다중 정보 은폐 및 실시간 추출 시스템의 광-디지털적 구현

정회원 김 정 진*, 최 진 혁*, 김 은 수*

Opto-Digital Implementation of Multiple Information Hiding & Real-time Extraction System

Jung-Jin Kim*, Jin-Hyug Choi*, Eun Soo Kim* ***Regular Members***

요 약

본 논문에서는 광-디지털적 신호처리 기법을 이용한 새로운 다중 정보은폐 및 실시간 정보추출 시스템을 제시하였다. 즉, 공간영역에서 랜덤 시퀀스와 하다마드 행렬을 조합하여 생성된 스테고 키를 사용하여 하나의 커버영상에 여러 개의 정보를 은폐시킬 수 있는 다중 정보은폐 시스템과, 이들 은폐된 다중 정보를 실시간적으로 추출할 수 있는 광 상관기 기반의 광 정보추출 시스템을 구현하였다. 실험에서 다중 정보인 512 X 512 픽셀의 영문 알파벳 "N", "R", "L"을 8 X 8 블록 형태로 구성한 다음, 64 X 64 픽셀의 스테고 키와 곱해져 커버영상인 "Lena" 영상에 더해짐으로써 스테고 영상을 만들었다. 그리고, 이러한 스테고 영상은 각각의 스테고 키와 함께 NJTC 광 상관기에 입력되어 상관됨으로써 은폐정보를 실시간적으로 추출할 수 있었다. 특히, 본 실험에서 사용한 NJTC 광 상관기의 경우 위상형 광 상관기의 특성을 갖는 k=0.4이하에서 기존의 JTC보다 상관 출력값의 신호대 잡음비가 평균 7dB 이상 개선됨으로써 다중 정보은폐 및 추출 시스템의 실시간적 구현 가능성을 제시하였다.

ABSTRACT

In this paper, a new opto-digital multiple information hiding and real-time extracting system is implemented. That is, multiple information is hidden in a cover image by using the stego keys which are generated by combined use of random sequence(RS) and Hadamard matrix(HM) and these hidden information is extracted in real-time by using a new optical correlator-based extraction system. In the experiment, 3 kinds of information, English alphabet of "N", R", "L" having 512x512 pixels, are formulated 8x8 blocks and each of these information is multiplied with the corresponding stego keys having 64 x 64 pixels one by one. And then, by adding these modulated data to a cover image of "Lena" having 512×512 pixels, a stego image is finally generated. In this paper, as an extraction system, a new optical nonlinear joint transform correlator(NJTC) is introduced to extract the hidden data from a stego image in real-time, in which optical correlation between the stego image and each of the stego keys is performed and from these correlation outputs the hidden data can be easily extracted in real-time. Especially, it is found that the SNRs of the correlation outputs in the proposed optical NJTC-based extraction system has been improved to 7dB on average by comparision with those of the conventional JTC system under the condition of having a nonlinear parameter less than k=0.4. This good experimental results might suggest a possibility of implementation of an opto-digital multiple information hiding and real-time extracting system.

* 광운대학교 전자공학과 국가지정 3차원 미디어 연구실(kjj@explore.kwangwoon.ac.kr)
논문번호 : 020450-1015, 접수일자 : 2002년 10월 15일
※본 연구는 과학기술부 국가지정 연구실(NRL) 사업의 지원 아래 수행되었습니다.

Ⅰ. 서 론

최근, 컴퓨터 네트워크 및 멀티미디어 관련 기술이 급속도로 발전하고 인터넷과 같은 정보통신망을 이용한 디지털 매체의 사용은 그 수요가 상상하지 못할 정도로 증가함에 따라 이러한 디지털 정보의 진위 여부를 쉽게 판단할 수 있는 저작권 보호에 대한 문제가 심각하게 대두되고 있으며, 최근 이를 해결하기 위한 새로운 접근 방법으로 디지털 정보 은폐(digital information hiding) 기술에 대한 많은 연구가 활발히 진행되고 있다.

현재까지 발표된 디지털 미디어에 대한 대표적인 정보은폐 기술은 과거 군사적 목적으로 사용되어 왔던 대역확산(spread spectrum)기법으로 Direct-sequence(DS)와 Frequency hopping(FH) 방법 등이 있다. 이 두 가지 방법은 모두 은폐하고자 하는 정보를 랜덤 시퀀스(random sequence)라 불리는 잡음 성격의 확산코드에 의해 정보 에너지를 공간적으로 확산시켜 임의의 디지털 영상 전역에 은폐시키는 기법이다. 여기서, DS 기법을 이용한 대역확산은 원래의 정보보다 매우 큰 광대역 특성을 갖는 확산 신호를 정보신호에 직접 곱해서 대역확산된 은폐정보를 얻을 수 있고, 은폐정보를 추출하기 위해서는 사용된 동일한 확산신호를 곱해야만 얻을 수 있게 된다. 즉, 사용된 확산코드를 모르는 불법 사용자에게는 아무 의미없는 잡음에 불과하지만 정확한 확산코드를 알고 있는 사람은 은폐된 정보를 추출할 수 있기 때문에 자연히 높은 비화특성을 갖게 된다.[1][2]

