《연구논문》 Hankook Kwanghak Hoeji, Volume 19, Number 4, August 2008 DOI: 10.3807/HKH.2008.19.4.262

다중 복호화 키들을 이용한 영상 워터마크 방법

이형석 · 서동환†

한국해양대학교 전기전자공학부
㊞ 606-791 부산광역시 영도구 동삼동 1

조규보

경북대학교 전자전기컴퓨터학부
㊞ 701-702 대구광역시 북구 산격동 1370

(2008년 7월 8일 받음, 2008년 8월 14일 수정본 받음, 2008년 8월 15일 게재 확정)

본 논문에서는 다중 복호화 키들을 이용한 영상 워터마크 방법을 제안하였다. 하나의 워터마크 영상에서 다중 복호화 키들을 이용하여 여러 개의 원 영상을 복원 할 수 있고 왈시 코드를 이용하여 복호화 과정에서 간단하게 사이드 로브를 제거한 복원 영상을 얻을 수 있는 장점을 갖고 있다. 삽입 과정에서 제로 패딩(zero-padding)된 원 영상들을 무작위 위상 영상들과 곱하여 푸리에 변환 후 실수부를 취하여 부호화된 영상을 생성한다. 삽입 영상들은 확장된 부호화 위상 영상들을 새롭게 생성된 무작위 위상영상들과 곱한 후 이 영상들의 개수만큼 독립적으로 생성한 왈시 코드 영상들을 곱하여 생성하고 이 때 사용된 무작위 위상영상들에 동일한 왈시 코드 영상들을 곱하여 복호화 키 영상들로 사용한다. 스테고(stego) 영상은 삽입 영상들과 새로운 왈시 코드 영상이 곱하여진 커버(cover) 영상의 중첩에 의해 생성한다. 원 영상은 스테고 영상과 다중 복호화 키를 곱하여 비확산을 취한 후 역-푸리에 변환하여 복원할 수 있다. 컴퓨터 모의실험을 통하여 제안한 워터마크 방법의 적합성과 다중 복호화 키로 복원이 가능하고 영상에 잡음이 발생하더라도 원 영상의 복원이 가능함을 확인하였다.

주제어: Phase encoding, Optical encryption, Walsh code, Watermark

I. 서 론

현대는 디지털 시대를 지나 멀티미디어의 시대로서 인터넷, 컴퓨터, 디지털 텔레비전, 휴대폰, PDA 등으로 대표되는 다양한 디지털 기기들을 통해 대량의 영상 및 음성정보가 교환되고 인간의 모든 생활영역에서 그 영향력을 넓혀가고 있다. 이에 따른 정보 보호에 대한 필요성은 공공기관, 연구소, 산업현장 뿐만 아니라 개인의 사생활에 이르기까지 다양한 분야에서 대두되고 있으며, 그 영향으로 정보 보호 시스템에 대한 연구들이 다양하게 진행되고 있다. 하지만 각종 카드나 화폐들을 보다 정밀하게 복제 또는 위조하게 되었으며, 이로 인한 경제적 피해뿐만 아니라 개인의 인권에 대한 피해도 증가되고 있다. 특히 여권이나 신분증의 위조는 각종 범죄와 밀입국의 수단으로 사용되고 있어 사회불안에까지 영향을 미치고 있다.[1,2] 이를 예방하기 위해서 최근에 CCD 카메라, 복사기, 스캐너 등과 같은 기존의 광세기 검출기로는 볼 수도 복제할 수도 없는 복소함수 형태의 랜덤 위상 패턴을 사용하는 광학적 정보보호 기술이 연구되고 있으며 이는 광을 이용한 신호는 세기정보와 위상(phase) 정보를 동시에 광학적인 매질 또는 공간광변조기(spatial light modulator)에 기록이 가능하다는 특성에 기인하며 광전자 소자들을 이용하여 실 시간적인 구현이 가능하고 랜덤 위상 암호 키를 사용함으로써 정보를 위조하거나 해독하지 못하도록 함으로써 우리의 생활을 심각하게 위협하는 개인정보보호의 문제를 해결할 수 있는 접근방법으로 제시되고 있다.

광 암호화 시스템은 주로 공간영역이나 주파수영역에서 원 영상을 백색잡음 형태를 가지는 복소함수로 암호화한 후 4-*f* 광 상관기(correlator)[3-5]나 간섭계[6] 또는 결합 변환 상관기(joint transform correlator, JTC)[7,8]를 이용하여 복호화 한다. 이중 4-*f* 광 상관기를 이용한 암호화 시스템은 광축 정렬 문제로 실질적인 시스템 응용에 문제가 있으며 간섭계를 이용하는 시스템은 시스템 구성이 외부 교란에 민감한 단점을 가지고 있다. 또한 결합 변환 상관기는 광축 정렬 문제를 해결할 수 있으나 출력 평면에 자기 상관 성분이 큰 세기로 나타나는데, 이것이 실질적인 시스템에 적용하기 어렵게 만드는 주원인이 된다. 이중 무작위 위상 부호화 방법 또한 앞서 제안한 방법에서 암호화된 영상이 여러 형태의 외부 영향에 얼마나 강한 방법인가를 확인하였다.[9,10] 한편으로 앞서 제안된 방법들을 응용하여 정보의 중요성에 따라 상위 수준(high-level) 사용자와 하위수준(low-level) 사용자들로 분리하여 계층적으로 시스템에 접근하는 광 보안 시스템이 제안되었다. 이 방법은 반복 알고리즘을 사용함으로써 시간소모가 많고 정보의 중요성이 높아질수록 입력 정보가 많아지는 단점을 가지고 있다.[11]

