랜덤 시퀀스와 직교코드를 이용한 디지털 정보은폐에 관한 연구

°김 장 환, 김 규 태, 김 은 수
광운대학교 전자공학과

A Study on Digital Information Hiding using the Random Sequence and Orthogonal Code

°Jang-Hwan Kim, Kyu-Tae Kim, Eun-Soo Kim
Dept. of Electronic Eng., Kwangwoon Univ.

요 약

본 논문에서는 랜덤 시퀀스와 직교코드를 이용하여 비화성이 강한 디지털 정보은폐 방법을 제시하였다.

Ⅰ. 서 론

컴퓨터 네트워크와 멀티미디어 관련 기술이 급격하게 발전함에 따라서 디지털화된 매체인 음성이나 정지영상(still image) 및 동영상(moving image) 등에 대한 수요도 급격하게 증가하고 있다. 이와 같은 디지털 매체에 대한 서비스가 21세기 고도의 정보화 사회에서 점점 종합적인 멀티미디어 서비스로 발전함에 따라 인터넷과 같은 통신망을 이용한 디지털 영상의 사용은 그 수요가 상상하지 못할 정도로 증가할 것으로 예상된다. 그리고 영화나 비디오와 같은 영상 매체는 주문형 비디오(VOD : video on demand) 형태의 서비스가 구체적으로 실현될 것이기 때문에 문서, 영상 그리고 음성 등과 같은 정보의 디지털화는 필연적이라고 할 수 있다. 따라서 이러한 디지털 정보에 대한 보안문제가 심각하게 대두되고 있으며 현재 디지털 정보 은폐에 대한 많은 연구가 진행과 더불어 상품화되고 있다.[1][2]

정보은폐기술은 indexing, captioning, 저작권보호, 비화통신(secret communication) 등에 사용될 수 있으며 용도에 따라 요구되는 특성이 다르다.[3] 예를 들어 captioning에서는 은폐하고자 하는 정보의 양이 중요하지만 저작권 보호에서는 저작권 정보의 불법 제거에 대한 강건성(robustness)이 더 중요시된다. 그러나 모든 용도에서 범용적으로 사용될 수 있는 정보은폐 방법이 이상적이다. 이러한 관점에서는 정보은폐기술이 은폐하고자 하는 정보의 양을 많이 사용할 수 있으며, 외부의 불법 제거에 대해 높은 강건성을 가져야 한다. 그러나 이러한 조건들을 동시에 만족하기에는 불가능하기 때문에 현재의 정보은폐기술에서는 사용목적에 따른 타협점(trade-off)을 찾는 것이 필요하다.

현재까지 발표된 디지털 매체에 대한 대표적인 정보은폐기술이 과거 군사목적으로 사용해 왔던 대역확산(spread spectrum) 방법이다.[4][5][6] 이러한 대역확산 방법에는 direct-sequence spread spectrum(DS) 방법과 frequency hopping 방법 등이 있다. 이 두 가지 방법은 모두 은폐하고자 하는 원래의 정보를 의사랜덤 시퀀스(pseudo-random sequence)라 불리는 잡음의 성격을 갖는 확산코드에 의해 정보의 에너지를 확산시킴으로서 은폐된 정보의 추출을 어렵게 할 수 있다. 여기서 DS 대역확산 방법은 원래의 정보보다 매우 큰 광대역 특성을 갖는 확산신호를 정보신호에 직접 곱해서 대역확산시킨 은폐된 정보를 얻을 수 있고, 원래의

정보를 복원하기 위해서는 사용된 동일한 확산신호를 곱해야만 원래의 정보를 얻을 수 있다. 즉, 사용된 확산코드를 모르는 사람에게는 아무 의미없는 잡음에 불과하지만 정확한 확산코드를 알고 있는 사람은 은폐된 정보를 복원할 수 있기 때문에 자연히 높은 비화특성을 갖는다. 그리고 이러한 코드는 거의 무한히 만들 수 있기 때문에 임의의 확산코드를 쉽게 재생할 수 없다.