그러나, 지금까지의 정보은폐 기술은 임의의 디지털 영상에 의미없는 신호를 삽입하여 저작권 인증 시 삽입된 정보의 유무만을 검사하거나 단일 정보만을 은폐시키는 방법으로 제한되어 제 3자의 공격이나 방해로부터 강건성과 은폐 정보량이 제한되고 있다.[2][3] 또한, 기존의 디지털 기법을 이용한 은폐정보의 추출과정은 은폐된 정보량에 따라 많은 계산시간이 소요되고 결과적으로 고속 인증이 요구되는 실질적인 응용이 제한되고 있다.

최근에는, 디지털 정보은폐 기법으로 랜덤 시퀀스(RS: random sequence)와 하다마드행렬(HM: Hardamard matrix)을 상호 보완적으로 조합하여 여러 개의 정보를 임의의 디지털 영상에 은폐시키는 새로운 다중 정보 은폐기법이 제시되었다[4]. 이러한 방법에서는 불법 사용자가 RS를 정확하게 재생하는 것은 거의 불가능함으로 강한 비화성을 가지며 또한, HM 행렬의 직교성으로 서로 다른 확산코드간의 상관성이 발생하지 않기 때문에 다중 은폐정보의 에러없는 추출도 가능하다. 그러나, 은폐정보의 양이 증가함에 따라 동시에 은폐된 다중 정보의 실시간적 추출이 요구되게 되는데 기존의 디지털적 상관 기법은 계산시간의 과다로 그 응용이 크게 제한되고 있다.

따라서, 이러한 문제를 해결하기 위한 새로운 접근방법으로 본 논문에서는 고속, 병렬처리 특성을 갖고 있는 광 정보처리 기술인 NJTC(nonlinear joint transform correlator) 광 상관기[4-7] 기반의 새로운 광 정보추출 시스템을 제시하고 실험을 통해 다중 정보의 은폐 및 추출 시스템의 실시간적 구현 가능성을 제시하고자 한다.

Ⅱ. 광-디지털 다중 정보은폐 및 실시간 추출 시스템

1. 제안된 시스템의 개요

디지털 정보은폐 기법에서 위조방지 및 저작권 보호를 위해 사용되는 정보를 워터마크(watermark)라 하고 이를 은폐시키기 위해 사용되는 디지털 영상을 커버영상(cover image)이라고 한다. 그리고, 은폐 정보가 포함된 커버영상을 스테고 영상(stego image)이라 하고 정보를 은폐하거나 추출할 때 사용되는 코드를 스테고 키(stego key)라고 한다.[1][4]

본 논문에서는 제 3 자에 의해 쉽게 모방될 수 없고 디지털적인 변형, 압축 등에도 강건하며 다중 정보를 은폐시킬 수 있는 디지털 정보은폐 기술로 RS와 HM을 상호 보완적으로 조합하여 생성된 스테고 키를 이용한 다중 정보은폐 시스템을 사용하였다[4]. 즉, RS의 강한 랜덤성은 확산된 은폐정보의 추출을 불가능하게 할 뿐만 아니라 다양한 신호처리 기법에도 강건한 특성을 갖으며 HM의 강한 직교성은 다중으로 은폐된 정보를 서로 간섭없이 추출할 수 있게 한다. 그러나 하나의 커버영상에 다중으로 은폐된 정보를 디지털적인 상관방법에 의해 추출할 경우 은폐된 정보의 양에 따라 많은 계산시간이 소요되기 때문에 본 논문에서는 이를 해결할 수 있는 새로운 접근방법으로 고속 및 병렬처리가 가능한 NJTC 기반의 광 정보추출 시스템을 제시하였다.

그림 1은 본 논문에서 새로이 제시한 광-디지털 다중 정보은폐 및 실시간 정보추출 시스템의 블럭

다이어그램을 나타낸 것이다.

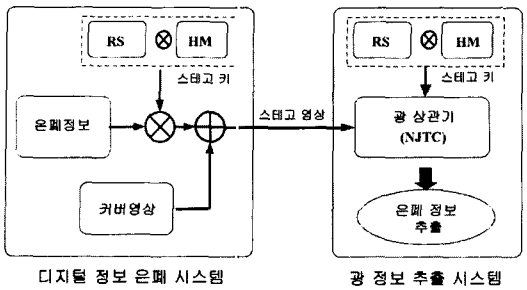


그림 1. 제안된 광-디지털 다중 정보은폐 및 추출 시스템의 블럭 다이어그램

그림 1에서 은폐시키고자 하는 각 정보는 RS와 HM의 조합으로 생성된 각각의 스테고 키와 곱해진 후 임의의 커버영상에 삽입됨으로써 스테고 영상이 만들어진다. 이 때, 스테고키는 은폐정보의 개수와 동일하게 생성되며 정보의 은폐 뿐만 아니라 정보의 추출에도 사용되게 된다. 그리고, 광 정보추출 시스템은 NJTC 기반의 위상형 광상관기로 구성된다. 즉, NJTC 입력 평면에 스테고 영상과 스테고 키를 동시에 위치시켜 퓨리에 변환한 다음 광 검출기로 광 간섭계기인 JTPS(joint transform power spectrum)를 검출하고 비선형적 신호변환을 통해 다시 역퓨리에 변환시킴으로써 상관 평면에서 상관첨두치 형태로 은폐정보를 추출할 수 있다.

