한국정보전자통신기술학회논문지(jkiiect)'20-12, Vol.13 No.6
논문 20-13-06-503 http://dx.doi.org/10.17661/jkiiect.2020.13.6.503

다중 암호화 기법을 적용한 영상 워터마킹 기법

정수목*

Image watermarking technique applying multiple encryption techniques

Soo-Mok Jung*

요 약 본 논문에서는 다중으로 암호화한 워터마크를 영상 픽셀의 LSB에 은닉하여 워터마크의 보안성을 크게 향상시키는 효과적인 기법을 제안하였다. 영상 픽셀의 LSB에 은닉되어 있는 다중 암호화된 워터마크를 추출하여도 이를 해독하는 것이 불가능하기 때문에 워터마크의 보안성이 매우 높게 유지된다. 제안된 기법을 사용하여 워터마크를 다중으로 암호화하여 영상에 은닉하면, 워터마크가 은닉된 영상의 시각적 화질이 매우 높아 원본 영상과 워터마크가 은닉된 결과 영상의 구별이 불가능하다. 워터마크를 다중으로 암호화하여 원본 영상에 은닉한 결과 영상으로부터, 제안 기법의 절차를 따라 원본 워터마크 데이터를 손실 없이 온전히 추출할 수 있다. 제안된 기법의 성능을 수학적으로 분석하고 제안된 기법의 우수성을 실험을 통하여 확인하였다. 제안된 기법은 기존의 기법에 비하여 영상에 은닉된 워터마크의 보안성을 크게 향상시킨 우수한 영상 워터마킹 기법이다.

Abstract In this paper, we proposed an effective technique that greatly improves the security of the watermark by concealing the multiple-encrypted watermark in the LSB of the image pixel. Even if multiple encrypted watermark hidden in the LSBs of an image pixel are extracted, it is impossible to decrypt them, so the security of the watermark is maintained very high. If the watermark is multiple encrypted and hidden in the image using the proposed technique, the visual quality of the watermark-hidden image is very high, making it impossible to distinguish between the original image and the resulting image in which the watermark is hidden. The original watermark data can be completely extracted without loss, according to the procedure of the proposed technique, from the resulting image that the watermark is encrypted and hidden in the original image. The performance of the proposed technique was analyzed mathematically and the superiority of the proposed technique was confirmed through experiments. The proposed technique is an excellent image watermarking technique that greatly improves the security of the watermark hidden in the image compared to the existing technique.

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

1. 서론

영상의 저작권 관련 기밀 정보인 문자, 그림, 기호 등의 디지털 워터마크를 일반 사용자가 인식할 수 없도록 영상에 은닉하는 기법이 영상 워터마킹 기법이다. 영상 워터마킹 기법에서는 워터마크가 은닉된 영상의 화질이 우수하여 원본 영상과 워터마크가 은닉된 영상 간의 차이를 시각적으로 구별 할 수 없어야 하고, 워터마크가 은닉된 영상으로부터 워터마크를 손실 없이 추출할 수 있어야 한다.

영상 워터마킹 기법으로 영상 픽셀의 LSB에 워터마크 데이터의 비트들을 은닉하는 기법들이 개발되어 왔다 [1]-[4]. 영상 픽셀의 LSB에 워터마크 비트들을 은

* Division of Computer Science & Engineering, Sahmyook University
Received December 04, 2020 Revised December 04, 2020 Accepted December 15, 2020

닉하는 기법은 절차가 단순한 장점이 있으나, 영상 픽셀의 LSB에 은닉되어 있는 워터마크의 비트들을 추출하여 워터마크를 구성할 수 있어 보안에 취약한 단점이 있다.

또한 절차가 복잡하고 워터마킹에 적용할 수 있는 영상에 제약이 있는 가역 워터마킹 기법들이 제안되었고 [5]-[7], 최근에는 본 연구팀에서 제안한 가역 워터마킹 기법이 있다 [8].

