Gram-Schmidt 직교화를 이용한 다중 워터마킹 기법

오윤희*, 이혜주**, 박지환***
*부경대학교 전산정보학과
**한국정보통신대학원대학교 암호 및 정보보안연구실
***부경대학교 컴퓨터멀티미디어공학전공
e-mail:yhoh@mail1.pknu.ac.kr

Multiple Watermarking Using Gram-Schmidt Orthogonalization

Yun-Hee Oh*, Hye-Joo Lee**, Ji-Hwan Park***
*Dept of Computer & Information Science, Pukyoung Nat'l University
**Cryptology & Information Security Lab., Information & Communications University
***Dept of Computer & Multimedia Engineering, Pukyoung Nat'l University

요약

다중 워터마킹은 하나의 컨텐츠에 2개 이상의 다른 워터마크를 삽입하는 것으로 각 워터마크는 유일한 키로 정확하게 추출할 수 있어야 한다. 대역확산법(spread spectrum)을 이용한 다중 워터마킹은 삽입되는 워터마크간의 직교성(orthogonality)이 제공되어야 삽입된 워터마크들의 정확한 추출이 가능하다. 랜덤계열과 Hadamard 계열을 이용한 기존의 방법은 직교성이 보장되지 않기 때문에 워터마크가 정확히 추출되지 않는 문제가 발생한다. 따라서, 본 논문에서는 랜덤계열들을 Gram-schmidt 직교화 과정을 이용하여 직교화시킨 후, 직교화된 랜덤계열로 워터마크를 삽입하여 정확한 추출이 가능한 방법을 제안하였다.

1. 서론

멀티미디어 산업의 발전과 인터넷과 같은 네트워크 기술의 보편화로 인해 음성, 영상, 동영상 등의 디지털화된 멀티미디어 컨텐츠의 수요가 급격하게 증가하고 있다. 디지털 멀티미디어 컨텐츠의 네트워크를 이용한 불법 복사 및 변조 등은 저작권 침해라는 문제를 야기시킴에 따라 컨텐츠의 저작권을 보호하기 위한 기술적 접근방법으로써 디지털 워터마킹(digital watermarking)에 관한 연구가 최근 몇년동안 활발하게 이루어지고 있다.

디지털 워터마킹은 저작권이나 사용권한에 관한 정보인 워터마크를 컨텐츠에 삽입함으로써 컨텐츠의 저작권을 보호하는 기법이다. 워터마크 삽입에 대한 비가시성(invisibility), 의도적 또는 비의도적 영상의 변형에 대한 강인성(robustness), 워터마크의 삽입과정이 알려져 있더라도 정확한 키를 알고 있는 경우에만 워터마크의 확인이 가능한 보안성(security), 워터마크가 삽입되어진 영상에 대해 명확한 소유권 주장할 수 있는 명확성(unambiguity) 등을 만족해야 한다[1].

워터마크 기법 중에서 다중 워터마킹(multiple watermarking)은 하나의 컨텐츠에 2개 이상의 다른 워터마크를 삽입하는 것으로, 이전에 삽입된 워터마크들은 삽입되어질 워터마크에 의해 영향을 받게 된다. 그러므로, 워터마크 삽입시에는 워터마크들의 정확한 추출이 가능하도록 최소한의 영향을 주어야 한다.

따라서, 본 논문에서는 삽입되는 워터마크간의 직교성(Orthogonality)을 이용해서 정확한 워터마크의 추출이 가능한 대역확산법을 이용한 다중 워터마킹 기법을 제안한다. 먼저, 2장에서는 기존의 다중 워터마크기법 및 문제점에 대해서 살펴보고, 3장에서는 기존 방법의 문제점 해결을 위하여 직교화 과정을 적용한 방법을

본 연구는 한국과학재단 2000 지역대학 우수과학자 지원연구에 의해 수행되었음

제안한다. 그리고, 4장에서는 제안 방법의 효율성을 확인하기 위한 시뮬레이션을 수행한 결과를 나타내고, 5장에서는 결론 및 향후 연구과제를 제시한다.

