상의 화질이 매우 뛰어나 원본 영상과의 구분이 시각적으로는 거의 불가능하다. 또한 은닉되어 있는 기밀 데이터는 다양한 공간적인 암호화 기법들을 사용하여 암호화 되어 있기 때문에 보안성이 매우 높다.



(a-1) Lenna (a-2) Watermarked Image

(b-1) airplane (b-2) Watermarked Image

(c-1) Tiffany (c-2) Watermarked Image

(d-1) pepper (d-2) Watermarked Image

그림 4. 원본 영상과 기밀데이터가 은닉된 영상
Fig. 4. Cover images & watermarked images

기밀 데이터가 은닉된 영상의 RGB 평면에서 각 픽셀의 LSB에 은닉되어 있는 비트들을 추출하여 각 평면의 임베딩 정보를 구성하고, 구성된 임베딩 정보에 따라 기밀 데이터가 손실 없이 복원된다.

5. 결론

본 논문에서는 공간적 암호화 기법, 선택적인 비반전/반전/skip 기법, 컬러 평면의 임베딩 순서 변환 기법 등을 적용하여 기밀 데이터인 워터마크를 영상에 은닉하는 보안이 우수한 워터마킹 기법을 제안하였다.

제안기법을 적용하여 워터마크를 컬러 영상에 은닉하면 워터마크가 안전하게 저장되어 보안성이 높게 유지되고, 기밀 데이터인 워터마크를 손실 없이 복원할 수 있다.

제안 기법을 512x512 크기를 갖는 Lenna, airplane, Tiffany, pepper 영상에 적용하여 기밀 데이터를 은닉한 경우, 워터마크가 은닉된 영상의 PSNR 값은 40dB보다 큰 53.91dB, 54.10dB, 54.09dB, 54.13dB 이었다. 따라서 워터마크가 은닉된 영상과 원본 영상의 구분이 시각적으로 거의 불가능하기 때문에 기밀 데이터를 일반 사용자가 인지 할 수 없게 된다. 비록 워터마크가 은닉된 영상의 LSB에서 기밀 데이터를 얻어도 다양한 공간적인 암호화 기법들을 적용하여 암호화 되어 있기 때문에 기밀 데이터의 보안이 매우 높게 유지될 수 있다.

제안기법을 적용하여 기밀 데이터를 은닉하면 최대 {(H-1)·W}x3 비트를 은닉할 수 있다. H와 W는 영상의 높이와 너비를 각각 나타낸다. 본 실험에 사용된 컬러 영상에서는 최대 784,896비트를 은닉할 수 있다.

제안된 기법의 임베딩 정보를 사용하여 워터마킹을 수행한 후 워터마크가 은닉된 이미지의 LSB에서 데이터를 추출하여 임베딩 정보를 구성하고 구성된 임베딩 정보를 사용하여 기밀 데이터를 손실 없이 추출할 수 있다. 따라서 제안된 기법은 기밀 데이터인 워터마크를 은닉하는 다양한 응용에 효과적으로 사용 될 수 있다.

REFERENCES

[1] H. C. Huang, C. M. Chu, J. S. Pan, "The optimized copyright protection system with genetic watermarking", Soft Computing, Vol. 13, No. 4, pp. 333-343, October, 2009.

[2] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, "Reversible data hiding", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 16, No. 3, pp. 354-362, March, 2006.

[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.

[7] T. Halder, S. Karforma, R. 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, April, 2019.

저자약력

정수목(Soo-Mok Jung) **[종신회원]**

- 1984: 경북대학교 전자공학 공학사
- 1986: 경북대학교 대학원 전자공학 공학석사
- 2002: 고려대학교 대학원 컴퓨터학 이학박사
- 현 재: 삼육대학교 컴퓨터학부 교수

〈관심분야〉 멀티미디어, 영상처리