본 논문에서는 워터마크를 다중으로 암호화하여 영상 픽셀의 LSB에 은닉하는 기법을 제안하였다. 제안된 기법은 본 연구팀에서 제안한 기법들을 개선하여 발전시킨 기법이다 [9]-[11]. 제안된 기법은 영상에 은닉되는 워터마크의 보안성을 획기적으로 향상시킨 효과적인 영상 워터마킹 기법이다.

본 논문의 구성은 다음과 같다. 2장에 워터마크 데이터를 영상 픽셀의 LSB에 은닉하는 기법에 대하여 기술하고, 3장에 워터마크의 데이터를 다중으로 암호화 하여 영상 픽셀의 LSB에 은닉하는 제안 기법을 기술하였다. 4장에 실험 결과를 기술하였다. 그리고 5장에 결론을 기술하였고, 6장에 향후 연구에 대하여 기술하였다.

2. LSB에 워터마크를 은닉하는 기법

컬러 영상의 각 픽셀은 R, G, B 성분 값들로 구성된다. R, G, B 성분 값은 각각 1바이트로 표시되기 때문에 0~255사이의 값을 갖고, 1개의 픽셀은 3바이트로 구성된다. 워터마크를 LSB에 은닉하는 경우에는 R, G, B 각 성분의 LSB에 워터마크 데이터의 비트들을 삽입한다. 그림 1은 흰색(R: 255, G:255, B:255)인 픽셀에 기밀 데이터인 워터마크 데이터의 비트 “110”을 은닉한 경우를 보여주고 있다. 워터마크 데이터의 비트가 R, G, B 성분의 LSB에 삽입됨으로 R, G, B 성분의 값이 미세하게 변하게 된다. 그림 1에서 R, G, B 성분의 값이 각각 255, 255, 254가 된 것을 볼 수 있다. 이러한 미세한 차이는 각 성분 별로 평균 0.5가 된다. 각 성분의 미세한 차이 때문에 발생하는 픽셀의 컬러 변화를 시각적으로는 거의 인식할 수 없게 된다. 따라서 원본 영상과 워터마크가 은닉된 영상을 시각적으로 구분하는 것은 불가능하다.

컬러 영상의 각 픽셀의 LSB에 워터마크 데이터를 은닉하는 경우에는 그림 1에서 보는 바와 같이 각 픽셀 당 최대 3비트를 은닉시킬 수 있다. 이러한 기법은 단순하기 때문에 구현이 간단하다. 그러나 LSB에 워터마크 데이터를 은닉하면, 워터마크가 삽입된 이미지로부터 간단히 워터마크를 추출할 수 있다. 따라서 영상 픽셀의 LSB에 기밀 데이터를 은닉하는 기법을 사용하면 워터마크의 보안에 문제가 발생하게 된다.

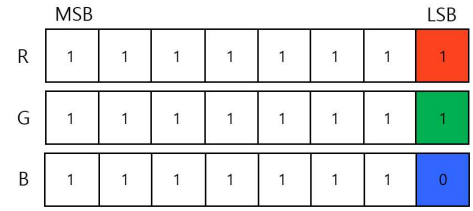


그림 1. R, G, B 성분의 LSB에 기밀 데이터 은닉
Fig. 1. Confidential data concealment in LSBs of R, G, B components

3. 제안 기법

컬러 영상의 각 픽셀은 R, G, B 성분을 갖기 때문에 컬러 영상을 R, G, B 평면(plane)으로 분리할 수 있다. 각 평면에서 워터마크 데이터의 비트들을 각 픽셀의 LSB에 다중으로 암호화하여 은닉함으로 워터마크의 보안성을 획기적으로 높이는 제안기법에서는 워터마크 데이터를 식 (1)과 같이 두 개의 암호화 키(Key) K1, K2를 사용하여 암호화 한다. K1과 K2는 각각 8비트를 갖는 값이다. 식 (1)에서 사용된 기호는 비트별 배타적 논리합(exclusive-OR, XOR)과 나머지 연산(mod)을 나타내는 기호들이다.

$$ED = D \ XOR \ (K1 \ mod \ K2) \qquad (1)$$

암호화된 워터마크 데이터 ED를 원본 영상의 LSB에 다양한 공간적인 암호화 기법을 사용하여 은닉하기 위한 삽입 정보(embedding information)를 표 1과 같이 정의한다. 표 1에 나타난 삽입 정보는 R, G, B 평면의 최상위 행(row)에 저장되기 때문에 삽입 정보가 저장되는 영역의 길이는 영상의 폭(W)과 같게 된다.