2. 대역확산법을 이용한 워터마킹

기존의 워터마킹 기법들은 공간이나 주파수 영역상에서 워터마크를 삽입하고, 추출하기 위하여 다양한 방법들을 이용하였다[2,3,4,5]. 통신이론에서 이용되는 대역확산법을 이용한 워터마킹 기법[3,4,5]은 원영상 $C=\{c(x,y)|1\le x,y\le n\}$ $W=\{w_i|w_i\in(0,1),i=1\ldots m\}$ 인 워터마크를 삽입하기 위해 대칭적(symmetric)이고 0의 평균을 가지는 계열인 $S=\{s(x,y)|1\le x,y\le n$ 를 이용하여

$$\hat{c}(x,y)=c(x,y)+m(x,y) \quad (1)$$

단, $m(x,y)\equiv w\cdot s(x,y)\ \ 1\le x,y\le n$

와 같이 워터마크가 삽입된 영상 $\hat{C}$를 얻게 된다. 워터마크의 추출은 워터마크가 삽입된 영상 $\hat{C}$와 S의 상관을 이용하여

$$\begin{aligned}\delta &= \langle \hat{C}, S\rangle \\ &= \sum_{(x,y)}^{n} c(x,y)s(x,y)+w_i\sum_{(x,y)}^{n}s^2(x,y)\end{aligned} \quad (2)$$

와 같이 계산하게 된다. 이때, S는 대칭이고 0의 평균을 가지고 있는 계열이기 때문에 식(2)의 첫번째 항의 값은 두번째 항과 비교하여 매우 작은 값이 되어진다. 따라서, 식(2)에 의해 계산된 δ의 값에 따라

$$\hat{w}=\begin{cases}1, & \text{if } \delta>0\\ 0, & \text{if } \delta<0\end{cases} \quad (3)$$

에 의해 삽입된 워터마크 $\hat{w}$를 추출하게 된다.

이와 같은 대역확산기법을 두개 이상의 워터마크를 삽입하는 다중 워터마킹에 적용한 기존의 방법[6]은 랜덤시퀀스와 Hadamard 행렬을 이용하여 워터마크를 삽입하고 있다. 이 방법은 동일한 위치 (x,y)에 t개의 서로 다른 워터마크 비트 $w_i(1\le i\le t)$를 랜덤계열 $R=\{r_i(x,y)|1\le i\le t,1\le x,y\le n$ Hadamard 행렬 $H=\{h_i(x,y)|1\le i\le t,1\le x,y\le n$ 이용하여 삽입하게 된다. 위치 (x,y)에 대해서 t개의 워터마크는

$$\hat{c}(x,y)=c(x,y)+m(x,y) \quad (4)$$

단, $m(x,y)=\sum_{i=1}^{t} w_i r_i(x,y)h_i(x,y)$

에 의해 워터마크가 삽입된 영상 $\hat{C}$를 생성하게 된다.

이때, 식(4)에 의해 얻어진 영상 $\hat{C}$으로부터 각각의 워터마크를 추출하기 위해서 삽입시 사용된 랜덤계열과 Hadamard 행렬을 정확하게 대응시키면 워터마크를 추출할 수 있다. 예를 들어, i번째의 워터마크를 추출하기 위해서, $S_i=r_ih_i$라고 할 때

$$\begin{aligned}\langle \hat{C}, S_i\rangle &= \sum_{(x,y)}^{n} c(x,y)S_i+\sum_{(x,y)}^{n} m(x,y)S_i \\ &= \sum_{(x,y)}^{n} c(x,y)S_i+\sum_{(x,y)}^{n}\sum_{j=i} w_i(S_i)^2+\sum_{(x,y)}^{n}\sum_{j\ne i} w_j S_j \\ &= \sum_{(x,y)}^{n} c(x,y)S_i+\sum_{(x,y)}^{n}\sum_{j=i} w_i(S_i)^2+\sum_{j\ne i} w_j\langle S_i,S_j\rangle\end{aligned}$$

