

랜덤시퀀스와 Hadamard 행렬을 이용한 디지털 정보은폐 기술에 관한 연구

정희원 김장환*, 김규태*, 김은수*

A Study on Digital Information Hiding Technique using Random Sequence and Hadamard Matrix

Jang-Hwan Kim*, Kyu-Tae Kim*, Eun-Soo Kim* *Regular Members*

요약

본 논문에서는 랜덤시퀀스와 Hadamard 행렬을 이용하여 다중 정보를 은폐시킬 수 있는 새로운 디지털 정보은폐 기법을 제안하였다. 기존의 디지털 정보은폐에 사용된 기법은 하나의 랜덤시퀀스를 정보신호에 직접 곱하여 정보신호의 에너지 레벨을 매우 낮게 낮춤으로서 불법 이용자로 하여금 은폐된 정보의 검출이나 교란을 어렵게 하였다. 그러나 여러 개의 정보를 동일한 디지털 영상에 은폐시킬 경우에는 직교성이 보장되는 은폐코드를 사용해야 하기 때문에 어느 정도 상관성을 갖는 랜덤시퀀스만으로는 정보은폐가 어렵다. 따라서, 본 논문에서는 랜덤시퀀스의 장점과 더불어 직교성을 갖을 수 있도록 같은 행렬을 곱할 때만 정확한 신호로 추출되는 Hadamard 행렬을 랜덤시퀀스와 함께 사용하여 다수의 은폐정보에 대해서도 정확하게 은폐된 신호를 추출할 수 있는 새로운 디지털 정보은폐 방법을 제안하였다.

ABSTRACT

In this paper we propose the digital information hiding technique by which we use the combination of random sequence and Hadamard matrix to hide multiple information. The prior work used only one random sequence multiplied by information signal to lower the energy level of information signal and thus it is difficult for a third party to detect the information signal or jam it. But because we have to use the orthogonal code for hiding key in order to hide multiple information in the same digital image, only the use of random sequence that are not uncorrelated has some problems in the information hiding scheme. Thus we present a new information hiding scheme that can be used in hiding multiple information by the use of random sequence that spreads the energy level of the data to be hidden and Hadamard matrix that makes the random sequence uncorrelated.

I. 서론

최근, 컴퓨터 네트워크 및 멀티미디어 관련 기술이 급속도로 발전함에 따라 디지털화된 음성 및 영상 매체에 대한 수요도 급격하게 증가하고 있다. 이와 같은 디지털 매체에 대한 서비스는 21세기 정보화 사회에서 점점 종합적인 멀티미디어 서비스로

발전함에 따라 인터넷과 같은 통신망을 이용한 디지털 매체의 사용은 그 수요가 상상하지 못할 정도로 증가할 것으로 예상되고 있다. 따라서 이러한 디지털 정보의 진위 여부를 쉽게 판단할 수 있는 저작권 보호에 대한 문제가 심각하게 대두되고 있으며, 최근 이를 해결하기 위한 새로운 접근 방법으로 디지털 정보은폐(information hiding) 기술에 대한 많은 연구가 활발히 진행되고 있다.^{[1][2]}

* 광운대학교 전자공학부 (eskim@daisy.kwangwoon.ac.kr)

논문번호 : 99084-0305, 접수일자 : 1999년 3월 5일

* 본 연구는 한국학술진흥재단 자유공모과제(1998-001-E00746) 지원으로 수행되었습니다.

현재 연구 중에 있는 여러 가지 디지털 정보은폐 기술에서 고려되고 있는 특성은 크게 세 가지로 나눌 수 있다. 즉, 디지털 영상에 은폐된 후 추출될 수 있는 정보의 용량(capacity)과 은폐된 정보의 무인지성(imperceptibility), 그리고 우연적으로나 혹은 그 밖의 다른 의도에 의해 은폐된 정보를 쉽게 제거할 수 없는 강건성(robustness) 등이 있다. 그러나 이러한 것들은 서로 상충되는 특성을 갖고 있고 모든 것을 동시에 만족하는 정보은폐 기술의 실현은 매우 어렵기 때문에 사용목적에 따라 적당한 타협점을 찾아야 한다.^[3] 예를 들어 디지털 정보은폐 기술중의 하나인 captioning에서는 은폐하고자 하는 정보의 양이 중요하고 저작권 보호에서는 저작권 정보의 불법 제거에 대한 강건성을 보다 중요시 한다. 그리고 비화통신(secure communication)에서는 무인지성을 가장 크게 고려하고 있다. 그렇지만 이상적인 정보은폐 기술은 모든 용도에서 범용적으로 사용될 수 있어야 하며, 이러한 관점에서 정보은폐 기술은 은폐하고자 하는 정보의 양이 많고, 불법 사용자가 은폐된 정보를 인지할 수 없을 뿐만 아니라 외부의 불법 제거에 대해 높은 강건성을 가져야 한다.