표 1. R, G, B 평면의 최상위 행에 저장되는 삽입 정보
Table 1. Embedding information stored in the top row of the R, G, and B planes

Field (R)	F_R	Key		Starting point		Pattern	Normal Inverse Skip	RGB order
		$K1_R$	$K2_R$	X_R	Y_R	P_R	NIS_R	RGB_R
bits	7	8	8	A	B	C	3,3,3	3

Field (G)	F_G	Key		Starting point		Pattern	Normal Inverse Skip	RGB order
		$K1_G$	$K2_G$	X_G	Y_G	P_G	NIS_G	RGB_G
bits	7	8	8	A	B	C	3,3,3	3

Field (B)	F_B	Key		Starting point		Pattern	Normal Inverse Skip	RGB order
		$K1_B$	$K2_B$	X_B	Y_B	P_B	NIS_B	RGB_B
bits	7	8	8	A	B	C	3,3,3	3

표 1의 각 필드(field)의 의미는 다음과 같다.

Key 필드의 K1, K2는 식 (1)에서 사용된 암호화키를 나타낸다.

Starting point 필드는 R, G, B 평면에서 암호화된 워터마크가 다시 공간적으로 암호화 되어 픽셀에 은닉되는 시작 위치의 X, Y 좌표를 나타낸다. X, Y 좌표를 나타내는 비트수 A, B는 식 (2), (3)과 같이 계산된다. 식 (2), (3)에서 사용된 W와 H는 원본 영상의 폭(W)과 높이(H)를 각각 나타내고, 수식에서 사용된 기호는 천장 함수(ceiling function)를 나타내는 기호이다. 따라서 시작 위치(starting point)의 X 좌표는 $0\sim(2^A-1)$, Y 좌표는 $0\sim(2^B-1)$ 사이의 값 중에서 각각 W-1, H-1 이하의 값만을 가질 수 있다. R, G, B 평면에서 시작 위치를 다르게 설정하여 각 평면에서 암호화된 워터마크 데이터를 공간적으로 암호화하여 은닉하는 시작 위치를 다양하게 지정할 수 있다.

$$A=\lceil \log_2{}^W \rceil \quad (2)$$

$$B=\lceil \log_2{}^H \rceil \quad (3)$$

Normal/Inverse/Skip 필드는 해당 평면에서 암호화된 워터마크 데이터를 은닉 하는 형태를 나타낸다. Normal은 암호화된 워터마크 데이터의 비트를 반전시키지 않고 그대로 연속적으로 은닉하는 비트수를 나타낸다. Inverse는 암호화된 워터마크 데이터의 비트를 반전시켜 연속적으로 은닉하는 비트수를 나타낸다. Skip은 암호화된 워터마크 데이터의 비트를 은닉하지 않고 건너뛰는 픽셀 수를 나타낸다. Normal/Inverse/Skip을 나타내는 비트수를 모두 3비트로 하였기 때문에 Normal/Inverse/Skip은 0~7 사이의 정수 값을 갖는다. 그리고 Normal과 Inverse 값이 모두 0인 경우에는 해당 평면의 은닉 패턴에 따라 암호화된 워터마크 데이터의 비트를 반전 없이 은닉하는 것으로 정의 한다.

Pattern 필드는 암호화된 워터마크 데이터를 은닉하는 패턴을 나타낸다. 이 필드의 비트가 C비트인 경우에는 은닉 패턴은 2^C가지 정의 될 수 있다. 은닉 패턴을 나타내는 Pattern 필드의 비트수 C는 W-(A+B+35)가 된다.