2. 다중 정보은폐 및 추출 알고리즘

다중정보를 은폐하는데 사용되는 스테고 키 k_i는 랜덤 시퀀스와 하다마드 행렬이 $r_i(x,y)$, $h_i(x,y)$라고 주어지는 경우, 식(1)과 같이 나타낼 수 있다.

$$k_i(x,y) = r_i(x,y)\, h_i(x,y) \quad (i=1,2,3,\ldots\ldots) \tag{1}$$

여기서, i는 다중 정보 은폐시 사용되는 스테고 키의 개수를 나타낸다. 따라서, 식(1) 과 같이 구한 스테고 키는 각 은폐정보와 곱해져서 식(2)와 같은 대역 확산된 변조신호로 나타낼 수 있다.[3]

$$m(x,y) = \sum_i d_i(x,y)\, k_i(x,y) \tag{2}$$

여기서, $d_i(x,y)$와 $m(x,y)$는 은폐정보 및 스테고 키에 의해 변조된 은폐정보를 각각 나타내며, 은폐정보의 개수에 따라 사용될 스테고 키의 개수가 정해지게 된다.

스테고 키에 의해 변조된 은폐정보 $m(x,y)$는 임의의 커버영상 $c(x,y)$에 삽입되어 최종적으로 식(3)과 같은 스테고 영상 $s(x,y)$가 만들어지게 된다.

$$s(x,y) = c(x,y) + m(x,y) \tag{3}$$

식 (1)에서 사용된 스테고 키 $k_i(x,y)$는 다중 은폐된 각각의 정보의 오류없는 추출을 위해서 스테고 키 간에 직교성이 유지되어야 하며 기본 직교함수 수식은 식(4)와 같다.[1][3][4]

$$\langle k_i(x,y), k_j(x,y)\rangle = \sum_{x,y} k_i(x,y)\, k_j(x,y) = nG^2\delta_{ij} \tag{4}$$

여기서, n은 코드에 사용된 픽셀수이고 <.>은 직교함수를 나타내고 있으며 G^2와 δ_{ij}은 스테고 키 각 픽셀에 존재하는 평균 에너지와 디락 델터(Dirac delta)함수를 각각 나타낸다. 또한, 스테고 키와 커버영상이 서로 상관성을 갖지 않는 이상적인 경우에는 최소한의 에너지를 갖는 정보로 은폐해도 정확하게 본래의 은폐정보를 추출할 수 있지만, 실질적인 응용에서는 스테고 키와 커버영상 사이에 어느 정도의 상관성이 존재하기 때문에 식(5)와 같이 은폐정보의 정확한 추출을 위해서는 삽입되는 은폐정보의 에너지의 조정이 필요하다.[3]

$$\langle k_i(x,y), c(x,y)\rangle = \sum_{x,y} k_i(x,y)\, c(x,y) \approx 0 \tag{5}$$

이러한 과정을 통해 만들어진 대역확산된 은폐정보는 커버영상에 비해 낮은 에너지 레벨로 포함되기 때문에 시각적으로 은폐정보의 존재유무를 인식할 수 없으며 설사 은폐정보의 존재여부가 인지된다 하더라도 수많은 조합에 의해 만들어진 랜덤한 스테고 키에 대한 정보를 모르는 경우에는 은폐정보의 검출이 불가능하다. 또한, 직교성이 보장되는 스테고 키를 사용하여 다중 정보를 은폐시키기 때문에 단일 정보 은폐의 경우 보다 강건하면서 의미있는 여러 정보를 동시에 은폐시킬 수 있는 특징이 있다.

식 (6)은 스테고 영상으로부터 은폐된 다중정보를 추출하는 알고리즘을 나타낸 것이다. 즉, 정보은폐시 사용한 동일한 스테고 키를 사용한 상관을 통해 스테고 영상으로부터 각각의 은폐정보를 추출할 수 있다. 정보추출시 사용되는 스테고 키는 RS와 HM의 조합으로 생성되므로 랜덤성과 직교성이

보장되기 때문에 스테고 키 간의 상호상관 성분이 제거되어 은폐정보의 영상누화(crosstalk) 없는 추출이 가능하다.