현재까지 발표된 디지털 매체에 대한 대표적인 정보은폐기술은 과거 군사목적으로 사용해 왔던 대역확산(spread spectrum) 기법으로 direct-sequence (DS)와 frequency hopping(FH) 방법^[4,6] 등이 있다. 이 두 가지 방법은 모두 은폐하고자 하는 원래의 정보를 랜덤시퀀스(random sequence)라 불리는 잡음의 성격을 갖는 확산코드에 의해 정보의 에너지를 확산시킴으로서 불법 사용자로 하여금 은폐된 정보의 추출을 어렵게 한다. 여기서 DS 기법을 이용한 대역확산은 원래의 정보보다 매우 큰 광대역 특성을 갖는 확산신호를 정보신호에 직접 곱해서 대역확산시킨 은폐 정보를 얻을 수 있고, 원래의 정보를 추출하기 위해서는 사용된 동일한 확산신호를 곱해야만 얻을 수 있다. 즉, 사용된 확산코드를 모르는 불법 사용자에게는 아무 의미없는 잡음에 불과하지만 정확한 확산코드를 알고 있는 사람은 은폐된 정보를 추출할 수 있기 때문에 자연히 높은 비화특성을 갖는다. 또한, 넓은 주파수 대역폭을 갖고 있기 때문에 FFT나 DCT 등과 같은 신호처리 기술을 이용한 영상압축에도 강건성을 갖는다.

DS 기법을 이용하여 하나의 디지털 영상에 여러 개의 정보를 은폐하는 다중 정보은폐의 경우에 서로 다른 확산코드를 사용하게 된다. 따라서 이러한

경우에는 은폐된 정보의 어려운 추출을 위해서는 사용된 확산코드 사이에 상호상관성이 존재해서는 안된다. 즉, 사용된 확산코드가 백색잡음(white noise)과 같은 특성을 가지고 있어야 하는데 이와 같은 특성을 만족하기 위해서는 반복 주기가 무한히 길어야 한다. 그러나 디지털 영상에 곱하여 사용될 확산코드의 경우 1차원적으로나 2차원적으로 제한된 길이나 면적을 갖는 신호이기 때문에 완전하게 상호상관성을 제거할 수는 없다. 따라서 은폐된 정보의 정확한 추출을 위해서는 확산코드의 직교성을 보장할 수 있는 기능이 보완되어야 한다.

따라서, 본 논문에서는 DS 기법에서 사용되는 확산코드로 디지털적으로 발생시킬 수 있는 랜덤시퀀스와 강한 직교성을 갖는 Hadamard 행렬을 상호보완적으로 조합하여 원하는 여러 개의 정보를 임의의 디지털 영상에 다중 은폐시키는 새로운 기법을 제시하였다. 이와 같은 방법으로 은폐된 정보는 정보은폐시 사용된 두 가지 성분이 정확하게 일치될 경우에만 추출될 수 있으므로 불법 사용자가 무한히 발생시킬 수 있는 랜덤시퀀스를 정확하게 재생하는 것은 거의 불가능하므로 강한 비화성을 가지며, Hadamard 행렬의 직교성으로 서로 다른 확산코드간의 상관성이 발생하지 않기 때문에 어려운 은폐정보의 추출이 가능하다. 본 논문에서 제시된 방법의 검증을 위해 디지털적으로 발생된 랜덤시퀀스와 Hadamard 행렬을 이용한 정보은폐 및 추출에 대한 시뮬레이션을 수행하였다. 또한, 정보가 은폐된 디지털 영상을 네트워크를 통해 전송할 경우 전송로상에서 발생할 수 있는 가우시안 잡음뿐만 아니라 데이터의 대역폭을 줄이기 위해서는 JPEG과 같은 영상압축 알고리즘을 사용하므로 이와 같은 두 가지 영향에 의한 은폐정보의 추출 과정을 통해 제시된 알고리즘의 강건성에 대한 시뮬레이션을 수행하였다.