RGB order 필드는 기밀 데이터가 임베딩 되는 R, G, B 평면의 순서를 나타낸다. 따라서 RGB order 필드의 비트수는 $\lceil \log_2{}^6 \rceil$=3이 된다. RGB order 필드가 3비트로 구성되기 때문에 RGB order는 0(000), 1(001), 2(010), 3(011), ... , 7(111)의 값을 가질 수 있지만, 0(000)부터 5(101)까지의 값만을 사용한다. 이 값들은 각 평면이 임베딩 되는 순서를 나타내며, 이 값들은 차례대로 RGB, RBG, GRB, GBR, BRG, BGR을 나타내는 것으로 정의한다. RGB order 필드의 3비트 값은 모든 평면에 동일하게 적용된다.

표 1의 첫 번 째 필드인 F(Format) 필드는 뒤에 있는 5개의 필드(Key, Starting point, Pattern, Normal/Inverse/Skip, RGB order)가 최상위 행에 삽입 정보로 저장되는 배열 순서를 나타낸다. 따라서 가능한 배열의 경우는 총 5!=120가지가 된다. 그러므로 F 필드의 길이는 $\lceil \log_2{}^{120} \rceil$ = 7비트가 된다. 삽입 정보가 저장될 때, 각 평면의 최상위 행에 F 필드 7비트가 먼저 저장되고 나머지 5개의 필드는 F 필드에서 정해진 순서대로 저장된다.

표 1의 삽입 정보는 영상의 각 평면의 최상위 행(row)에 저장되기 때문에, 삽입 정보가 저장되는 최상위 행을 제외한 나머지 영역에 암호화된 워터마크 데

이터 비트들이 다양하게 공간적으로 암호화되어 저장된다. 따라서 512x512 크기를 갖는 영상에서는 각 평면별로 암호화된 워터마크 데이터 비트들이 최대 261,632(511x512)비트 저장될 수 있고, 영상 전체에는 784,896비트가 저장될 수 있다. 그리고 표 1의 삽입 정보의 Starting point 필드와 Pattern 필드의 A, B, C는 각각 9비트, 9비트, 459비트가 된다.

그림 2는 R, G, B 각 평면에서 암호화된 워터마크 데이터가 다양하게 공간적으로 암호화 되어 은닉되는 3가지의 경우를 보여주고 있다. 그림 2는 표 1의 삽입 정보에서 Starting point, Pattern, Normal /Inverse/Skip 필드의 값에 따른 다양한 경우를 각각 보여 주고 있다.

그림 2에서 검은 사각형은 암호화된 워터마크의 데이터 비트가 반전되어 LSB에 삽입되는 위치를 나타낸다. 그리고 X로 표시된 위치는 픽셀의 LSB에 암호화된 워터마크의 데이터 비트를 은닉하지 않고 건너뛰는 픽셀 위치를 나타낸다. 검은 사각형이나 X가 표시되지 않은 위치는 암호화된 워터마크의 데이터 비트를 변경하지 않고 그대로 픽셀의 LSB에 은닉하는 위치를 나타낸다.

워터마크가 다중으로 암호화되어 은닉되기 시작하는 위치를 외곽선만 있는 단순 원으로 표기하였고, 마지막 위치는 색깔이 채워진 원으로 표기하였다.

그림 2는 R, G, B 평면의 최상위 행에 저장되는 삽입 정보인 Pattern 필드에서 지정된 은닉 패턴이 (a), (b), (c)의 형태와 같다고 가정하였다. 그림 2 (a)는 Normal/Inverse/Skip 필드의 값이 1(001)/1(001)/2(010)이고 Starting point 필드의 값 (X, Y)가 (1, 1) 로 설정된 경우에 암호화된 워터마크의 데이터 비트들이 은닉되는 예를 보여주고 있다. (b)는 Normal/Inverse/Skip 필드의 값이 1(001)/2(010)/1(001)이고 Starting point 필드의 값 (X, Y)가 (510, 2)로 설정된 경우의 예를 보여 주고 있다. (c)는 Normal/Inverse/Skip 필드의 값이 2(010)/2(010)/0(000)이고 Starting point 필드의 값 (X, Y)가 (509, 1)로 설정된 경우의 예를 보여주고 있다. 그림 2는 임베딩 정보의 RGB order필드가 0(000)의 값을 갖는 것으로 가정하여, 암호화된 워터마크 데이터 비트가 RGB 순으로 은닉되는 것을 가정하였다.