$$
\begin{aligned}
&\langle k_i(x,y), s_j(x,y)\rangle \\
&= \sum_{x,y} k_i(x,y)s(x,y) \\
&= \sum_{x,y} k_i(x,y)[c(x,y)+m(x,y)] \\
&= \sum_{x,y} k_i(x,y)\sum_j d_j k_j(x,y) + \langle k_i(x,y), c(x,y)\rangle \\
&= \sum_j d_j \sum_{x,y} k_i(x,y)k_j(x,y) + \langle k_i(x,y), c(x,y)\rangle \\
&= \sum_j d_j nG^2\delta_{ij} + \langle k_i(x,y), c(x,y)\rangle \\
&\approx nG^2 d_i
\end{aligned}
\tag{6}
$$

식 (6)에서 스테고 키와 스테고 영상간의 상관시 은폐정보가 존재하는 스테고 영상 블럭에서는 은폐시 사용된 동일한 스테고 키가 곱해지기 때문에 자기상관에 의한 상관 첨두치 형태로 정보의 추출이 가능하게 된다. 이때, 커버 영상과의 상호상관 성분의 영향으로 정보가 존재하는 블럭에 따라 자기상관 성분의 에너지 레벨 차이가 존재할 수는 있으나 일정한 임계처리 과정을 통해 은폐정보의 추출이 가능하다. 또한, 각 스테고 키는 서로 직교성이 보장되기 때문에 각 스테고 키에 대해 그에 대응한 하나의 은폐정보 만이 추출되게 된다.

그러나, 실질적인 정보은폐 응용 시스템에서는 다중으로 은폐된 정보의 실시간적 추출이 요구되고 있으나 기존의 디지털 상관기법에 의한 은폐정보의 추출은 은폐 정보량이 증가함에 따라 많은 계산시간이 소요되기 때문에 실시간적 응용이 크게 제한되고 있다. 따라서, 본 논문에서는 이러한 문제를 해결할 수 있는 새로운 접근방식으로 고속, 병렬처리가 가능한 JTC 광 상관기 기반의 광 정보추출 시스템을 제시하였다. 특히, 기존의 JTC 광 상관기는 다중 키로 구성된 은폐정보의 추출시 잡음에 의한 상관 성능의 저하 및 상관 에러 등이 발생할 수 있기 때문에 위상형태의 광 상관기인 NJTC (nonlinear JTC)[6-8] 시스템을 사용하여 은폐정보 추출 시스템을 구현하고자 한다.

Ⅲ. NJTC 광 상관기 기반의 실시간 광 정보추출 시스템

일반적으로, 광상관 시스템에는 실수함수에 기반한 JTC(joint transform correlator) 광 상관기와 복소 정합필터에 기반한 VanderLugt형 광 상관기가 있다. 이 중 JTC는 별도의 복소 정합필터 구성없이 입력영상 및 기준영상을 입력평면에 나란히 배치한 뒤 동시에 퓨리에 변환함으로서 광 상관을 수행하는 것으로 시스템 구성이 간단하고 실시간적 구현이 가능하기 때문에 널리 사용되고 있다.[6][8-10] 또한, 최근 고속처리가 가능한 고해상의 공간광변조기(SLM: spatial light modulator)가 개발되어 비디오 프레임 수준의 실시간 광 상관기의 구성도 가능하다.

그림 2는 실시간 소자를 이용한 JTC 광상관 시스템을 나타낸 것이다. 즉, JTC 광 상관기에서는 실수함수로 구성되는 2개의 입력영상 간의 퓨리에 변환결과를 광 검출기를 통해 광 간섭세기 분포인 JTPS(joint transform power spectrum)형태로 검출하게 된다. 이러한 JTPS는 SLM에 입력되고 다시 퓨리에 변환됨으로써 상관 평면에서 최종적으로 2개의 입력영상 간의 상관 결과를 얻을 수 있다.

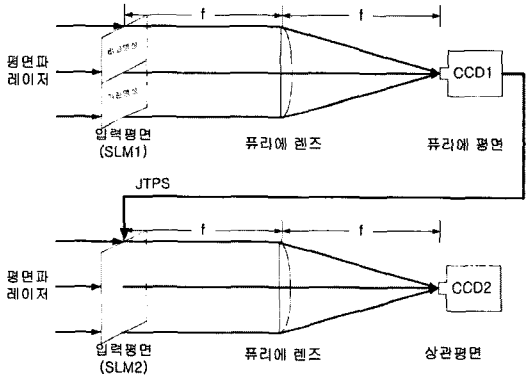


그림 2. JTC 광 상관기를 이용한 은폐정보 추출 시스템

따라서, 본 논문에서 제시한 광 상관기 기반의 실시간 은폐 정보추출 시스템에서는 비교영상인 스테고 영상과 기준영상인 스테고 키를 JTC 입력평면의 상, 하단에 동시에 입력시켜 상관시킴으로써 은폐정보를 실시간적으로 추출할 수 있다.