II. DS 대역확산 기법을 이용한 정보은폐 기술

특정 정보를 연관성이 없는 임의의 디지털 영상에 은폐시킬 때, 은폐하고자 하는 정보를 신호(signal)라고 하고, 위조방지 및 저작권의 보호가 필요한 디지털 영상이나 필요한 정보를 은폐시키기 위한 수단으로 사용되는 디지털 영상을 커버영상(cover-image)이라 한다. 그리고 신호와 커버영상이 합쳐진 것을 스테고영상(stego-image)이라 하고, 이것을 컴퓨터 네트워크 및 멀티미디어 관련 기술 등

을 이용하여 사용자에게 배포함으로써 암호키를 갖고있는 허가된 사용자만이 사용할 수 있다. 그림 1은 DS 대역확산 기법을 이용한 정보은폐 기술을 나타내고 있다.

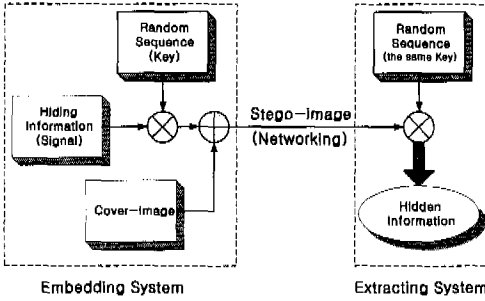


그림 1. DS 대역확산 기법을 이용한 정보은폐

이러한 정보은폐 기술에는 크게 스테고영상에서 신호를 추출해낼 때 원래의 커버영상이 필요한 경우와 사용된 암호키만 이용하여 원신호를 추출하는 경우로 나눌 수 있다. 전자의 경우에는 사용자에게 커버영상에 대한 정보를 배포하지 않는 한, 숨겨진 정보에 대한 접근이 불가능하기 때문에 제한된 응용분야에만 사용할 수 있고, captioning, indexing, 비화통신 등이 불가능하다. 또한, 다수의 커버영상을 이용하여 배포된 영상에 대한 저작권 보호를 수행할 때에도 데이터의 불법복사를 감시하는 자동 감시 엔진이 커버영상에 대한 정보를 갖고 있어야 한다. 따라서 감시하고자 하는 정보의 개수가 늘어나면 대용량 저장시스템을 필요로 하며, 많은 계산 시간이 소요되므로 고속처리가 요구되는 응용분야에서는 사용이 제한된다. 후자의 경우에는 최근 소개된 정보은폐 기술 중에서 대역확산 기법을 이용하여 원하는 정보를 은폐할 수 있는데, 이 방법은 정보은폐 과정에서 사용된 여러 가지 파라미터 값들을 변화시킴으로써 은폐된 정보가 보이는 정도, 은폐 정보량, 은폐정보의 에너지 확산정도를 쉽게 조절할 수 있는 장점이 있어서 여러 응용 분야로 확장할 수 있다.

III. 제안된 정보은폐 알고리즘

서로 다른 은폐 신호와 각 은폐신호에 곱해지는 랜덤시퀀스를 각각 d_i 와 r_i 라 하고, 확산된 은폐신호와 커버영상을 $M(x, y)$, $C(x, y)$ 이라고 한다면, 확산된 은폐신호 $M(x, y)$ 와 여러 사용자에게 배포될

정보가 은폐되어 있는 스테고영상 $S(x, y)$ 는 각각 식 (1), (2)로 각각 나타낼 수 있다.

$$M(x, y) = \sum_i d_i r_i(x, y) \quad (i=1, 2, 3, \dots) \quad (1)$$

$$S(x, y) = C(x, y) + M(x, y) \quad (2)$$

여기서 i 는 다중 은폐시 사용되는 랜덤시퀀스와 은폐신호의 개수를 나타낸다. 식 (1)에서 사용된 랜덤시퀀스 r_i 는 은폐된 정보의 오류없는 추출을 위하여 식 (3)과 같이 상호간에 직교성을 가져야 한다.

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

여기서, n 은 픽셀수이고, G^2 은 랜덤시퀀스 각각의 픽셀에 존재하는 평균 에너지를 나타낸다.