Normal/Inverse/Skip 필드의 값이 1(001)/1(001)/2(010)로 설정된 그림 2 (a)에서 기밀 데이터인 워터마크가 삽입되는 형태는 다음과 같다. Starting point 필드의 값 (X, Y)가 (1, 1)이기 때문에 기밀 데이터 은닉 시작 위치가 (1, 1)이 된다. Pattern 필드에서 지정된 은닉 패턴상의 픽셀 위치를 시작점부터 순차적으로 진행하면서, 암호화된 워터마크 데이터의 1 비트는 반전시키지 않고 (1, 1) 위치에 있는 픽셀의 LSB에 은닉하고, 다음 1 비트는 반전시켜서 (2, 1)위치에 있는 픽셀의 LSB에 은닉한다. 그 후 (3, 1), (4, 1)위치의 픽셀에는 암호화된 워터마크 데이터 비트를 은닉하지 않고 건너뛰게 된다. 그 뒤 (5, 1) 위치의 픽셀부터는 위의 과정을 반복한다. 마지막으로 (509, 511)위치에 있는 픽셀의 LSB에 암호화된 워터마크 데이터 1비트가 반전되지 않고 그대로 은닉되고, (510, 511)위치에 있는 픽셀의 LSB에는 암호화된 워터마크 데이터 1 비트가 반전되어 은닉된다. 그리고 (511, 511)위치와 (0, 1)위치에 있는 픽셀의 LSB에는 암호화된 워터마크 데이터 비트가 은닉되지 않고 R 평면에서의 은닉과정이 종료된다.

영상의 크기가 512x512이고, 그림 2 (a), (b), (c)에 나타낸 은닉 패턴을 각각 0, 1, 2라고 가정하고, 각 평면에서 삽입 정보의 F 필드 값이 0이어서 표 1에 표시된 삽입 정보의 필드들이 순서대로 저장된다고 가정하고, Key 필드의 K1이 255이고 K2가 0이라고 가정하고, RGB order 필드가 0의 값을 갖는 것으로 하여 RGB평면 순으로 다중으로 암호화된 워터마크 데이터가 은닉된다고 가정하면, RGB 각 평면의 최상위 행에 저장되는 512비트의 임베딩 정보는 0X01FE0001008 0...0250, 0X01FE01FE0100..028,0X01FE01FD0080..0480이 된다. 여기서 0X는 16진수 표기임을 나타내고, 0..0은 0이 114개 반복되는 것을 나타낸다.

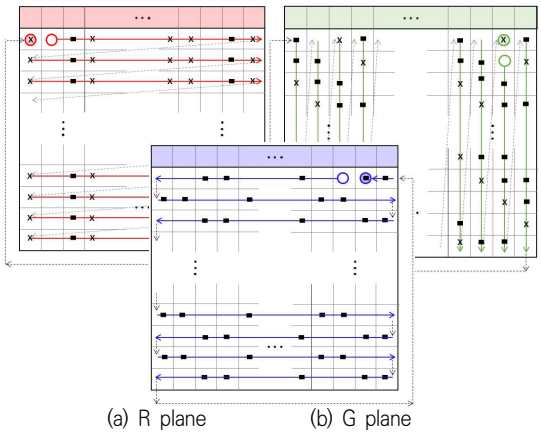


그림 2 RGB평면에서 워터마크 데이터 임베딩의 예
Fig. 2. Examples of embedding watermark data in R, G, and B planes

4. 실험 결과

제안된 기법의 성능을 측정하기 위하여 실험에 사용된 영상은 512x512 크기를 갖는 Lenna, sailboat, pepper, Tiffany 영상이다. 본 논문의 Abstract를 이진 파일로 변환한 결과를 기밀 데이터인 워터마크로 사용하였고, 이를 제안된 기법의 절차에 따라 다중으로 암호화하여 원본 영상에 은닉하였다. 각 원본 영상의 R, G, B 평면의 최상위 행에 있는 픽셀들의 LSB에 그림 2와 같은 삽입 정보를 은닉하였다. 이 때 F 필드의 값은 000으로 하여 표 1의 삽입 정보의 필드들이 순서대로 은닉되도록 하였다.