또한 현재 사용되는 암호화 기법의 콘텐츠 보호는 디지털 콘텐츠에 대한 접근이 극히 제한된다는 단점과 한번 암호가

†E-mail: dhseo@hhu.ac.kr

풀린 콘텐츠는 더 이상 보호할 수 없다는 한계를 가지고 있다. 이러한 문제점을 해결하기 위한 하나의 수단으로 디지털 워터마크(digital watermark) 기법이 제안되고 있다. 디지털 워터마크는 정지 영상, 동영상, 오디오, 컴퓨터 프로그램과 같은 데이터에 인간이 인지할 수 없도록 삽입한 디지털 코드를 말한다. 일반적으로 워터마크는 공격에 대한 내성에 따라서 크게 세 가지로 구분된다. 첫번째로 로버스트(robust·저작권 증명) 워터마크는 가장 기본적인 형태의 워터마크로 일반적인 공격에 강인하게 제작되어 주로 소유권 주장이나 저작권 문제를 해결하기 위해 사용된다. 두번째는 프래절(fragile·원본증명) 워터마크로 대부분 인증이나 무결성에 관련된 목적에 적합하다. 이 워터마크의 경우 공격을 받으면 쉽게 손상돼서 공격받은 위치나 공격의 형태 등에 대한 정보를 준다. 마지막으로 로버스트 워터마크와 프래절 워터마크의 중간 형태인 세미프래절 워터마크는 비의도적으로 공격했거나 코드를 변경하는 경우에는 살아남고, 삭제하거나 가공하는 식의 의도적인 공격에 대해서는 공격한 위치를 확인할 수 있다. 또한 원본 및 키의 사용 여부에 따라서도 크게 두 가지로 구분되며 하나는 워터마크 검출 시 원본을 사용하는 경우로 이를 논 어블리비어스(non oblivious) 워터마크로 원본을 사용해 워터마크 된 데이터와 원 데이터간의 관계를 활용해 워터마크를 검출하게 된다. 이 방법의 경우 워터마크 된 영상과 원본 영상을 일일이 대조해야 하는 등 여러 가지 문제점이 있다. 또 하나는 검출 시 원본 없이 워터마크 된 데이터만을 사용해 워터마크를 검출하는 어블리비어스 워터마크로 거의 대부분의 워터마크 방법은 이 기법을 사용하고 있다. 논어블리비어스 워터마크나 어블리비어스 워터마크 역시 키가 없으면 워터마크를 검출할 수 없다. 워터마크 알고리듬들을 스터마크(stirmark)라고 불리는 공격 툴을 사용해서 공격자의 영상에 대한 의도적인 공격에 어느 정도의 강인성을 갖는지 테스트하는 것이 일반적이다. 이 툴은 영상을 압축(compression), 절삭(cropping), 회전(rotation), 확대 및 축소(scaling), 가로 대 세로 비율 변화(aspect ratio change) 등의 공격을 가한다. 이러한 알고리듬들의 강인성 증가로 인해 최근에는 영상 자체 내의 공격보다는 워터마크 알고리즘을 사용하는 환경의 취약점을 공격하는 기법들이 나오고 있다.[12-20] 이 방법들 중에서 서로 다른 다중 정보를 직교성(orthogonality)과 랜덤 시퀀스 방법을 이용하여 커버 영상에 다중 정보를 삽입하고 이를 복원하는 방법이 제안되었다.[13] 이 방법은 직교성을 이용하여 복호화키들 간의 상호 상관 성분을 제거하여 다중 정보 재생이 가능함을 제안하였으며 커버영상 스펙트럼 성분의 완벽한 제거를 위하여 문턱치(thresholding) 처리가 필요하다. 한편으로 웨이블릿에 근거한 CDMA 워터마크 방법으로 커버 영상에 삽입할 수 있는 다중 정보의 량과 커버 영상 손실을 최대한 줄이기 위한 삽입조절 연산자의 영향을 모의실험을 통하여 조절연산자의 값이 매우 작은 값에서 다중 정보 삽입이 가능함을 나타내었다.[18]

본 논문에서는 하나의 워터마크된 영상에 서로 다른 다중 정보를 암호화하여 삽입하고 이를 다중 복호화 키들을 사용하여 원하는 정보만을 복원하고 왈시 코드를 커버 영상에 곱하여 복원 영상의 사이드 로브 성분을 제거하는 시스템을 제안하였다. 제안한 삽입(embedding) 영상들은 원 영상들을 제로 패딩(zero-padding)하고 무작위 위상 영상을 곱하여 푸리에 변환 후 이 변환된 영상들의 실수부를 확산 및 위상 변조시키고 새로운 무작위 위상 영상들과 곱한 뒤 허수부를 취하고 이를 독립적으로 생성된 왈시 코드(Walsh code) 영상을 곱하여 생성한다. 이때 곱한 무작위 위상 영상들의 실수부에 왈시 코드를 곱하여 복호화 키로 사용하고 독립적으로 만들어진 삽입 영상들과 커버(cover) 영상에 새로운 왈시 코드 영상을 곱한 후 서로 더하여 워터마크 혹은 스테고 영상을 생성한다. 따라서 허가받지 않은 사용자가 세기검출 및 위상 측정 방법 등을 통하여 삽입된 영상의 위상 및 세기 값을 추출하더라도 복호화 키들의 정보와 확산 및 비확산 코드의 정보 없이는 원 영상들의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하다. 복호화 과정은 삽입된 워터마크 영상과 복호화 키 영상을 곱하여 만들어진 영상을 왈시 코드 크기만큼 비확산 과정을 통해 원 영상들의 크기로 줄인 후 이 영상을 역-푸리에 변환하여 출력평면에 DC성분 제거를 위한 공간필터를 두어서 원 영상들을 복원한다. 이때 커버 영상에 왈시 코드를 곱하므로 복원과정에서 커버영상의 사이드 로브(side lobe) 성분이 제거되어 복원 영상의 해상도를 높일 수 있으며 또한 다중 복호화 키들을 사용함으로써 하나의 워터마크 영상에 삽입된 다중 삽입 영상들 중에서 원하는 정보만 복원이 가능함을 컴퓨터모의실험을 통하여 확인하였다.