즉, JTC 입력평면에 나타난 상하 두 평면 영상을 동시에 퓨리에 변환하여 광 검출기로 검출하게 되면 식 (7)과 같은 광 간섭세기 분포인 JTPS를 얻을 수 있다.

$$
\begin{aligned}
JTPS(u,v) &= |R(u,v) + I(u,v)|^2 \\
&= |R(u,v)|^2 \\
&\quad + |I(u,v)|^2 + R^*(u,v)I(u,v) \\
&\quad + R(u,v)I^*(u,v)
\end{aligned}
\tag{7}
$$

여기서, *는 복소공액 성분을 $R(u,v)$와 $I(u,v)$는 기준영상과 비교영상의 퓨리에 변환을 각각 나타낸다. 식 (7)의 JTPS를 SLM에 다시 입력시켜 역 퓨리에 변환함으로써 최종적으로 식 (8)와 같은 상관결과를 얻을 수 있다.

$$I_{JTC}(x,y) = s(x,y)\otimes r_i(x,y)\oplus\delta[x+x(x_s-x_r), y+y(y_s-y_r)] + s(x,y)\otimes r_i(x,y)\oplus\delta[x-x(x_s-x_r), y-y(y_s-y_r)] \quad (8)$$

여기서, ⊗는 상관을 나타내며 ⊕는 콘볼루션(convolution)을 각각 나타낸다. 이와 같은 실수형 광 상관기인 JTC는 복소 정합필터 구성없이 구현되기 때문에 시스템 구성이 간단하고 실시간적 구현이 가능하지만 다중 정보은폐 시스템에 적용할 경우 다중정보의 주기적인 배치로 상관 오류 및 상관 유실이 나타나게 된다.[5][6] 따라서, 본 논문에서는 이러한 문제를 해결하기 위해 기존 JTC 광 상관기에서 검출된 JTPS에 비선형적 특성을 부여함으로써 위상형 광 상관기 특성을 갖는 NJTC(Nonlinear JTC) 광 상관기로 변형하고 이를 통해 상관 성능이 크게 개선된 NJTC 기반의 광 정보추출 시스템을 제시하였다.

즉, JTPS에 비선형성을 부여하기 위해 그림 3과 같은 시그모이드(sigmoid) 함수를 적용하였다. 그림 3에서 가로축은 식 (7)에 의해 구성된 JTPS를 세로축은 비선형 출력값을 각각 나타낸다.

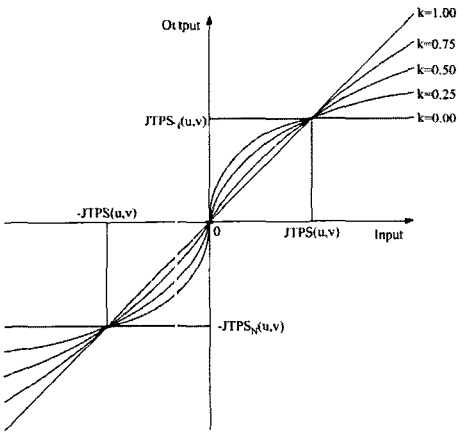


그림 3. NJTC 구현을 위한 시그모이드 함수

식 (9)는 기존의 JTPS에 시그모이드 함수를 적용하여 새로 구성된 비선형 JTPS를 나타낸 것이다.

$$JTPS_N(u,v) = |JTPS(u,v)|^k sgm[JTPS(u,v)] \quad (9)$$

여기서, sgm은 시그모이드 함수를 k는 비선형 특성을 결정하는 매개변수로 0에서 1의 범위에서 주어지는 실수값을 각각 나타낸다. 즉, 식 (9)에서 k값이 1에 가까워 질수록 $JTPS_N(u,v)$는 선형적인 출력결과로 기존의 JTPS와 같이 주어지며, k값이 0에 가까워 질수록 $JTPS_N(u,v)$는 2진 값을 갖게 되는 위상형태로 변환되어 바이어스는 감소하고 회절효율이 높아지게 된다. 이와 같은 위상형 광 상관기인 NJTC의 특성을 적절히 이용함으로서 스테고 영상으로 부터 은폐된 정보를 효과적으로 추출할 수 있다. 즉, NJTC를 이용한 은폐정보 추출 시스템에서는 정보은폐 시 사용된 스테고 키를 기준영상으로 하여 입력된 스테고 영상과 서로 상관시켜 상관첨두치의 크기와 위치를 파악함으로서 은폐된 정보의 추출이 가능하다. 그림 4는 NJTC를 이용한 실시간 광 정보추출 시스템의 블록 다이어그램을 나타낸 것이다.

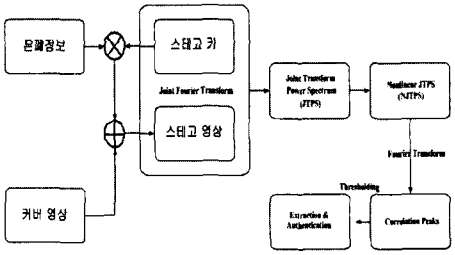


그림 4. 제안된 NJTC 광 정보추출 시스템 구성도

그림 4에서 보면, 스테고 키에 의해 다중정보가 은폐된 스테고 영상과 스테고 키가 동시에 퓨리에 변환되어 JTPS로 검출되게 된다. 그리고 이러한 JTPS는 비선형 양자화를 통해 $JTPS_N(u,v)$ 형태로 재구성되고 이는 공간광변조기에 입력시켜 다시 퓨리에 변환됨으로써 최종적으로 상관평면에서 스테고 키와 스테고 영상 간의 상관 결과를 얻을 수 있다.