최상위 행을 제외한 나머지 영역에 기밀 데이터인 워터마크 데이터들을 다중으로 암호화하여 원본 영상에 은닉하였다. 이 때 RGB 평면별 삽입 정보의 각 필드들의 값은 그림 2 (a), (b), (c)와 동일하게 하여 실험을 수행하였고, RGB order는 0으로 하여 워터마크가 은닉되는 평면의 순서가 RGB 순이 되도록 하였다.

표 2는 제안된 기법을 사용하여 기밀 데이터를 은닉할 때, Normal/Inverse/Skip 필드의 Skip 값에 따라 영상에 은닉되는 기밀 데이터 비트 수와 PSNR 값을 나타낸다. 표 2에서 사용된 기호 N_0 는 Normal/Inverse/Skip 필드의 Skip 값이 0인 경우, 실험 영상에 은닉되는 기밀 데이터 비트수를 나타낸다. N_0를 (Normal+Inverse+Skip) 으로 나눈 값을 r로 표기하였다. (Normal+Inverse+Skip)은 Normal/Inverse/Skip 필드의 각 값을 더한 값을 나타낸다. 표 2에서 사용된 ⌊ ⌋ 기호는 바닥 함수(floor function)를 나타내고, ⌈ ⌉는 천장 함수(ceiling function)를 나타낸다. 표 2에서 $\lceil\ \rceil_{\max\le(N+I)}$는 천장 함수의 값이 (N+I)를 초과하는 경우에는 (N+I)로 대체하는 경우를 나타낸다. 표 2에서 보는 바와 같이, Normal/Inverse/Skip필드의 Skip 값이 0인 경우에는 은닉 가능한 최대 기밀 데이터가 261,632x3비트가 된다.

결과영상의 화질을 평가하기 위한 PSNR은 식(4), (5)를 사용하여 측정하였다. 식 (5)에 표시된 I, O는 원본 영상과 워터마크가 은닉된 결과 영상을 각각 나타낸다.

$$PSNR = 10\log_{10}(255^2/MSE) \quad (4)$$

$$MSE = (1/\sum_{i=0}^{H-1}\sum_{j=0}^{W-1} [I(y,x) - O(y,x)]^2 \quad (5)$$

워터마크가 다중으로 암호화되어 각 픽셀의 LSB에 저장 될 때에는 최상위 행에 있는 픽셀들을 제외한 나머지 영역에 있는 픽셀들에 기밀 데이터가 은닉된다. 따라서 영상의 크기가 증가할수록 은닉되는 비트와 픽셀의 LSB의 값이 일치하는 확률은 50%로 수렴하게 되어 각 픽셀 당 평균적인 차이는 0.5가 된다. 따라서 Skip값이 0인 경우, 워터마크가 삽입된 결과 영상의 PSNR 값은 54.151dB에 수렴하는 값을 갖게 된다.

Skip 값이 증가할수록 MSE 값이 감소하게 되어 PSNR 값은 증가하게 되지만, 영상에 은닉되는 다중으로 암호화된 워터마크의 데이터 비트 수는 감소하게 된다. 따라서 Skip 값을 사용하여 은닉되는 기밀 데이터 비트 수와 결과 영상의 화질을 미세하게 조절할 수 있다. 표 2에서 사용된 D는 Normal/Inverse/Skip 값에 따라 영상의 픽셀에 기밀 데이터가 은닉될 때, 기밀 데이터의 LSB와 각 픽셀의 LSB와의 평균 차이를 나타낸다.