또한, 랜덤시퀀스와 커버영상이 서로 상관성을 갖지 않는 이상적인 경우에는 최소한의 에너지를 갖는 정보신호로 은폐하여도 정확하게 원신호를 추출할 수 있지만, 실제의 경우에는 식 (4)와 같이 랜덤시퀀스와 커버영상 사이에 어느 정도의 상관성이 존재하기 때문에 은폐정보의 정확한 추출을 위해서 삽입되는 은폐신호의 에너지를 최소로 조정할 필요가 있다.

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

은폐된 정보신호의 추출과정은 스테고영상과 랜덤시퀀스와의 상관관계에 의해서 식 (5)와 같이 나타낼 수 있다.

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

이러한 과정을 통해 만들어진 스테고영상에 존재하는 은폐정보는 커버영상에 비해 낮은 에너지 레벨로 포함되어 있기 때문에 시각적으로 은폐정보의 존재유무를 쉽게 인식할 수 없으며, 은폐정보의 존재여부를 인지하더라도 수많은 조합에 의해 만들어

진 랜덤시퀀스에 대한 정보를 모르는 경우에는 은폐된 정보의 검출이 불가능하다. 또한, 일반적으로 주파수영역을 이용하는 신호처리 기술을 이용한 스테고영상의 변형에도 은폐정보가 모든 주파수영역에 존재하기 때문에 은폐정보의 검출이 가능하다. 그러나 필요에 따라 하나의 커버영상에 여러 개의 정보를 은폐시킬 경우 사용된 랜덤시퀀스간의 상호상관성이 존재하지 않도록 유지해야 하는데 커버영상의 크기에 대응하여 사용되는 랜덤시퀀스의 경우 크기가 제한되기 때문에 완전한 상호상관성을 제거하는 것이 어렵다. 따라서 본 논문에서는 이러한 문제를 해결할 수 있는 접근 방법으로 부호화 과정에서 직교성을 갖는 Hadamard 행렬을, 랜덤시퀀스에 곱하여 사용함으로써 복호화 과정에서 상호상관성에 의해 발생될 수 있는 추출 정보의 에러를 없앨 수 있다.

Hadamard 행렬을 $h_i(x, y)$ 라 하면 새로운 랜덤시퀀스는 식 (6)과 같이 나타낼 수 있다.

$$r'_i(x, y) = r_i(x, y)h_i(x, y) \quad (6)$$

여기서, 새로 만들어진 랜덤시퀀스 r'_i 를 식 (3), (4), (5)의 r_i 대신 사용하게 되면, 랜덤시퀀스의 성질을 유지하는 동시에 Hadamard 행렬의 직교성을 만족할 수 있으므로 동일한 공간상에서 직교성을 갖는 랜덤시퀀스들을 만들 수 있다. 따라서 기존의 랜덤시퀀스만을 이용한 방법에 비해 많은 정보신호를 은폐시킬 수 있다. 그림 2는 랜덤시퀀스만을 정보은폐 코드로 사용할 경우와 직교성을 갖는 Hadamard 행렬을 함께 사용할 경우 나타나는 잡음을 비교한 것이다. 그림 2(a)는 500개의 서로 다른 랜덤시퀀스들을 사용하여 시뮬레이션한 결과 랜덤시퀀스만을 사용하였을 때 추가된 잡음 대 랜덤시퀀스와 Hadamard 행렬을 함께 사용했을 때의 잡음비를 나타내며, 그림 2(b)는 이에 대한 히스토그램을 나타낸다.

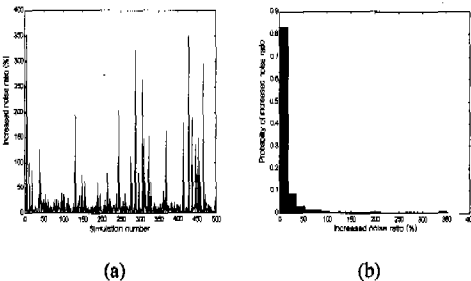


그림 2. 정보은폐 코드에 따른 상관잡음비

그림 2에서와 같이 랜덤시퀀스만을 이용할 경우에는 잡음으로 인하여 Hadamard 행렬을 함께 사용했을 때보다 대부분 40% 이내의 잡음이 추가되며, 랜덤시퀀스에 따라서는 최고 343%의 추가된 잡음이 나타나기 때문에 정보의 추출시 에러를 유발할 수 있다.