Ⅳ. 실험 및 결과 고찰

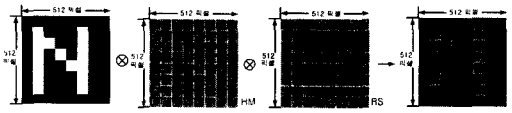
그림 5는 본 실험에서 사용한 3개의 은폐정보인 영문 알파벳 "N", "R", "L"과 커버영상인 "Lena" 영상을 각각 나타낸 것이다. 본 실험에서 은폐정보의 크기는 커버영상과 동일하게 512×512 픽셀로 구성하였으며, 그림 6과 같이 스테고 키와 같은 블럭 크기인 64×64픽셀 단위로 영역을 나누어 전체

적으로 8×8 블럭으로 분할한 다음 분할된 각 블럭에 대응되는 은폐정보를 세그멘트 형태인 "1"과 "0"의 값으로 표현하였다.

(a) 커버 영상 (b) 은폐 정보

그림 5. 실험에 사용된 커버영상 및 은폐정보(512×512)

그리고, 은폐정보를 변조시키기 위한 3개의 스테고 키는 RS와 HM 생성 알고리즘을 이용하여 64×64 픽셀크기로 생성한 다음 8×8 블럭으로 재조합한 후에 그림 6과 같이 각각의 은폐정보에 곱하게 되고 이것을 커버영상에 차례로 삽입시킴으로서 최종적으로 스테고 영상을 만들게 된다.



(a)은폐정보 (b)스테고키 (c) 변조된 정보

그림 6. 스테고 키를 이용한 은폐정보의 변조과정

그림 7은 스테고 키를 이용하여 커버영상인 "Lena" 영상에 다중 은폐정보인 "N", "R", "L"을 은폐시킴으로써 최종적으로 스테고 영상을 생성하는 과정을 나타낸 것이다. 즉, RS와 HM을 통해 생성된 3개의 서로 다른 스테고 키와 각각의 은폐정보가 곱해져 대역 확산된 후에 커버영상에 차례로 더해짐으로써 스테고 영상이 만들어지게 된다.

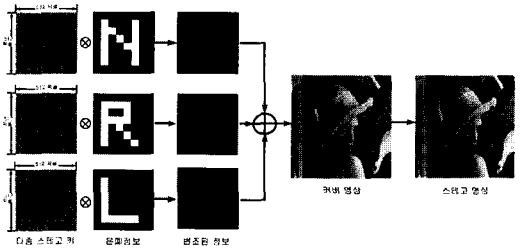


그림 7. 스테고 키를 이용한 다중정보 은폐과정

그림 8은 스테고 영상으로부터 은폐된 정보를 추출하는 과정을 나타낸 것이다. 즉, 입력된 스테고 영상에 정보 은폐시 사용했던 각각의 스테고 키를 서로 상관시키고 임계처리함으로써 대응되는 은폐정보를 추출할 수 있다. 이 때, 정보 추출시 사용되는 스테고 키는 RS와 HM의 조합으로 생성되므로 랜덤성과 직교성이 보장되기 때문에 스테고 키 간의 상호상관 성분이 제거되어 은폐정보의 영상누화(crosstalk) 없는 추출이 가능하다.

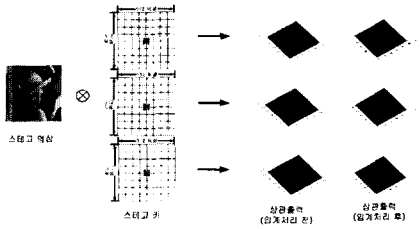


그림 8. 스테고 영상과 스테고 키 간의 상관을 통한 은폐정보 추출과정

그림 9는 광 NJTC를 이용한 실시간 정보추출 시스템의 광학 실험 구성도를 나타낸 것이다. 실험에서 레이저 광원은 파장이 532nm이고 출력이 100mW인 Nd-YAG 레이저(Model: P13VM215, Coherent)를 사용하고 공간광변조기로는 1024x768 픽셀의 해상도를 갖는 Sony사의 TFT-LCD를 사용하였고 CCD카메라는 1/2인치 크기, 41만화소이며, 0.04lux의 초 저조도를 갖는 삼성 SCC-341A를 사용하였다. 또한, 공간필터는 배율이 10배인 대물렌