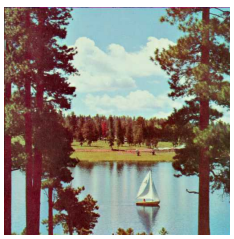
표 2. Skip 값에 따른 은닉되는 기밀 데이터 비트 수와 PSNR 값
Table 2. The embedded confidential data bits and PSNR values according to the Skip values

Skip	은닉되는 기밀 데이터 비트 수 N_S (S: 0~7)	PSNR(dB)
0	N_0=261,632*3	54.151
1~7	$N_{1\sim7}=\lfloor r \rfloor*(N+I)+\lceil (r-\lfloor r \rfloor)*(N+I) \rceil_{max<=(N+I)}$	$10\log_{10}(255^2/MSE)$ $MSE=(N_{1\sim7}+W)*D^2/H$ W


(a-1) Lenna

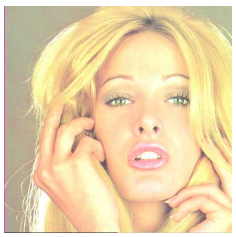

(b-2) Watermarked Image


(b-1) sail-boat


(b-2) Watermarked Image


(c-1) pepper


(c-2) Watermarked Image


(d-1) Tiffany


(d-2) Watermarked Image

그림 3. 원본 영상과 기밀데이터가 은닉된 영상
Fig. 3. Cover images & watermarked images

그림 3은 실험에 사용된 원본 영상과 워터마크가 다중으로 암호화되어 원본 영상에 은닉된 결과 영상을 보여주고 있다. 제안된 기법에 따라 워터마크를 다중으로 암호화하여 원본 영상인 Lenna, sailboat, pepper, Tiffany에 은닉하면 결과 영상의 PSNR 값은 각각 54.144dB, 54.149dB, 54,161, 54.126B이었다.

일반적으로 원본 영상에 대하여 어떤 처리를 한 결과 영상의 PSNR 값이 40dB 이상이 되면, 인간의 시각으로는 결과 영상과 원본 영상의 차이를 구분할 수 없게 된다. 따라서 제안된 기법으로 워터마크를 다중으로 암호화하여 영상에 은닉하면 워터마크가 은닉된 결과 영상의 PSNR 값은 40dB보다 큰 값을 갖게 되어 원본 영상과 워터마크가 은닉된 결과 영상의 차이를 시각적으로 구분 할 수 없게 된다.

그림 3에서 보는 바와 같이 제안된 기법에 따라 각 원본 영상에 워터마크를 은닉하면, 워터마크가 은닉된 결과 영상의 화질이 매우 뛰어나 원본 영상과의 구분이 불가능하다. 워터마크를 다중으로 암호화하여 은닉한 결과 영상의 RGB 평면에서 각 픽셀의 LSB로부터, 은닉되어 있는 비트들을 추출한 후 각 평면의 삽입 정보를 구성하고, 구성된 삽입 정보에 따라 기밀 데이터인 워터마크를 손실 없이 복원할 수 있다.

제안된 기법에서는 워터마크를 다중으로 암호화하여 영상에 은닉하였기 때문에 워터마크 보안성이 획기적으로 향상 된다.

5. 결론

본 논문에서는 기밀 데이터인 워터마크를 다중으로 암호화하여 영상에 은닉하는 기법을 제안하였다. 제안 기법에서는 Key 필드의 K1, K2를 사용하여 기밀 데이터인 워터마크를 암호화한다. 암호화된 워터마크를 Starting point 정보, Pattern 정보, Normal/Inverse/Skip 정보, 컬러 평면의 임베딩 순서를 나타내는 RGB order 정보, F(Format) 정보를 사용하여 영상의 각 평면에 공간적으로 암호화하여 은닉한다.

제안기법에서는 다음과 같이 7회에 걸쳐 워터마크 데이터를 다중으로 암호화하여 영상에 은닉하기 때문

에 보안성이 획기적으로 향상되게 된다. 워터마크 데이터를 식 (1)과 같이 암호화 하고, 암호화된 워터마크 데이터를 각 컬러 평면에서 2^{459} 가지 중의 하나의 은닉 패턴에 따라 공간적으로 암호화하여 은닉하고, Normal/Inverse/Skip 필드의 값을 사용하여 추가적으로 공간적인 암호화기법으로 은닉하고, 은닉되는 RGB 평면 순서를 지정하여 다중으로 암호화된 워터마크 데이터를 정해진 순서대로 은닉하고, 은닉과 관련된 임베딩 정보의 필드들의 순서를 결정하는 F(Format) 필드를 사용하여 삽입 정보를 암호화하기 때문에 영상에 은닉되는 기밀 데이터인 워터마크의 보안성이 획기적으로 향상된다.