II. 제안한 워터마크 및 복원 과정

삽입할 제로 패딩된 원 영상들 $f_i(x,y)$, 무작위 위상 영상 $\exp[jn(x,y)]$, 여기서 $n(x,y)$는 정규화 된 $[0,2\pi]$사이 값을 가진다. 먼저 입력 영상들과 무작위 영상을 위상 변조하여 곱한 후 푸리에 변환하여 실수 값을 취하면 푸리에 면에 균일하게 분포된다. 이 부호화된 영상은

$$E_i(\zeta,\eta) = \mathrm{FT}_{\mathrm{real}}\{f_i(x,y)\exp[jn(x,y)]\}, \tag{1}$$

로 표현되고 여기에서 $\mathrm{FT}_{\mathrm{real}}\{\bullet\}$는 푸리에 변환 후 실수 값을 취하는 연산이고 아래첨자 i는 원 영상들의 개수를 의미하고 이를 정규화하면 [-1, 1] 사이의 값을 갖는다. 이 영상들을 다시 왈시 코드의 크기에 맞게 확장시켜 $A_i(\zeta,\eta)$로 표현하면,

$$\begin{aligned} A_i(\zeta,\eta) &= E_i[s_x(\zeta-1)+\alpha, s_y(\eta-1)+\beta] \\ &\quad where\ \ \alpha = 1,2,3,\cdots,s_x,\ \ \beta = 1,2,3,\cdots,s_y \end{aligned} \tag{2}$$

와 같으며 여기서 s_x와 s_y는 각각 왈시 코드 영상의 크기에

맞게 확장시키기 위한 요소의 최대값이며 α와 β는 확장 요소로 사용된다. 이렇게 확장된 영상과 새로운 무작위 영상들을 위상변조한 후 곱한 식은,

$$\exp[j2\pi r_{hi}(\zeta,\eta)] = \exp[j2\pi\{A_i(\zeta,\eta)+r_i(\zeta,\eta)\}], \tag{3}$$

와 같이 표현되며 $r_i(\zeta,\eta)$는 무작위 영상들로 삽입 영상들의 암호화 수준을 향상시키고 복호화 키들의 주성분으로 사용한다. 식 (3)의 좌변 항에 허수 값, 우변 항의 $\exp[j2\pi r_i(\zeta,\eta)]$ 성분에 실수 값을 취하면

$$\begin{aligned}\widetilde{h}_i(\zeta,\eta) &= \mathrm{Im}\{\exp[j2\pi r_{hi}(\zeta,\eta)/K]\} \\ &= \sin[2\pi r_{hi}(\zeta,\eta)/K] \\ \widetilde{k}_i(\zeta,\eta) &= \mathrm{Re}\{\exp[2\pi r_i(\zeta,\eta)/K]\} \\ &= \cos[2\pi r_i(\zeta,\eta)/K],\end{aligned} \tag{4}$$

와 같고 여기에서 $\mathrm{Im}\{\bullet\}$, $\mathrm{Re}\{\bullet\}$. 그리고 정수 K는 각각 허수부와 정수부 그리고 가시성을 조절하는 연산자로 복원 영상의 해상도를 높이고 스테고 영상과 커버 영상 사이의 PSNR을 높이는데 사용된다. 여기서 허수 값의 영상들과 실수 값의 영상들에 독립적인 왈시 코드 영상들을 곱하여 각각 삽입 영상들과 복호화 키들로 사용한다. 다중 삽입 및 복호화를 위해 이 삽입 영상들과 커버 영상에 새로운 왈시 코드 영상을 곱한 후 서로 더한 스테고 영상은

$$S(\zeta,\eta) = \alpha\sum_{i=1}^{n} W_i\widetilde{h}_i(\zeta,\eta) + W_k C(\zeta,\eta), \tag{5}$$

와 같고 여기에서 $C(\zeta,\eta)$는 커버 영상으로 [0, 1] 사이의 값을 갖고 $S(\zeta,\eta)$는 삽입 영상들과 커버 영상이 선형적으로 중첩되어진 스테고 영상이다. 여기에서 α는 삽입 영상들을 커버 영상에 최대한 영향을 줄이기 위해 조절하는 연산자이고 n은 영상의 개수이다. W_i와 W_k는 왈시 코드를 이용하여 생성한 이진위상영상이다. 삽입 영상과 복호화 키에는 왈시 코드가 곱해져 있으므로 영상의 크기가 왈시 코드의 크기만큼 확산되어 영상 복원 시 그 확산된 부분만큼 비확산 처리과정이 필요하다. 따라서 왈시 코드의 크기와 정보를 알아야 원 영상을 복원할 수 있고 삽입 및 복호화 키 영상들의 생성 과정에서 곱한 왈시 코드와 서로 다른 왈시 코드를 커버 영상에 곱하므로 복원 과정에서 커버 영상 정보에 의해 발생되는 복원 영상의 사이드 로브(side lobe) 성분이 제거된다.

제안한 복원 방법은 원 영상을 얻기 위해 스테고 영상과 복호화 키를 곱하고 비확산을 거친 후 역 푸리에 변환을 하면 실수 값의 푸리에 변환에 의해 원점에 대칭하는 원하는 원 영상을 얻을 수 있다. 우선 스테고 영상과 임의의 복호화 키 $\widetilde{k}_j(\zeta,\eta)$와의 곱에서 얻어진 수식은

$$\begin{aligned}&\widetilde{k}_j(\zeta,\eta)S(\zeta,\eta) \\ &= W_j\cos[2\pi r_j(\zeta,\eta)/K]\left\{\alpha\sum_{i=1}^{n} W_i\sin[2\pi r_{hi}(\zeta,\eta)/K] + W_k C(\zeta,\eta)\right\} \\ &= \alpha W_i W_j\sum_{i=1}^{n}\sin[2\pi r_{hi}(\zeta,\eta)/K]\cos[2\pi r_j(\zeta,\eta)/K] \\ &\quad + W_j W_k C(\zeta,\eta)\cos[2\pi r_j(\zeta,\eta)/K]\end{aligned} \tag{6}$$

와 같이 표현할 수 있으며 여기에서 식 (6)의 우변 항의 첫 번째 성분은 K값이 충분히 크다면 테일러 급수전개로 근사화하여 정리하면

$$\begin{aligned}&W_i W_j\sum_{i=1}^{n}\left[\frac{\alpha}{2}\sin[2\pi\{r_{hi}(\zeta,\eta)-r_j(\zeta,\eta)\}/K] + [\frac{\alpha}{2}\sin[2\pi\{r_{hi}(\zeta,\eta)+r_j(\zeta,\eta)\}/K]\right] \\ &= W_i W_j\sum_{i=1}^{n}\left[\frac{\alpha}{2}\sin[2\pi A_i(\zeta,\eta)/K] + \frac{\alpha}{2}\sin[2\pi\{A_i(\zeta,\eta)+2r_j(\zeta,\eta)\}/K]\right] \\ &\approx W_i W_j\sum_{i=1}^{n}\left[\frac{\alpha}{2}\{2\pi A_i(\zeta,\eta)/K + 2\pi\{A_i(\zeta,\eta)+2r_j(\zeta,\eta)\}/K\}\right]\end{aligned} \tag{7}$$