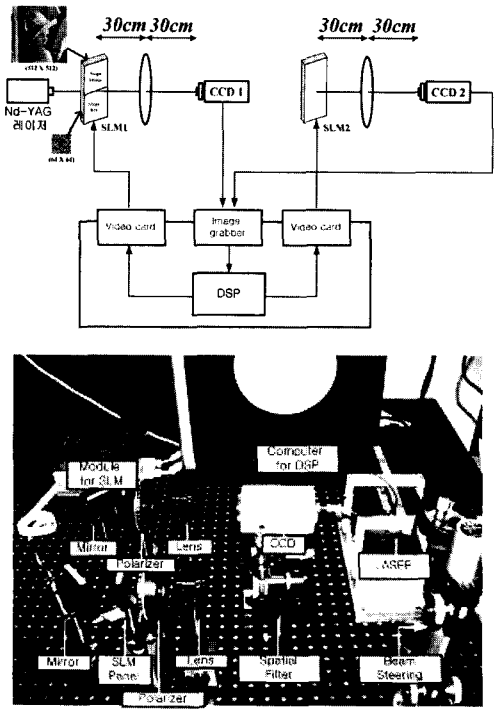


그림 9. 광 NJTC 기반의 은폐정보 추출 시스템의 광학실험 구성도 및 장치

즈와 25μ 크기의 핀홀을 조합하여 사용하였으며. 광 상관기는 초점 거리가 30cm인 퓨리에 렌즈를 사용하여 구성하였다.

그림 10-12는 NJTC 광 상관기를 이용한 은폐정보 추출 실험결과를 나타낸 것이다. 즉, 디지털적으로 양자화 하여 광학실험으로 복원한 결과이다. 그림 10은 NJTC 시스템의 비선형 매개변수를 k=1.0으로 설정한 경우의 실험결과로 이 경우는 NJTC 시스템이 기존의 JTC 상관기인 복소 정합필터(complex matched filter)와 같이 동작하게 된다. 그림 10에서 보면 기존의 JTC 광 상관기에서는 주기적으로 존재하는 은폐정보로 인한 상관에러가 발생되어 정확한 상관결과의 검출이 어렵고 따라서 은폐정보를 효과적으로 추출할 수 없음을 알 수 있다. 또한, 상관에러에 의해 은폐된 정보영역 뿐만 아니라 다른 영역에서도 상관첨두치가 발생되는 것을 볼 수 있다. 특히, 임계치 적용 전에는 은폐정보의 상관에너지 값이 매우 낮기 때문에 정확한 상관 출력을 거의 얻을 수가 없었다. 그러나, 그림 11은 NJTC 시스템의 비선형 매개변수를 k=0.0으로 설정한 경우의 실험결과로 이 경우는 NJTC 시스템이 이진 위상형 필터(binary phase only filter)로 동작하게 된다. 그림에서 보면 완전 이진 위상필터에 의한 상관이 이루어지기 때문에 복소필터 보다는 훨씬 개선된 상관 첨두치를 얻을 수 있는 반면에 많은 고조파 항의 발생하여 상관에러의 가능성이 있음을 알 수 있다. 그리고, 그림 12는 비선형 매개변수를 k=0.4로 설정한 경우의 실험결과로 이 경우는 NJTC 시스템이 기존의 JTC 상관기에서 위상성분이 강조된 형태로 동작하게 된다. 그림 11과 비교해 보면 완전 이진 위상형보다는 진폭 성분이 보상된 위상형 광 상관기에서 상관성능이 보다 개선되는 것을 알 수 있다.

그림 10. 광 NJTC를 이용한 은폐정보의 추출결과(k=1.0인 경우)

그림 11. 광 NJTC를 이용한 은폐정보의 추출결과(k=0.0인 경우)

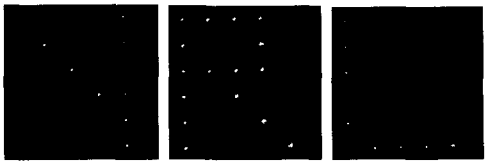


그림 12. 광 NJTC를 이용한 은폐정보의 추출결과(k=0.4인 경우)

그림 13는 NJTC 시스템의 비선형 매개변수인 k 값을 변화시키면서 구한 각 은폐정보에 대한 상관출력의 신호대 잡음비(SNR : signal-to-noise ratio)를 나타낸 것이다. 그림 13에서 보면 기존의 JTC 시스템 경우인 k 값이 1.0에서 SNR이 가장 낮게 나타났으며 k값을 감소시킴에 따라 SNR은 계속 증가하여 k=0.4에서 가장 큰 SNR을 갖게 됨을 알 수 있다. 또한, k=0.4 이후부터 k=0.0까지는 약간 감소하나 비교적 크고 일정한 SNR 값을 유지함을 알 수 있었다.

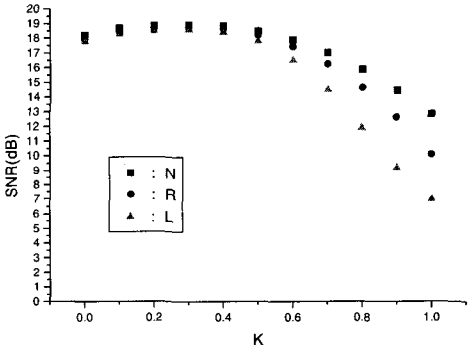


그림 13. 광 NJTC 시스템에서 비선형 상수 k값에 따른 SNR 변화

따라서, 이상 실험을 통해 k=0.4인 NJTC 광 상관기의 경우 기존 JTC 광 상관기에 비해 SNR이 평균 7dB 이상 개선됨을 알 수 있었다. 그리고, 랜덤성과 직교성이 보장되는 스테고키의 사용으로 각 스테고 키에 대응한 은폐정보를 서로 상호상관 없이 추출할 수 있었다. 또한, 실험을 통해 광 간섭세기 분포인 JTPS의 위상성분을 최대한 이용하면서 진폭성분을 적당히 보상해 줌으로써 최적화된 광 NJTC 은폐 정보추출 시스템의 구현 가능성을 제시하였다.