와 같이 계산하여 식(3)을 적용하게 된다. 이때, 정확한 추출을 위해서는 식(5)의 세 번째 항이 0이 되어야 하며, 이것은 삽입되는 워터마크들이 서로 직교성을 가져야 함을 의미한다. 기존의 방법은 키에 의해 워터마크를 삽입하고 추출하기 위해 랜덤계열을 이용하였으나, 랜덤계열 자체는 직교성을 가지지 않기 때문에 직교성을 갖는 대표적 계열인 Hadamard 행렬을 적용하여 직교성을 제공하는 것이 그 목적이다. 그러나, 실제 직교성이 보장되는 Hadamard 행렬을 랜덤시퀀스에 곱해서 새로운 계열을 생성하더라도 직교성이 보장되지 않는다. 예를 들어,

$$r_1=\begin{bmatrix}-1&1&-1&1\\-1&1&-1&1\\1&-1&-1&1\\-1&1&-1&1\end{bmatrix},\quad h_1=\begin{bmatrix}1&-1&-1&1\\-1&1&1&-1\\1&-1&-1&1\\-1&1&1&-1\end{bmatrix}$$

$$r_2=\begin{bmatrix}1&1&-1&-1\\1&-1&1&-1\\-1&1&-1&1\\-1&1&-1&1\end{bmatrix},\quad h_2=\begin{bmatrix}1&-1&1&-1\\-1&1&-1&1\\-1&1&-1&1\\1&-1&1&-1\end{bmatrix}$$

인 경우에 대하여 계산하면 $\langle r_1h_1, r_2h_2\rangle\ne 0$이므로 직교성이 보장되지 않는다. 따라서, 워터마크의 정확한 추출이 불가능하게 된다.

3. 제안방법

기존의 방법에서는 직교성을 갖는 Hadamard행렬을 이용함에도 불구하고 랜덤계열에 의해 직교성이 보장되지 않는다는 문제점이 발생되었다. 이러한 문제점을 해결하기 위한 방법으로 Gram-Schmidt 직교화를 이용하여 계열간의 직교성을 부여하여 워터마크를 삽입하고 정확하게 추출할 수 있는 방법을 제안한다.즉, 제안 방식은 그림1과 같이 t개의 워터마크를 삽입하기 위해 먼저, 워터마크와 동일하게 t개의 랜덤계열을 생성하고, 각각의 랜덤계열들을 직교화한 후, 직교화된 계열을 이용하여 워터마크를 원영상에 삽입하게 된다.

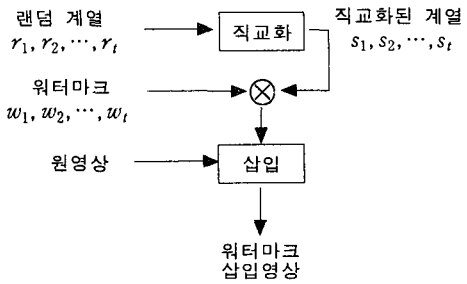

그림 1. 워터마크 삽입 과정

랜덤계열간에 직교성을 제공하기 위해 직교화 방법 중 Gram-Schmidt 직교화를 이용한다[7].

집합 $U=\{u_1, u_2, \ldots, u_n\}$을 R^n의 임의의 기저라 하면, Gram-Schmidt직교화는 아래의 단계로 수행된다.

[단계1] $v_1 = u_1$

[단계2] $v_2 = u_2 - \left[\frac{\langle u_2, v_1\rangle}{\langle v_1, v_1\rangle}\right] v_1$

[단계3] $v_3 = u_3 - \left[\frac{\langle u_3, v_1\rangle}{\langle v_1, v_1\rangle}\right] v_1 - \left[\frac{\langle u_3, v_2\rangle}{\langle v_2, v_2\rangle}\right] v_2$

[단계n] $v_n = u_n - \left[\frac{\langle u_n, v_1\rangle}{\langle v_1, v_1\rangle}\right] v_1 - \left[\frac{\langle u_n, v_2\rangle}{\langle v_2, v_2\rangle}\right] v_2 - \cdots - \left[\frac{\langle u_n, v_{n-1}\rangle}{\langle v_{n-1}, v_{n-1}\rangle}\right] v_{n-1}$

단, $\langle u_i, v_i\rangle = \sum_{i=1}^{N} u_i v_i$이다.