로 표현된다. 식 (7)에서 영상 $A_i(\zeta,\eta)$는 식 (2)를 통하여 확산된 영상이기 때문에 원 영상의 크기만큼 다시 비확산 과정이 필요하다. 따라서 비확산 영상 $D_{Di}'(\zeta,\eta)$는

$$D_{Di}'(\zeta,\eta) = \sum_{\zeta'=0}^{M-1}\sum_{\eta'=0}^{N-1} D_{Si}'(\zeta',\eta')\exp[-j2\pi(\frac{\zeta'\zeta}{M}+\frac{\eta'\eta}{N})], \tag{8}$$

과 같이 표현할 수 있다. 이때 M,N은 왈시 코드를 이용하여 생성한 영상의 한 블록 크기이며, $D_{Si}'(\zeta',\eta')$는 $M\times N$으로 확산된 $A_i(\zeta,\eta)$의 한 블록을 나타내고, ζ, η와 ζ', η'은 동일한 주파수 영역에서의 변수이며 그리고 $\zeta=0$, $\eta=0$일 때 확산된 영상 D_{Si}'의 한 블록만큼 비확산 과정이 처리된다. 그리고 위 식 (8)의 과정을 블록 계수만큼, 즉 원 영상의 크기만큼, 반복적 처리하여 조합을 하면, 원 영상의 크기를 구할 수 있다. 식 (8)을 광학적으로 구현하기 위해서는 현재의 공간 광변조기가 표현할 수 있는 데이터의 범위가 보다 확장됨으로써 가능하리라 판단된다. 식 (6)의 우변 항 첫 번째 성분에서 n개의 영상들과 곱하여진 임의의 복호화 키 $\widetilde{k}_j(\zeta,\eta)$에서 $W_i W_j$는 왈시 코드 영상들의 곱으로 비확산과정을 통하여 $i=j$일 경우 $W_i W_j=1$이 되고 $i\neq j$일 경우에는 $W_i W_j=0$이 된다. 또한 식 (6)의 우변 항 두 번째 성분에서 $j\neq k$이고 따라서 $W_j W_k=0$이므로 복원 영상에서 커버영상의 사이드 로브가 제거된다. 비확산과정을 통하여 식 (6)의 우변 항 첫 번째 성분 즉 식 (7)의 비확산된 성분만 남게 되고 이때 식 (7)의 우변항 성분들은 $i=j$일 경우를 제외하고 모든 성분이 0이 되고 $i=j$일 경우 $A_j(\xi,\eta)$는 식 (2)의 역 과정으로 $E_j(\xi,\eta)$로 표현되고 식 (7)의 우변항 두 번째 성분에서 무작위 영상 $r_j(\xi,\eta)$는 비확산과정을 통하여 거의 상수 값을 가지는 DC성분으로 변환된다. 따라서 식 (8)의 과정을 반복한 후 역-푸리에 변환하면

$$\mathrm{IFT}\{D_{Dj}'(\zeta,\eta)\}=\mathrm{IFT}\left[\frac{2\alpha\pi}{K}E_j(\zeta,\eta)\right]+\mathrm{IFT}\left[\frac{2\alpha\pi}{K}(\mathrm{quasi-constant})\right]$$
$$\approx\frac{2\alpha\pi}{K}f_j'(x,y)\exp[jn'(x,y)]+\frac{2\alpha\pi}{K}\delta(x,y), \quad (9)$$

로 표현되며 여기서 IFT{ • }는 역-푸리에 변환 연산이고 $f_j'(x,y)\exp[jn'(x,y)]$는 $\mathrm{Re}[\mathrm{FT}\{\exp[f_j(x,y)jn(x,y)]\}]$은 역-푸리에 변환의 결과이며 식 (9)의 우변항 두 번째 항은 델타 함수로 나타나게 된다. 이 DC성분 $\delta(x,y)$을 공간 필터를 이용하여 제거한 후 CCD에 나타나는 출력세기함수 $R_{CCD}(x,y)$는

$$R_{CCD}(x,y)=\left|\frac{2\alpha\pi}{K}f_j'(x,y)\exp[jn'(x,y)]\right|^2$$
$$=\left|\frac{2\alpha\pi}{K}f_j'(x,y)\right|^2 \quad (10)$$

와 같이 표현된다. 식 (1)에서 제로 패딩한 임의의 영상 $f_j(x,y)$를 푸리에 변환하여 실수값만 취해 역 푸리에 변환한 영상인 $f_j'(x,y)$는 제로 패딩하기 전 영상이 각각 영차성분을 중심으로 쌍으로 존재하는 특성을 가지게 되고 따라서 식 (10)에서와 같이 복호화 과정을 거치게 되면, 한 영상 내에 두 개의 원 영상 성분이 대칭적으로 존재하는 $f_j'(x,y)$영상이 CCD 평면상에서 나타난다.

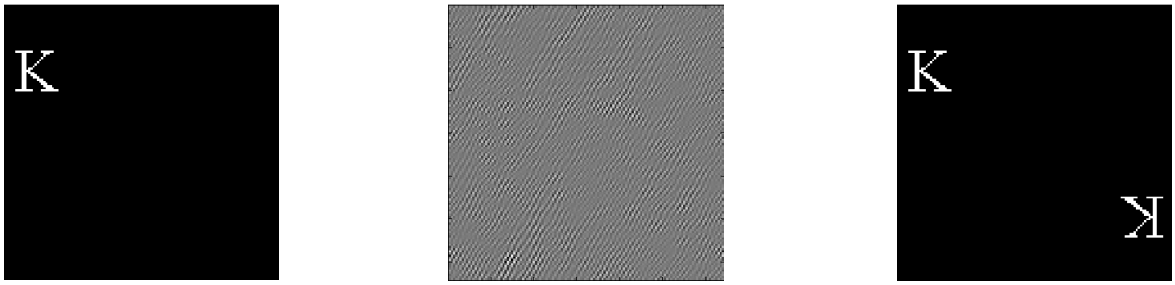
(a) (b) (c) (d)

그림 1. 컴퓨터 모의실험에 사용되는 원 영상들(64×64): (a) the letter 'K', (b) the letter 'M', (c) the letter 'U', and (d) the letter 'E'.