그림 3은 다중 정보은폐를 위해 본 논문에서 제시된 랜덤시퀀스와 Hadamard 행렬을 상호보완적으로 사용한 새로운 정보은폐신호를 나타낸 것이다. 그림 3에서와 같이 랜덤시퀀스와 Hadamard 행렬은 64×64 픽셀을 기본세트로 하여 전체적으로 512×512 픽셀로 구성되며, 하나의 기본세트는 64×64 픽셀이 '1'이나 '0'의 동일한 값으로 구성되는 1비트의 정보신호에 대응하여 직교성을 갖으면서 정보신호를 확산시키는 역할을 수행하게 된다.

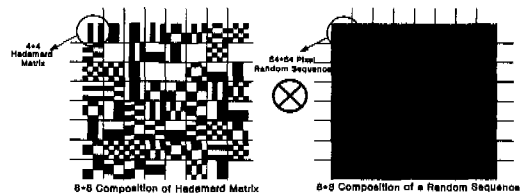


그림 3. 랜덤시퀀스와 Hadamard 행렬을 이용한 새로운 정보은폐코드

그림 4는 본 논문에서 제시한 랜덤시퀀스에 의해 원하는 정보신호를 은폐시키는 과정을 나타낸 것으로 랜덤시퀀스와 Hadamard 행렬에 의해 직교성을 갖는 대역확산된 정보신호를 커버영상에 삽입시킨 것이다. 이러한 과정에 의해 만들어진 스테고영상은 커버영상과 유사하여 정보의 은폐 유무를 쉽게 판단할 수 없으며, 비록 정보은폐의 유무를 알 수 있더라도 정보은폐 조합된 코드의 높은 비확성으로 인해 은폐된 정보를 쉽게 추출할 수 없다.

그림 5는 정보은폐 과정에서 사용된 동일한 랜덤시퀀스를 이용하여 은폐된 정보를 추출하는 과정을 나타낸 것이다. 스테고영상에 정보은폐 과정에서 사용되었던 정보은폐 코드를 곱함으로써 은폐시킨 정보를 정확하게 추출할 수 있다.

IV. 시뮬레이션

랜덤시퀀스와 Hadamard 행렬을 이용하여 512×512 크기를 갖는 커버영상에 여러 가지 원하는 정보를 은폐하기 위해 다음과 같은 시뮬레이션을 수행하였다. 시뮬레이션에 사용된 정보신호는 그림 6

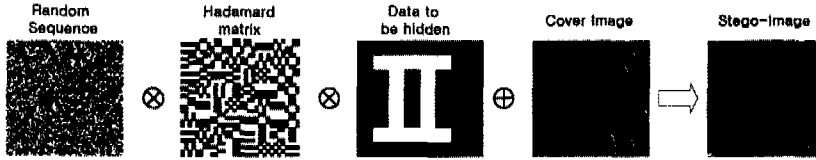


그림 4. 랜덤시퀀스와 Hadamard 행렬을 이용한 정보은폐 과정

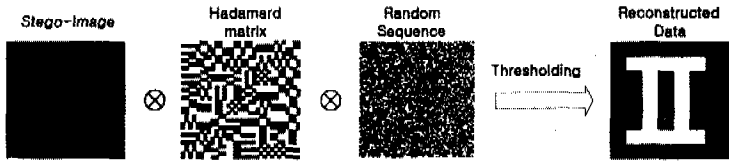


그림 5. 은폐정보의 추출과정

에 나타난 64×64 픽셀을 1비트로 하는 전체 64비트로 구성된 서로 다른 로마자 ‘I’, ‘II’, ‘III’ 세 개를 은폐하였고, 이것을 그림 7과 8에 나타난 랜덤시퀀스와 직교코드를 이용하여 커버영상에 은폐하였다.



그림 6. 은폐정보

그림 7은 정보신호와 랜덤시퀀스에 의하여 변조된 정보신호의 에너지 분포변화를 나타낸 것이다. 그림 7에서와 같이 은폐시키고자하는 협대역의 정보신호에 보다 높은 대역폭을 갖는 랜덤시퀀스를 곱해줌으로서 정보신호가 갖고 있는 일정한 에너지는 넓어진 대역폭의 크기에 반비례하여 작아지며, 이 확산신호에 동일한 랜덤시퀀스를 곱해주면, 확산신호의 대역폭이 다시 원래의 정보신호 대역폭으로 역확산되어 원래 정보신호로 추출된다.