위의 각 단계를 v_n까지 반복하면 집합 U에 대해서 직교 기저인 $V=\{v_1, v_2, \ldots, v_n\}$을 얻을 수 있게 된다. 즉, 랜덤계열 $R=\{r_1, r_2, \cdots, r_t\}$에 대해서 위의 과정을 수행하면 직교화된 계열의 집합인 V를 얻을 수 있게 된다.

제안 방식에서는 먼저 크기 $N\times N$의 원 영상 C을 $B\times B$ 블록으로 분할한 후, 각 블록에 대하여 위치 (x, y), $1\le x\le B$, $1\le y\le B$에 각 워터마크의 1비트가 다음의 과정으로 삽입하게 된다.

<워터마크 삽입 과정>

[단계1] 랜덤계열의 생성

$B\times B$인 n개의 대칭이면서 평균 0을 가지는 랜덤계열 R를 생성한다.

[단계2] Gram-Schmidt 직교화 과정의 수행

- $v_1 = r_1$
- for $i=2$ to n

$$v_i = r_i - \sum_{j=i-1}^{n} \frac{\langle r_i, v_j\rangle}{\langle v_j, v_j\rangle} r_j$$

[단계3] 삽입정보 $M(x, y)$의 구성

$$M(x, y) = \sum_{i=1}^{t} w_i s_i(x, y) \quad (i=1, 2, 3, \ldots.)$$

[단계4] 워터마크의 삽입

$$\hat{C}(x, y) = C(x, y) + M(x, y)$$

위 과정에서 [단계3,4]는 위치 (x, y)에 복수의 워터마크를 삽입하는 것을 의미하며, 이 단계를 전블록에 대해서 수행하게 되면 워터마크가 삽입된 영상 $\hat{C}$를 얻을 수 있게 된다.

워터마크의 추출과정은 그림2와 같이 추출하고자 하는 워터마크가 w_1일 때 대응되는 직교화 계열 s_1을 이용하여 식(2)와 식(3)으로부터 상관값을 계산함으로써 w_1을 추출할 수 있다.

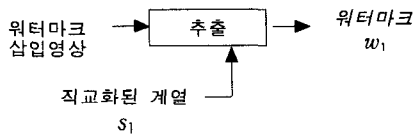

그림 2. 워터마크 w_1의 추출

삽입된 워터마크들은 원영상에 비해 낮은 에너지로 영상 전체에 분포되기 때문에 시각적으로 워터마크의 위치나 존재유무를 쉽게 알수 없고, 워터마크의 존재여부를 알게 되어도 랜덤계열에 대한 정보를 모르는 경우에는 워터마크의 추출이 불가능하게 된다.

4. 실험 결과 및 고찰

제안 방식의 효율성을 확인하기 위하여 그림3과 같이 256 그레이 레벨의 Lena(256×256, 8bits/pixel) 영상을 대상으로 하여 시뮬레이션하였다. 그림4는 16비트로 구성되는 3개의 워터마크를 나타내며, 비트 0은 흑을 나타내고 비트 1은 백으로 나타내어 시각적으로 확인할 수 있도록 표시하였다.

그림3. 원 영상(Lena)

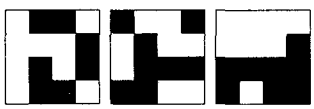

그림4. 삽입될 워터마크

시뮬레이션 결과, 그림4의 워터마크가 삽입된 워터

마크 삽입 영상을 그림5에 나타내었다.