III. 컴퓨터 모의실험 및 고찰

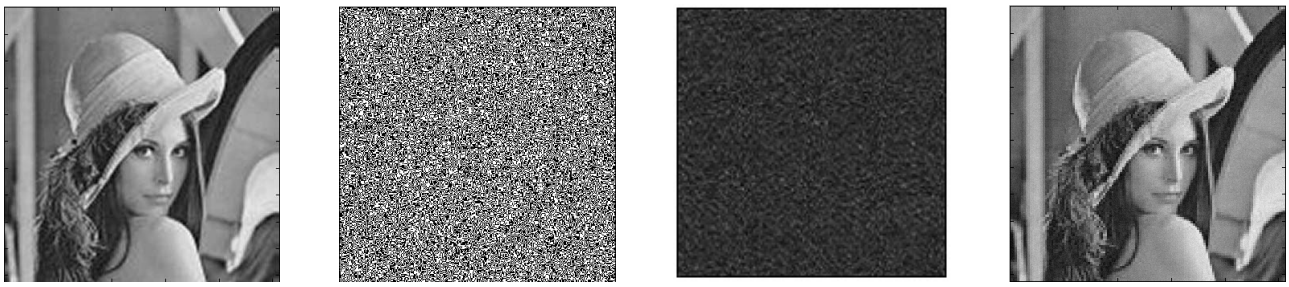
제안한 방법의 타당성을 검증하기 위해 컴퓨터 모의실험을 수행하였다. 하나의 커버 영상에 4개의 다중 영상들을 삽입하기 위하여 4개의 원 영상을 사용하였으며 그 영상들을 그림 1에 나타내었으며 이는 제로 패딩하기 전 영상들 즉 'K'와 'M', 'U', 'E'로서 그 크기는 64×64이며 이진 값을 가진다. 여기에서 제로 패딩 시 그림 1(a)와 그림 1(b)는 2사분면에 위치시키고 그림 1(c)와 그림 1(d)는 1사분면에 위치시켜서 컴퓨터 모의실험을 수행한다. 그림 2는 실수 값 복원영상의 한 예로서 그림 2(a)는 64×64 픽셀 크기를 가지는 그림 1(a)의 영상을 제로 패딩한 영상 $f_i(x,y)$이며 그 크기는 128×128이고 그림 2(b)는 그림 2(a)에 무작위 영상 $n(x,y)$을 위상 변조하여 곱한 후 푸리에 변환하여 실수 값을 갖는 부호화된 영상 $E_i(\zeta,\eta)$이고 그림 2(c)는 그림 2(b)를 역-푸리에 변환하여 표현되는 복원 영상의 예이다.

그림 3은 8×8 크기의 확산과정을 통하여 만들어진 영상들로서 그 크기는 각각 1024×1024이고 그림 3(a)는 커버 영상 $C(\zeta,\eta)$이고 그림 3(b)는 실험에 사용된 왈시 코드 영상 W_i의



(a) (b) (c)

그림 2. 실수 값 복원영상의 예(128×128) : (a) 제로 패딩한 원 영상 $f_i(x,y)$, (b) 실수 값으로 부호화된 영상 $E_i(\zeta,\eta)$, (c) 복원 영상.



(a) (b) (c) (d)

그림 3. 확산과정을 통하여 만들어진 영상들(1024×1024): (a) 커버 영상 $C(\zeta,\eta)$, (b) 왈시 코드 영상 W_i, (c) 삽입된 4개의 영상 $\alpha\sum_{i=1}^{4}W_i\tilde{h}_i(u,v)$, (d) 워터마크 영상 $S(\zeta,\eta)$.

한 예이며 그림 3(c)는 부호화된 각각의 영상과 서로 다른 왈시 코드 영상과 곱하여 만들어진 삽입 영상 $\alpha\sum_{i=1}^{4} W_i\widetilde{h}_i(u,v)$이며 그림 3(d)는 그림 3(a)와 그림 3(c)로 만들어진 영상들을 서로 더한 워터마크 즉 스테고 영상 $S(\zeta,\eta)$이다. 삽입 영상에 사용된 왈시 코드 영상은 Hadamard 행렬을 64×64로 생성한 뒤, 행의 크기가 64인 왈시 코드를 8×8 영상으로 대응시켰으며, 모두 1의 값인 코드의 첫 번째 행을 제외한 63개의 행을 이용하여, 삽입 영상의 각 픽셀 크기만큼 무작위 왈시 코드로 왈시 코드 영상(1024×1024)을 만들었다. 이때 각각의 삽입 영상들에 서로 다른 왈시 코드를 곱하여 사용하였으며, 만약 동일한 왈시 코드를 사용하여 중복성이 허용되면, 복원할 때 서로 간섭을 주어 원 영상의 복원이 어렵게 되고 또한 왈시 코드를 8×8로 확산 및 비확산 시키는 과정도 삽입영상을 복원하는 필수적인 요소로서 이 정보 없이는 원 영상의 복원이 어렵게 된다.

제안한 방법에서 커버 영상과 워터마크 영상의 해상도가 α와 K 값에 영향을 미치게 되므로 그에 따른 커버 영상과 워터마크 영상의 해상도를 표현하는 정량적 지표로서 첨두치 신호 대 잡음비 PSNR(Peak Signal to Noise Ratio)를 나타내었다. 여기서 사용된 PSNR의 표준은