제안된 기법을 사용하여 워터마크를 영상에 은닉하면, 비록 워터마크가 은닉된 영상의 LSB에서 워터 마크 데이터를 획득해도 워터마크를 다중으로 암호화하였기 때문에 기밀 데이터인 워터마크의 해독은 불가능하여 워터마크의 보안성이 획기적으로 향상된다. 워터마크가 은닉된 영상의 LSB에서 비트들을 추출하여 삽입 정보를 구성하고, 구성된 삽입 정보를 사용하여 원본 워터마크를 손실 없이 추출할 수 있다. 제안된 기법을 사용하여 은닉할 수 있는 최대 기밀 데이터 비트수는 {(H-1)·W}x3 비트가 된다. 표 2에서 보는 바와 같이 Normal/Inverse /Skip 필드의 Skip 값을 사용하여 영상에 은닉되는 기밀 데이터 비트수와 PSNR 값을 정밀하게 조절 할 수 있다.

512x512 크기를 갖는 Lenna, sailboat, pepper, Tiffany 영상에 제안 기법을 적용하여 워터마크를 다중으로 암호화하여 은닉한 경우, 워터마크가 은닉된 영상의 PSNR 값은 40dB보다 훨씬 큰 54.144dB, 54.149dB, 54,161, 54.126dB이었다. 따라서 워터마크가 은닉된 결과 영상과 원본 영상을 사람의 시각으로는 구분이 불가능하기 때문에 영상에 워터마크가 은닉되어있는지 여부를 일반 사용자가 인지 할 수 없게 된다.

제안된 기법은 기밀 데이터인 워터마크를 은닉하여 소유권을 안전하게 보호할 수 있기 때문에 그림, 만화, 애니메이션 등 다양한 응용분야에 효과적으로 사용될 수 있다.

6. 향후 연구

제안된 기법은 워터마크를 다중으로 암호화하여 픽셀의 LSB에 은닉하기 때문에 은닉된 워터마크의 보안성을 획기적으로 향상시키는 기법이다. 비록 워터마크가 은닉된 영상의 LSB에서 워터마크 데이터를 획득해도 워터마크를 다중으로 암호화하였기 때문에 기밀 데이터인 워터마크의 해독은 불가능하여 은닉된 워터마크의 보안성이 획기적으로 향상된다.

이러한 큰 장점이 있지만, 모자이크 공격이나 가우시안 노이즈 공격에 의하여 워터마크가 삽입된 영상이 변형될 경우에는 원본 워터마크를 온전히 추출할 수 없는 한계가 있다. 외부 공격에 대한 방어대책은 향후 연구에서 수행하고자 한다.

REFERENCES

[1] 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.

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

[3] 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.

[4] 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.

[5] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, "Reversible data hiding", IEEE Trans. Circuits Syst. Video Technol. Vol. 16, pp. 354-362, 2006,

[6] X. Li, J. Li, B. Li, B. Yang, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion", Signal Process. Vol. 93, pp. 198-205, 2013.

[7] S. Arunkumar, V. Subramaniyaswamy, N. Sivarama krishnan, "Reversible Data Hiding scheme using m

odified Histogram Shifting in Encrypted Images for Bio-medical images. Int. J. Pure Appl. Math. Vol. 119, pp. 13233-13240, 2018.
[8] S. M. Jung, B. W. On, "An Advanced Reversible Data Hiding Algorithm Using Local Similarity, Curved Surface Characteristics, and Edge Characteristics in Images", Applied Sciences, Vol. 10, No. 3, pp. 836-860, 2020.
[9] 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.
[10] S. M. Jung, "A technique of embedding confidential data in images by applying encryption and spatial encryption techniques", KIIECT Summer Conference 2020.
[11] S. M. Jung, "An improved technique to hide confidential data in image", KIIECT Winter Conference 2020.

저자약력

정 수 목(Soo-Mok Jung) **[종신회원]**

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

관심분야: 영상처리, 컴퓨터 아키텍쳐
E-mail: jungsm@syu.ac.kr