V. 결 론

본 논문에서는 광-디지털적 신호처리 기법을 이

용한 새로운 다중 정보은폐 및 실시간 정보추출 시스템을 제시하였다. 즉, 공간영역에서 랜덤 시퀀스와 하다마드 행렬을 조합하여 생성된 스테고 키를 사용하여 하나의 커버영상에 여러 개의 정보를 은폐시킬 수 있는 다중 정보은폐 시스템과, 이들 은폐된 다중 정보를 실시간적으로 추출할 수 있는 광 상관기 기반의 광 정보추출 시스템을 구현하였다. 실험에서 다중 정보인 영문 알파벳 "N", R", "L"을 8 x 8 블럭 형태로 구성한 다음, 64 X 64 픽셀크기의 스테고 키와 곱해져 512 x 512 픽셀의 커버 영상인 "Lena" 영상에 더해짐으로써 스테고 영상을 만들었다. 그리고, 이러한 스테고 영상은 각각의 스테고 키와 함께 NJTC 광 상관기에 입력되어 상관됨으로써 은폐정보를 실시간적으로 추출할 수 있었다. 특히, 본 실험에서 사용한 NJTC 광 상관기의 경우 위상형 광 상관기의 특성을 갖는 k=0.4 이하에서 기존의 JTC보다 상관 출력값의 SNR이 평균 7dB 이상 개선됨으로써 NJTC 기반의 다중 정보은폐 및 추출 시스템의 실시간적 구현 가능성을 제시하였다.

참 고 문 헌

[1] R. C. Dixon, Spread Spectrum Systems, *John Wiley & Sons*, New York, 1994

[2] I. J, Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking, *A Harcourt Science and Technology Company*, 2001

[3] S. Katzenbeisser, F. A.P. Petitcolas, Information Hiding techniques for Steganography and digital watermarking, Artech house publishers, pp. 64-66, 2000

[4] K. T. Kim, J. H. Kim, and E. S. Kim, "Multiple information hiding technique using random sequence and Hadamard matrix," *Opt. Eng.* vol. 40, no. 11, pp.2489-2494, 2001

[5] E. S. Kim, S. Y. Yi, and Y. H. Gee, "A BPEJTC-based segmentation for a non-stationary image," *Opt. Comm.*, vol. 123, pp. 716-724, 1996

[6] B. Javidi, J. Wang, and Q. Tang, "Nonlinear joint transform correlators," *Pattern Recognition*, vol. 27, no. 4, pp. 522-542, 1994

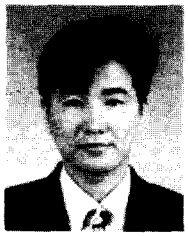
[7] H. G. Yang, and E. S. Kim, "Practical image encryption scheme by real-valued data," *Opt. Eng.*, vol. 35, no. 9, pp. 2473-2478, 1996

[8] D. Abookasis, O. Arazi, J. Rosen, and B. Javid, "Security optical systems based on a joint transform correlator with significant output images," *Opt. Eng.*, vol. 40, no. 8, pp. 1584-1589, 2001

[9] B. Y. Soon, M. A. Karim, and M. S. Alam, "Using the joint transform correlator as the feature extractor for the nearest neighbor classifier," *Opt. Eng.*, vol. 38, no. 1, pp. 39-46, 1999

[10] D. W. Weber, and J. Trollinger, "Novㄷ implementation of nonlinear joint transform correlators in optical security and validation," *Opt. Eng.*, vol. 38, no. 1, pp. 62-68, 1999

김 정 진(Jung-jin Kim) 정회원



2002. 2 : 광운대학교 전자공학과 국가지정 3차원영상미디어 연구실 박사 수료

2002. 3 ~ 현재 : (주)맥스 소프트 기술연구소 선임 연구원

<주관심 분야> 정보보호, 워터마킹, 암호화, 컴퓨터 비젼

최 진 혁(Jin-hyug Choi) 정회원

2002. 2 : 광운대학교 전자공학과 학사

2002. 3 ~ 현재 : 광운대학교 전자공학과 국가지정 3차원영상 미디어 연구실 석사 과정

<주관심 분야> 정보보호, 워터마킹, 암호화,

김 은 수(Eun-soo Kim) 정회원

현재 : 광운대학교 국가지정 3차원 영상미디어연구실 및 전자공학부 교수

(http://3dmedia.kwangwoon.ac.kr)

한국통신학회지 논문지 제26권 11호 참조