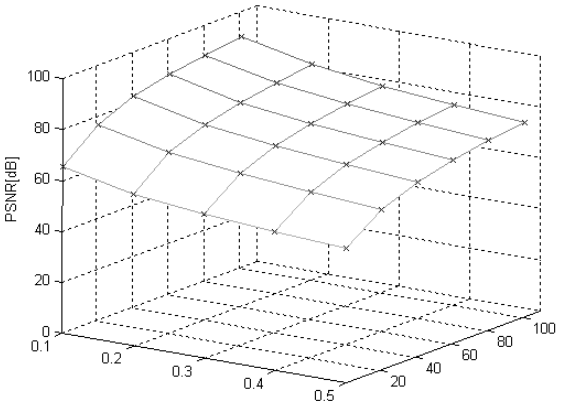


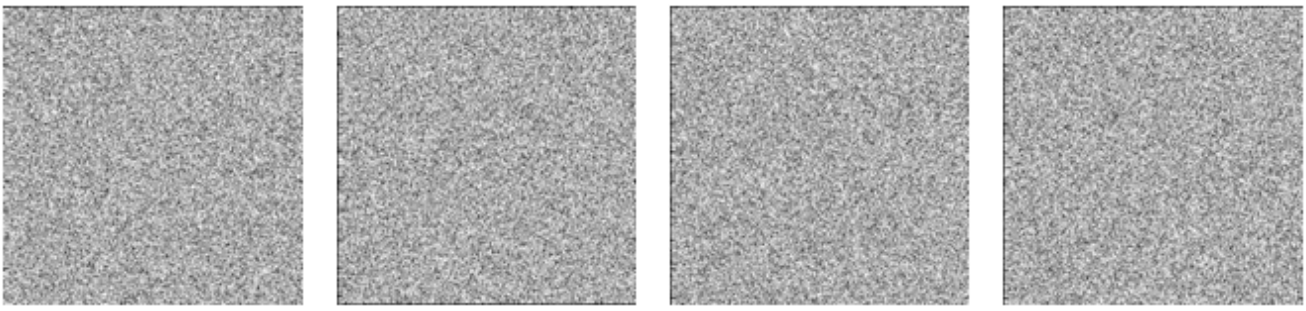
그림 4. α와 K 값의 변화에 따른 커버 영상과 워터마크 영상 사이의 PSNR.

$$\mathrm{PSNR} = 20\log\frac{2^{n_{bit}}-1}{\left\{\frac{1}{N\times M}\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left[\|f(x,y)|-|f'(x,y)\|^2\right]\right\}^{1/2}} \tag{11}$$

이며 여기에서 $f(x, y)$와 $f'(x, y)$는 각각 커버 영상과 워터마크 영상이며 n_{bit}는 픽셀을 표현하는 비트수이다. 그림 4은 α와 K값의 변화에 따른 커버 영상과 워터마크 영상 사이의 PSNR을 구한 것이다. 그림 4에서 보는 바와 같이 α 값이 커질수록 K 값이 적을수록 손실이 커진다는 것을 알 수 있다. 제안한 방법에서는 α와 K 값을 각각 0.2와 70으로 적절한 값을 선택하여 81.25[*dB*]에서 컴퓨터 모의실험을 실행하였다. 기존의 방법에서는[18] 조절 연산자 α 값이 0.02를 기준으로 하였으나 제안한 방법에서는 10배의 높은 값인 0.2를 사용함으로써 조절 연산자에 보다 강인성을 가지므로 효율적인 다중 영상 삽입이 가능함을 알 수 있다.

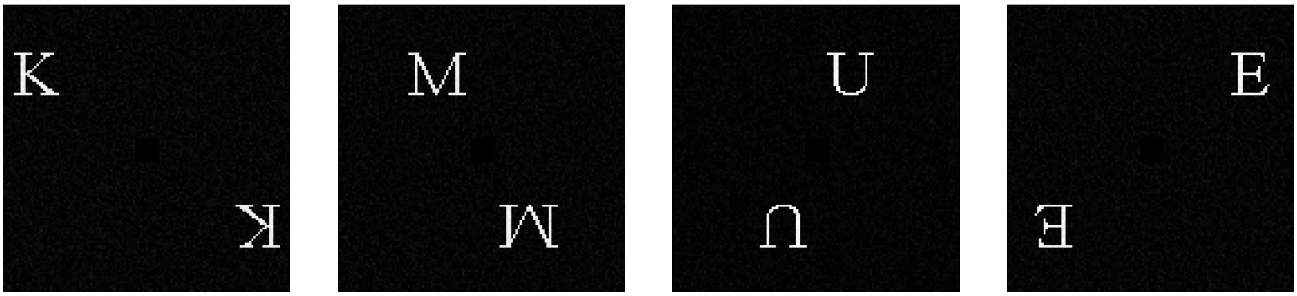
복원 과정에서는 스테고 영상과 임의의 복호화 키 영상을 곱하여 비확산 시킨 후 역-푸리에 변환을 하면 복원 영상을 얻을 수 있다. 그림 5(a)에서 그림 5(d)는 각각 'K', 'M', 'U'와 'E'를 복원하기 위한 복호화 키 영상(1024×1024)들이고 그림 6(a)에서 그림 6(d)는 그림 5의 복호화 키들을 각각 사용하여 복원한 'K', 'M', 'U'와 'E'의 복원 영상들이다. 제안한 방법은 하나의 워터마크 영상에서 원하는 삽입된 영상을 복호화 키를 사용하여 복구가 가능하고 커버 영상의 사이드로브가 제거된 복원 영상을 얻을 수 있다. 기존의 방법에서 커버영상 스펙트럼 성분의 완벽한 제거를 위하여 문턱치(thresholding) 처리가 필요하였으나 제안한 방법에서는 커버 영상 자체의 성분이 왈시 코드에 의해 제거되고 무작위 영상들은 비확산과정과 푸리에 변환에 의해 DC성분으로 변환됨으로써 복원 영상의 해상도를 높일 수 있다.

또한 워터마크 영상은 계속적인 사용 및 잘못된 관리로 인하여 정보의 손실이 발생할 수 있음으로 워터마크 영상을 임의로 블로킹하여 그에 대응하는 복원 영상을 표현하였다. 그림 7(a)에서 그림 7(d)는 워터마크 영상이 각각 x축 방향으로 5%, 25%, 50%, 75% 정보의 손실 즉 블로킹이 발생한 경우의 워터마크 영상이며, 그림 8은 그림 7에 대응하는 복원 영



(a) (b) (c) (d)

그림 5. 영상 복원을 위한 복호화 키 영상들 : (a) 'K' 복호화 키 영상, (b) 'M' 복호화 키 영상, (c) 'U' 복호화 키 영상, (d) 'E' 복호화 키 영상.