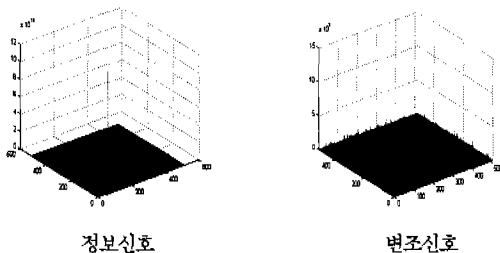


그림 7. 랜덤시퀀스에 의한 정보신호의 에너지 스펙트럼 분포

따라서 어느 정도의 에너지 레벨을 갖는 정보신호를 서로 다른 랜덤시퀀스를 이용하여 다중으로 중첩시키더라도 낮아진 에너지 레벨을 다중으로 중첩한 것이므로 스테고영상에서 정보신호가 인지되지 않을 뿐만 아니라 랜덤시퀀스를 다시 곱함으로써 다중의 정보신호를 추출할 수 있는 특징이 있다.

그림 8은 시뮬레이션에 사용된 랜덤시퀀스와 직교성을 갖는 Hadamard 행렬을 나타낸 것이다.

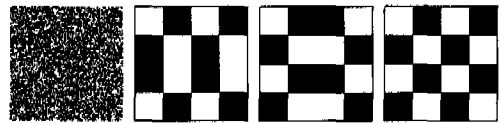


그림 8. 랜덤시퀀스와 Hadamard 행렬

본 논문에서 제시된 방법은 사용목적에 따른 랜덤시퀀스의 대역폭 확산분포 범위 내에서 랜덤시퀀스의 상관관계가 없기 때문에 사용된 파라미터들의 변형이 용이하여 보다 많은 정보를 어려없이 은폐시킬 수 있다. 그림 9의 (a)는 커버영상을 나타내고, (b)는 랜덤시퀀스와 Hadamard 행렬에 의해 대역 확산된 정보신호의 공간주파수를 나타내며, (c)는 정보신호가 은폐된 스테고영상을 나타낸 것이다.

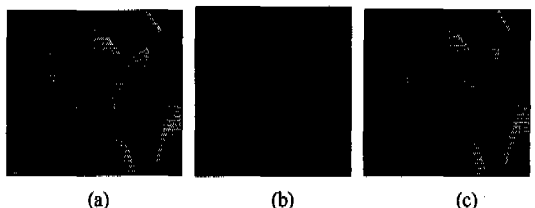


그림 9. 커버영상과 대역확산된 정보신호의 에너지 분포 및 스테고영상

그림 10과 11은 동일한 랜덤시퀀스를 사용하여 은폐정보를 추출한 것을 나타낸 것으로 그림 11의 경우는 커버영상과 랜덤시퀀스간의 상관치를 없애기 위해서 그림 10을 임계처리한 이미지를 나타낸 것이다. 시뮬레이션 결과 스테고영상로부터 은폐되어 있는 원래의 정보를 정확하게 추출할 수 있었다.

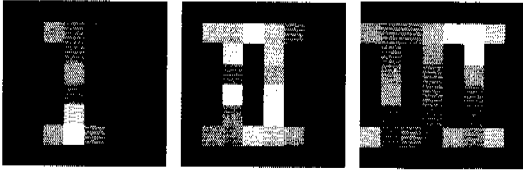


그림 10. 임계처리 이전의 추출영상

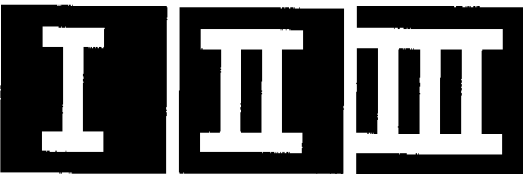


그림 11. 임계처리 이후의 추출정보

또한, 본 논문에서 제시된 정보은폐 알고리즘의 강건성을 실험하기 위하여 JPEG으로 영상압축되거나 가우시안 잡음이 섞인 스테고영상을 이용하여 은폐된 정보의 추출 실험을 수행하였다.

그림 12의 (a)는 크기가 512×512의 스테고영상을 image quality 80%인 JPEG으로 압축한 이미지를 나타내며, 그림 12의 (b)와 (c)는 각각 임계처리 이전과 이후의 추출된 정보신호를 나타낸 것이다.

그림 12의 시뮬레이션 결과와 같이 어느 정도까지의 이미지 압축에는 에러의 발생없이 정확한 정보신호를 추출할 수 있었다.