본 논문에서는 의사랜덤 시퀀스와 강한 직교성을 갖는 Hardamard code 집합을 조합하여 원하는 정보를 임의의 다른 디지털 정보에 은폐하고자 하였다. 이와 같은 방법으로 은폐된 정보는 정보은폐시 사용된 두 가지 성분이 정확하게 일치될 경우에만 복원될 수 있으므로 다른 사용자가 무한히 발생시킬 수 있는 랜덤 시퀀스를 정확하게 재생하는 것은 거의 불가능하다. 따라서 강한 비화성을 가지며 Hardamard code의 직교성으로 서로 다른 성분간의 상관성이 발생하지 않는 복원영상을 얻을 수 있다. 이를 증명하기 위해 본 논문에서는 임의적으로 발생된 여러 가지 성분들에 대한 정보은폐 및 복원에 대한 시뮬레이션을 수행하였다.

Ⅱ. 대역확산 방법을 이용한 정보은폐 기술

원하는 정보를 연관성이 없는 다른 디지털 영상에 은폐시킬 때, 은폐하고자 하는 정보를 신호(signal)라고 하고, 다른 영상을 cover-image라 한다. 그리고 신호와 cover-image가 합쳐진 것을 stego-image라 부르며 이것을 다른 여러 사용자에게 배포한다. 이러한 정보은폐 기술에는 크게 stego-image에서 신호를 추출해낼 때 원래의 cover-image가 필요한 경우와 사용된 암호키만 이용하여 원신호를 복원하는 경우로 나눌 수 있다. 전자의 경우에는 사용자에게 cover-image에 대한 정보를 배포하지 않는 한, 숨겨진 정보에 대한 접근이 불가능하기 때문에 제한된 응용분야에만 사용할 수 있고, captioning, indexing, 비화통신(secret communication) 등이 불가능하다. 또한, 다수의 cover-image를 이용한 배포 이미지 저작권 보호를 수행할 때에도 데이터의 불법복사를 감시하는 자동 감시엔진 등이 cover-image에 대한 정보를 갖고 있어야 한다. 따라서 감시하고자 하는 정보의 개수가 늘어나면 대용량 저장시스템을 필요로 하며, 많은 계산시간이 소요되므로 빠른 처리속도를 요하는 응용분야에서는 사용할 수 없다. 후자의 경우에는 최근 소개된 정보은폐 기술 중에서 대역확산 방법을 이용하여 원하는 정보를 은폐할 수 있는데, 이 방법은 정보은폐 과정에서 사용된 여러 가지 파라미터 값들의 변형을 통해 은폐된 정보가 보이는 정도, 은폐정보량, 정보의 에너지 확산정도를 쉽게 조절할 수 있는 장점이 있어서, 여러 응용 분야로 확장할 수 있다.

본 논문에서는 의사랜덤 시퀀스를 이용하여 협대역 정보를 광대역 정보로 확산시켜서 원하는 정보신호의 power를 다른 정보(cover-image)의 power보다 낮추어서 원신호를 다른 정보에 은폐시키는 직접시퀀스 대역확산 방법을 이용하였다. 또한, 완전한 직교성을 갖는 Hadamard code를 이용하여 동일 공간상에 있는 확산코드 간의 상관성을 제거함으로서, 은폐된 원신호의 복원 시, 확산코드 간의 상관성에 의한 에러를 없애고 보다 많은 정보신호를 은폐할 수 있는 장점이 있다.

Ⅲ. 알고리즘

은폐하고자 하는 한 비트의 정보신호와 정보에 곱해지는 의사랜덤 확산코드를 각각 d_i와 r_i라 하고, 확산된 정보신호와 cover-image를 각각 $M(x,y)$, $C(x,y)$라 하면, 확산된 정보신호 $M(x,y)$와 여러 사용자에게 배포될 stego-image $S(x,y)$는 다음과 같이 식 (1)과 식 (2)로 나타낼 수 있다.

$$M(x,y) = \sum_i d_i r_i(x,y) \tag{1}$$

$$S(x,y) = C(x,y) + M(x,y) \tag{2}$$

여기서 사용된 의사랜덤 시퀀스 r_i는 숨겨진 정보의 오류없는 추출을 위하여 상호간에 직교성을 가져야 한다.

$$\langle r_i, r_j \rangle = \sum_{x,y} r_i(x,y) r_j(x,y) = nG^2\delta_{ij} \tag{3}$$

여기서, n은 픽셀수이고, G^2은 의사랜덤 시퀀스의 픽셀 당 평균 power(average power per pixel)이다. 의사랜덤 시퀀스와 cover-image가 서로 상관성을 갖지 않는 경우에는 최소한의 에너지를 갖는 정보신호로 은폐하여도 정확하게 원신호를 복원할 수 있지만, 그렇지 않은 경우에는 정확한 복원을 위한 최소 에너지 한계