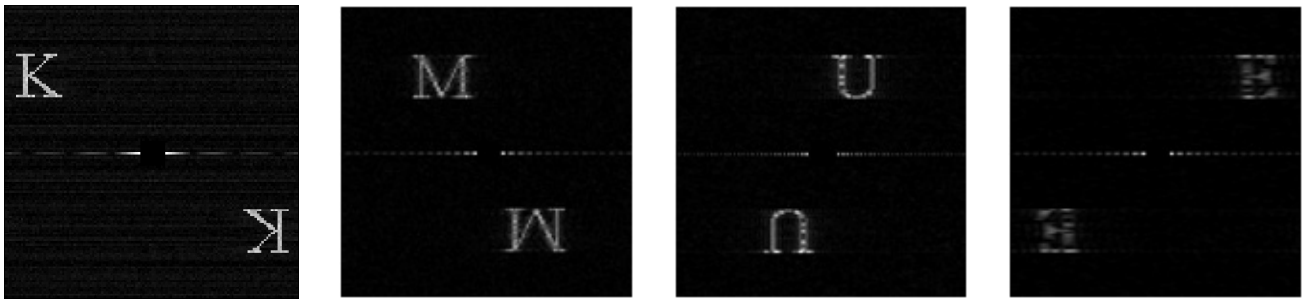


(a) (b) (c) (d)

그림 6. 복원 영상들 : (a) ‘K’ 복호화 키로 복원한 영상, (b) ‘M’ 복호화 키로 복원한 영상, (c) ‘U’ 복호화 키로 복원한 영상, (d) ‘E’ 복호화 키로 복원한 영상.

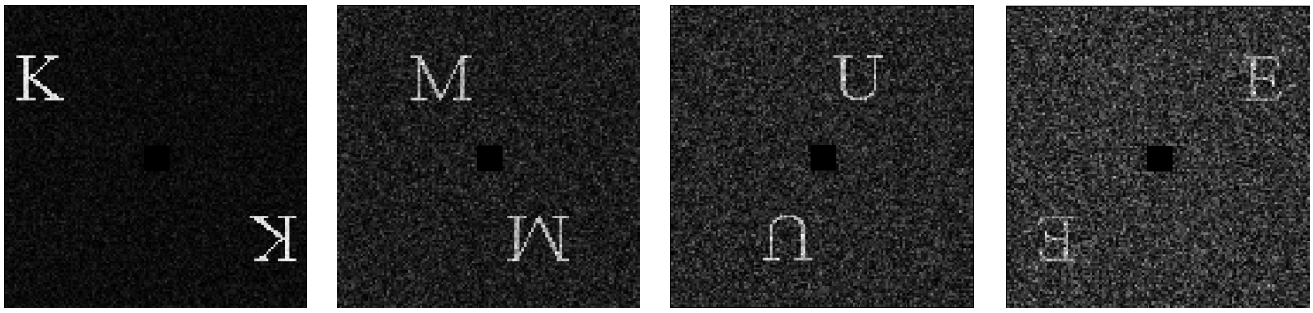
(a) (b) (c) (d)

그림 7. 블로킹된 워터마크 영상: (a) 5%, (b) 25%, (c) 50%, (d) 75%.



(a) (b) (c) (d)

그림 8. 블로킹된 워터마크 영상으로 복원한 영상: 워터마크 영상이 (a) 5% 블로킹되었을 때 ‘K’ 복호화 키에 의한 복원 영상, (b) 25% 블로킹되었을 때 ‘M’ 복호화 키에 의한 복원 영상, (c) 50% 블로킹되었을 때 ‘U’ 복호화 키에 의한 복원 영상, (d) 75% 블로킹되었을 때 ‘E’ 복호화 키에 의한 복원 영상.



(a) (b) (c) (d)

그림 9. 압축된 워터마크 영상으로 복원한 영상 : 워터마크 영상이 (a) 95%로 압축되었을 때 ‘K’ 복호화 키에 의한 복원 영상, (b) 80%로 압축되었을 때 ‘M’ 복호화 키에 의한 복원 영상, (c) 65%로 압축되었을 때 ‘U’ 복호화 키에 의한 복원 영상, (d) 50%로 압축되었을 때 ‘E’ 복호화 키에 의한 복원 영상.

상들을 나타내었다. 그림 8(a)는 워터마크 영상이 5% 블로킹 되었을 때 'K' 복호화 키에 의한 복원 영상, 그림 8(b)는 25% 블로킹되었을 때 'M' 복호화 키에 의한 복원 영상, 그림 8(c)는 50% 블로킹되었을 때 'U' 복호화 키에 의한 복원 영상이며 그림 8(d)는 75% 블로킹되었을 때 'E' 복호화 키에 의한 복원 영상이다.

그림 9는 또 다른 강인성 테스트를 위하여 워터마크 영상이 JPEG 압축되었을 경우 복원 영상을 각각 나타내었다. 그림 9(a)는 워터마크 영상이 95%로 압축되었을 때 'K' 복호화 키에 의한 복원 영상, 그림 9(b)는 80%로 압축되었을 때 'M' 복호화 키에 의한 복원 영상, 그림 9(c)는 65%로 압축되었을 때 'U' 복호화 키에 의한 복원 영상이며 그림 9(d)는 50%로 압축되었을 때 'E' 복호화 키에 의한 복원 영상이다. 컴퓨터 모의실험을 통해서 워터마크 영상이 블로킹 및 압축이 되더라도 원 영상이 복원됨을 알 수 있다.

VI. 결 론

본 논문에서는 하나의 워터마크된 영상에 서로 다른 다중 정보를 암호화하여 삽입하고 이를 다중 복호화 키들을 사용하여 원하는 정보만을 복원하는 시스템을 제안하였다.