또한, 그림 13의 (a)는 가우시안잡음을 첨가한 스테고영상이고, 그림 13의 (b)와 (c)는 각각 임계처리 이전과 이후의 추출된 정보신호를 나타낸 것이다.

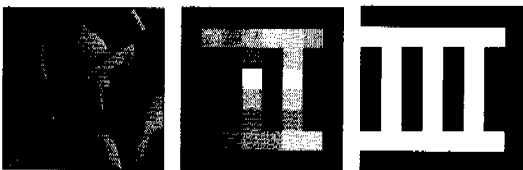


그림 12. JPEG에 의해 압축된 스테고영상에서 정보신호 추출

(a) JPEG 이미지 (b) 임계처리 이전
(c) 임계처리 이후

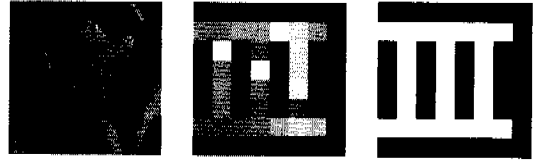


그림 13. 가우시안 잡음을 첨가한 스테고영상에서 정보신호 추출

(a) 가우시안 잡음을 첨가한 스테고영상
(b) 임계처리 이전 (c) 임계처리 이후

V. 결론

본 논문에서는 랜덤시퀀스와 직교성을 갖는 Hadamard 행렬을 상호보완적으로 사용하여 하나의 커버영상에 여러 개의 정보를 삽입함과 동시에 정확하게 추출할 수 있는 새로운 디지털 정보은폐 기법을 제시하였다. 기존에 사용된 랜덤시퀀스만을 이용한 정보은폐 기법을 이용하여 여러 개의 정보를 삽입한 후, 추출한 결과 랜덤시퀀스의 상호상관성 때문에 Hadamard 행렬을 함께 사용했을 때보다 40% 이내에서 최고 343%까지의 추가된 잡음이 존재했으며, 이로 인하여 은폐된 정보의 정확한 추출이 불가능하였다. 그러나 랜덤시퀀스를 직교성을 갖는 Hadamard 행렬과 함께 사용함으로써 랜덤시퀀스의 상호상관성에 의한 잡음의 발생을 제거함으로써 여러 개의 은폐된 정보에 대한 정확한 추출이 가능함을 시뮬레이션을 통해 입증하였다. 또한, 스테고영상이 네트워크를 통해 전송될 경우 JPEG과 같은 영상압축 알고리즘과 통신로 상에서 발생할 수 있는 가우시안 잡음에 대해서도 은폐된 정보의 추출이 가능함을 시뮬레이션을 통해 입증하였다.

참고 문헌

- [1] Jang-Hwan Kim, Kyu-Tae Kim, Eun-Soo Kim, "Information Hiding using Random Sequences", *Proc. of SPIE*, Vol.3814, 1999
- [2] Mitchell D. Swanson, B. Zhu, and Ahmed H. Tewfik, "Transparent Robust Image Watermarking," *Proc. of IEEE '96*, vol.III pp. 211-214, 1996
- [3] W.Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding" *IBM System Journal*, vol.35, no.3&4, pp.313-336, 1996
- [4] Rodger E. Ziemer, Roger L. Peterson. *Digital Communications and Spread Spectrum System*,

Macmillan, pp.327-357, 1985

- [5] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A Secure, Robust Watermarking for Multimedia", *Proc. of Information Hiding Workshop*, pp.185-206, 1996
- [6] Joshua R. Smith and Barret Q. Comiskey, "Modulation and Information Hiding in images", *Proc. of Information Hiding Workshop*, pp.207-226, 1996

김 장 환(Jang-Hwan Kim)

정회원



1998년 2월 : 광운대학교

전자 공학과 졸업

1998년 3월 ~ 현재 : 광운대학교

전자공학과 석사과정

<주관심 분야> Encryption, Optical Information Processing, Information Hiding

김 규 태(Kyu-Tae Kim)

정회원



1996년 2월 : 광운대학교

전자공학과 졸업

1998년 2월 : 광운대학교

전자공학과 석사

1998년 3월 ~ 현재 : 광운대학교

전자공학과 박사과정

<주관심분야> Encryption, Optical Information Processing, Information Hiding

김 은 수(Eun-Soo Kim)

정회원

한국통신학회논문지 제23권 제2호 참조