가 존재한다. 실제의 경우, 의사랜덤 시퀀스와 cover-image 사이에는 어느 정도의 상관성이 존재한다.

$$\langle r_i, C\rangle = \sum_{x,y} r_i(x,y)\,C(x,y) \approx 0 \tag{4}$$

은폐된 정보신호의 복원과정은 stego-image와 의사랜덤 시퀀스와의 상관관계에 의해서 식 (5)와 같이 나타낼 수 있다.

$$\begin{aligned}\langle r_i, S\rangle &= \sum_{x,y} r_i(x,y)[\,C(x,y)+M(x,y)\,] \\ &= \sum_{x,y} r_i(x,y)\sum_j d_j r_j(x,y)+\langle r_i, C\rangle \\ &= \sum_j d_j \sum_{x,y} r_i(x,y)\,r_j(x,y)+\langle r_i, C\rangle \\ &= \sum_j d_j nG^2\delta_{ij}+\langle r_i, C\rangle \\ &\approx nG^2 d_i\end{aligned} \tag{5}$$

이와 같은 방법에서는 의사랜덤 시퀀스의 길이를 늘릴수록 숨기고자 하는 정보신호의 에너지를 전 주파수 영역에 보다 균일하게 확산시킬 수 있다. 따라서 식 (4)에서 발생할 수 있는 상관성은 이론적으로 랜덤 시퀀스의 길이에 비례하여 감소한다. 그러나 제한된 크기를 갖는 cover-image에서 랜덤 시퀀스의 길이를 무한정 증가시킬 수는 없기 때문에 완전하게 상관성을 없애는 것은 불가능하다. 또한 랜덤 시퀀스들이 완전한 직교성을 갖기 위해서는 서로 공간적으로 분리되어야 한다. 그러나 이 경우도 cover-image의 제한된 크기로 인해 분리시킬 공간의 한계와 랜덤 시퀀스의 길이에 의해 은폐시킬 수 있는 정보의 양에는 한계가 있다. 따라서 제한된 크기를 갖는 cover-image와 제한된 길이를 갖는 랜덤 시퀀스를 이용하여 많은 정보를 은폐시키기 위해서는 같은 공간상에 직교성을 갖는 랜덤 시퀀스를 중첩시켜서 사용해야 한다. 이러한 경우 같은 공간에 사용된 랜덤 시퀀스 사이의 상관성은 정보 복원의 에러요인이 될 수 있기 때문에 상관성을 없애는 방법으로 본 논문에서는 완전한 직교성을 갖는 Hadamard code를 의사랜덤 시퀀스와 결합함으로서 완전한 직교성을 갖는 랜덤 확산코드를 제시하고자 한다. 이 경우 많은 정보신호를 cover-image에 은폐시킬 수 있음과 동시에 은폐정보의 에너지를 균일하게 확산시킬 수 있기 때문에 많은 은폐정보를 에러 없이 복원할 수 있다.

Hadamard code를 $h_i(x,y)$라 하면 새로운 의사랜덤 시퀀스는 식 (6)과 같이 나타낼 수 있다.

$$r_i'(x,y) = r_i(x,y)h_i(x,y) \tag{6}$$

여기서, 새로 만들어진 확산코드 r_i'를 식 (3), (4), (5)의 r_i대신 사용하게 되면, 의사랜덤한 성격을 유지하는 동시에 Hadamard code의 직교성을 동시에 만족할 수 있으므로 동일한 공간상에서 직교성을 갖는 확산코드들을 만들 수 있다. 따라서 기존의 랜덤 시퀀스만을 이용한 방법에 비해 많은 정보신호를 에러없이 은폐시킬 수 있다.

그림 1은 본 논문에서 제시한 확산코드에 의해 원하는 정보신호를 은폐시키는 과정을 나타낸 것으로 랜덤 시퀀스와 Hadamard code에 의해 직교성을 갖는 대역확산된 정보신호를 cover-image에 삽입시킨 것이다. 그림 2는 정보은폐 과정에서 사용된 동일한 확산코드를 이용하여 은폐된 정보를 복원하는 과정을 나타낸 것이다.