컴퓨터 모의실험을 통하여 제안한 암호화 방법을 검증하였으며 스테고 영상이 블로킹되더라도 원 영상의 정보를 가지고 있음을 확인하였다. 원 영상들은 왈시 코드의 행 크기만큼 증가한다는 단점이 있으나, 이는 코드의 특성상 필수부가 결한 요소이며, 왈시 코드의 크기 증가는 암호화 수준을 높이며, 계층의 수 또한 증가하는 장점이 있다. 복호화는 왈시 코드 영상을 생성할 때와 동일한 크기와 모양으로 비확산 과정을 수행한 후 역-푸리에 변환을 통하여 정보 영상을 복원하였다. 왈시 코드는 동일한 코드가 입력되면 1이 되며, 다른 코드가 입력되면 0이 되는 직교성의 특성에 의해 여러 코드를 동시에 합하여도, 각각 하나의 코드 특성은 상쇠 되거나 첨가 되지 않는 장점을 가진다. 그래서 단 하나의 커버 영상에 서로 다른 영상들을 삽입하여 삽입된 워터마크 영상을 생성이 가능하고 동일한 왈시 코드 영상이 포함된 다중 복호화 키 영상들로 복원이 가능하다. 또한 코드의 정보뿐만 아니라 원 영상의 확산된 크기와 모양의 정보를 알아야 원 영상들의 복원이 가능하다. 제안한 방법의 광학적 구현은 그레이 값을 정밀히 표현하여 영상의 왜곡을 최소화 할 수 있는 컴퓨터 형성 홀로그램의 제작이나 세기와 위상 정보를 기록 및 표현할 수 있는 공간 광 변조기 같은 광학 소자의 개발이 향상된다면 실현 가능하리라 판단된다.

참고문헌

[1] B. Schneier, *Applied cryptography-protocol, algorithms, and source code in C*, 2nd ed., John Wiley & Sons, New York, 1995.

[2] A. Shamir, "How to share secret," *Communications of ACM*, vol. 22, pp. 612-613, 1979.

[3] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.*, vol. 33, no. 6, pp. 1752-1756, 1994.

[4] R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," *Opt. Eng.*, vol. 35, no. 9, pp. 2464-2469, 1996.

[5] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767-769, 1995.

[6] B. Javidi and E. Ahouzi, "Optical security system with Fourier plane encoding," *Appl. Opt.*, vol. 37, no. 26, pp. 6247-6255, 1998.

[7] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," *Opt. Eng.*, vol. 39, no. 8, pp. 2031-2035, 2000.

[8] M. Yamazaki and J. Ohtsubo, "Optimization of encrypted holograms in optical security systems," *Opt. Eng.*, vol. 40, no. 1, pp. 132-137, 2001.

[9] B. Javidi, A. Sergent, G. Zhang, and L. Guibert, "Fault tolerance properties of a double phase encoding encryption technique," *Opt. Eng.*, vol. 36, no. 4, pp. 992-998, 1997.

[10] B. Wang, C. C. Sun, W. C. Su, and A. E. T. Chiou, "Shift-tolerance property of an optical double-random phase-encoding encryption system," *Appl. Opt.*, vol. 39, no. 26, pp. 4788-4793, 2000.

[11] C. H. Yeh, H. T. Cahng, H. C. Chien, and C. J. Kuo, "Design of cascaded phase Keys for a hierarchical security system," *Appl. Opt.*, vol. 41, no. 29, pp. 6128-6314, Oct. 2002.

[12] N-J Kim, D-H Seo, and S-G Lee, C-M Shin, K-B Cho, and S-J Kim, "Hierarchical Image Encryption System Using Orthogonal Method," *Journal of OSK*, vol. 17, no. 3, 2006.

[13] 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.

[14] D. Abookasis, O. Montal, O. Abramson, and J. Rosen, "Watermarks encrypted in a concealogram and deciphered by a modified joint-transform correlator," *Appl Opt.*, vol. 44, no. 15, pp. 3019-3023, 2005.

[15] G. Situ, J. Zhang, "Image hiding with computer-generated phase codes for optical authentication," *Opt. Commun.* 245 pp. 55-65, 2005.

[16] M. Z. He, L. Z. Cai, Q. Liu, X. C. Wang, X. F. Meng, "Multiple image encryption and watermarking by random phase matching," *Opt. Commun.* 247, pp. 29-37, 2005.

[17] Hsuan T. Chang and Chung L. Tsan, "Image watermarking by use of digital holography embedded in the discrete-cosine-transform domain," *Appl. Opt.*, vol. 44, no. 29, pp. 6211-6219, 2005.

[18] D. P, J. W, S. Y, S. W, and A. L, "CDMA based Multiple-user digital watermarking," Proceedings of the 2006 inter-

national conference on intelligent information hiding and multimedia signal processing, 2006.
[19] K-B. Cho, D-H. Seo, and S-J. Kim, "Practical Image Hiding Method Using a Phase Wrapping Rule and Real-Valued Decoding Key," *Opt. rev.*, Vol. 14, No. 3, 2007.
[20] S. Huang and J. K. Wu, "Optical Watermarking for Printed Document Authentication," *IEEE Trans. on Information Forensics and Security*, vol. 2, no. 2, pp. 164-173, 2007.

Image Watermark Method Using Multiple Decoding Keys

Hyung-Seok Lee and Dong-Hoan Seo†

Division of Electrical & Electronics Engineering, Korea Maritime Univerity, Busan, 606-791, Korea

†*E-mail: dhseo@hhu.ac.kr*

Kyu-Bo Cho

School of Electrical Engineering & Computer Science, Kyungpook National University, Daegu 702-701, Korea

(Received July 8, 2008; Revised manuscript August 14, 2008; Accepted August 15, 2008)

In this paper, we propose an image watermark method using multiple decoding keys. The advantages of this method are that the multiple original images are reconstructed by using multiple decoding keys in the same watermark image, and that the quality of reconstructed images is clearly enhanced based on the idea of Walsh code without any side lobe components in the decoding process. The zero-padded original images, multiplied with random-phase pattern to each other, are Fourier transformed. Encoded images are then obtained by taking the real-valued data from these Fourier transformed images. The embedding images are obtained by the product of independent Walsh codes, and these spreaded phase-encoded images which are multiplied with new random-phase images. Also we obtain the decoding keys by multiplying these random-phase images with the same Walsh code images used in the embedding images. A watermark image is then made from the linear superposition of the weighted embedding images and a cover image, which is multiplied with a new independent Walsh code. The original image is simply reconstructed by the inverse-Fourier transform of the despreaded image of the multiplication between the watermark image and the decoding key. Computer simulations demonstrate the efficiency of the proposed watermark method with multiple decoding keys and a good robustness to the external attacks such as cropping and compression.

OCIS codes: (070.0070) Fourier optics and optical signal processing; (070.2590) Fourier transforms; (100.1160) Analog optical image processing; (120.5060) Phase modulation.