(a) 기존의 방식 (b) 제안 방식

그림 5 워터마크 삽입 영상

그림3과 비교하여 볼 때 시각적으로 구분할 수 없을 뿐만 아니라, SNR(signal-to-noise ratio)을 측정한 결과 기존의 방식은 45.8584 dB, 제안 방식은 43.4510 dB로 측정되었다. 3개의 워터마크를 삽입하였을 때 기존의 방식은 -3~3의 원영상과의 변화량이 발생하지만, 제안 방식은 직교화 과정에서 이보다 많은 변화량 즉, -3.8~3.8로 변화하기 때문에 화질이 약간 떨어지게 되나 양호한 화질을 얻었다.

그림5로부터 기존의 방식에 의해 추출된 워터마크를 추출한 결과와 직교화계열들을 이용하여 각 워터마크를 추출한 결과를 기존의 방식에 의해 추출된 워터마크를 추출한 결과 그림6에 나타내었다. 기존의 방식은 키들간의 직교성이 보장되지 않기 때문에, 원영상이 필요한 경우에는 그림6(a)와 같이 어느 정도의 추출이 가능하지만 그렇지 않을 경우에는 추출 가능성이 불가능했다. 하지만, 제안방식에서는 정확하게 워터마크의 추출이 가능함을 알 수 있다.

(a) 기존 방식에 의한 추출

(b) 제안 방식에 의한 추출

그림6. 워터마크 추출 결과 및 비교

또한, 제안 방식에서는 랜덤계열에 직교성이 보장되기 때문에 보다 많은 워터마크를 삽입하더라도 명확한 추출이 가능하게 된다. 4개 이상의 워터마크를 삽입했을 때의 결과는 표1과 같다.

표 1. 4개이상의 워터마크 삽입시 결과

워터마크 개수	삽입영상의 SNR
4	41.7210 dB
5	41.6681 dB

5. 결론

다중워터마킹은 하나의 영상에 복수개의 워터마크를 삽입하는 기법으로 나중에 삽입되는 워터마크는 이전 워터마크의 추출에 영향을 주게 된다. 그러므로, 대역확산법을 이용한 다중워터마킹 기법은 삽입되는 워터마크간의 직교성이 보장되어야 한다. 랜덤계열과 Hadamard행렬을 이용한 기존의 다중워터마킹 기법은 랜덤계열로 인하여 직교성이 보장되지 않기 때문에 워터마크를 정확하게 추출하는 것이 불가능했다.

따라서, 본 논문에서는 워터마크간의 직교성이 보장되도록 Gram-Schmidt 직교화를 수행한 후에 다중워터마크를 삽입하고 정확하게 추출할 수 있는 기법을 제안하였다. 본 제안 방식은 랜덤계열의 직교화 과정에서 기존의 방식보다 계산량이 많고, 직교화 과정을 수행한 후 랜덤계열의 실수화로 추출시 오류가 발생할 우려가 있지만, 명확한 직교성이 제공되어 정확한 추출이 가능하다.

향후 연구과제로는 좀 더 효율적이고 공격에 강한 다중 워터마킹 기법에 관한 연구와 주파수 영역에서의 다중 워터마킹 기법과 접목하는 연구가 필요하다.

[참고문헌]

1. 원치선, "디지털 워터마킹 기술 동향", 한국통신학회 부호 및 정보이론 연구회 논문집, 제3권 1호, 1998

2. W. Bender, D.Gruhl, N.Morimoto, "Techniques for Data Hiding", Proc. of the SPIE, 1995.2.

3. J. Fridrich, "Robust Digital Watermarking Based on Key-Dependent Basis Functions", The 2nd Information Hiding Workshop, 1998

4. I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Images, Audio and Video", Proc. of Int'l Conf. on Image Processing, Vol.3, pp.243-246, 1996

5. M. Kutter, "Digital Image Watermarking : Hiding Information in Images," Ph.D thesis, Swiss Federal Institute of Technology, Lausanne, Switzerland, 1999

6. 김장환, 김규태, 김은수, "랜덤시퀀스와 Hadamard 행렬을 이용한 디지털 정보은폐 기술에 관한 연구", 한국통신학회논문지, 제24권 9A호, pp.1339-1345, 1999

7. http://www.math.unl.edu/~tshores/Book