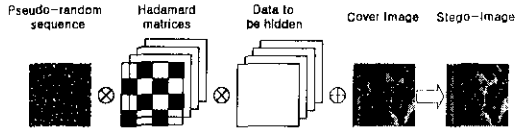

그림 1. 랜덤 시퀀스와 Hadamard code를 이용한 정보은폐 과정

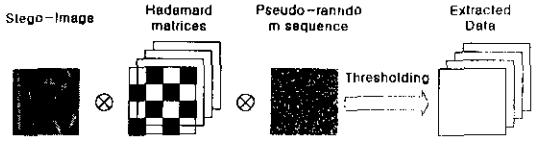

그림 2. 은폐정보의 복원과정

Ⅳ. 시뮬레이션

의사 랜덤 시퀀스와 Hadamard code를 이용하여 400×400 크기를 갖는 cover-image에 여러 가지 원하는 정보를 은폐하기 위해 다음과 같은 시뮬레이션을 수행하였다. 시뮬레이션에 사용된 cover-image는 그림 5의 (a)에 나타낸 Lena 이미지이며, 여기에 그림 3과 같이 16 bits로 구성된 서로 다른 정보신호 세 개를 은

폐하였다. 본 논문에서 제시된 방법은 사용목적에 따라 사용된 랜덤 시퀀스의 대역폭 확산분포 범위 내에서 확산코드의 상관관계가 없기 때문에 사용된 파라미터들의 변형이 용이하여 보다 많은 정보를 에러없이 은폐시킬 수 있다. 그림 4는 시뮬레이션에 사용된 Hadamard code를 나타낸다. 그리고 그림 5의 (b)는 랜덤 시퀀스와 Hadamard code에 의해 대역 확산된 정보신호의 공간주파수를 나타내며, 그림 5의 (c)는 정보신호가 은폐된 stego-image를 나타내는데, 여기서 은폐된 정보는 시각적으로 식별되지 않는다.

그림 6과 7은 동일한 확산코드를 사용하여 은폐정보를 복원한 것을 나타낸 것으로서, 그림 7의 경우는 cover-image와 확산코드간의 상관값을 없애기 위해서 그림 6을 threshold한 이미지이다.

그림 3. 은폐정보신호

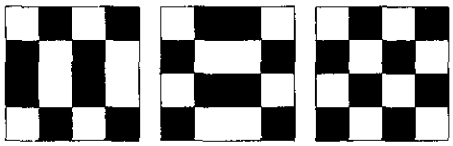

그림 4. Hadamard code

(a) (b) (c)

그림 5. cover-image와 stego-image

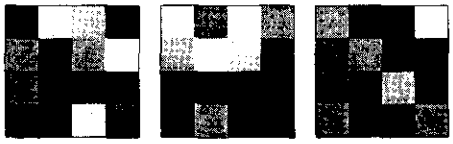

그림 6. threshold 전의 복원정보

그림 7. threshold 후의 복원정보

V. 결 론

본 논문에서는 의사랜덤 시퀀스와 Hadamard code를 이용하여 제한된 크기를 갖는 cover-image에 동일한 공간상에 3차원적으로 정보를 은폐시킬 때, 발생하는 확산코드간의 상관성을 제거하였다. 따라서 보다 많은 정보신호를 cover-image에 은폐시킬 수 있었고, 은폐정보의 복원도 에러없이 얻을 수 있었다. 이러한 정보은폐 기술은 비화통신 뿐만 아니라 컴퓨터 네트워크 상에서의 디지털 정보에 대한 저작권 보호 및 보안 기술로 다양하게 응용이 가능할 것이다.

참고문헌

[1] F. Takahashi, "Digital watermark safeguards multimedia copyright", Nikkei Electronics Asia, Vol.6, No.5, pp.46-52, 1997

[2] 한종욱, 박춘식, 김은수, "저작권 보호를 위한 디지털 워터마크", 한국통신정보보호학회, 7권 4호, 1997

[3] W.Bender, D. Gruhl, and N. Morimoto. "Techniques for data hiding" In proceeding of the SPIE, pages 2420-2440, San Jose, February 1991

[4] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt. "The Spread Spectrum Communications Handbook. McGraw-Hill, New York, 1994.

[5] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia", NEC Research Institute, Technical Report 95-10, 1995

[6] Joshua R. Smith and Barret O. Comiskey, "Modulation and Information Hiding in images", Proc. of Information Hiding Workshop, pp.207-226, 1996