《연구논문》 Hankook Kwanghak Hoeji, Volume 17, Number 3, June 2006

직교성을 이용한 계층적 영상 암호화

김남진

경북대학교 정보통신학과

㉾ 701-702 대구광역시 북구 산격동 1370

서동환† · 이성근

한국해양대학교 전기전자공학부

㉾ 606-791 부산광역시 영도구 동삼동 1

신창목 · 조규보 · 김수중

경북대학교 전자전기컴퓨터학부

㉾ 701-702 대구광역시 북구 산격동 1370

(2006년 3월 16일 받음, 2006년 6월 2일 수정본 받음)

본 논문에서는 직교성의 특성을 가진 Walsh code 영상과 무작위 위상 영상을 이용하여 계층적인 영상의 암호화 및 복호화로 영상 정보의 수준에 따른 효율적인 정보보호와, 암호화의 수준을 향상시키는 방법을 제안하였다. 제안한 암호화 과정은 각각의 원 영상과 무작위 위상 영상을 곱한 영상을 푸리에 변환 후, Walsh code 영상과 이진 무작위 위상영상을 곱한 영상에 확산시켜 암호화한다. 복호화 키는 암호화 과정에 사용된 Walsh code 영상을 정보의 수준에 따라 더함으로써 계층적인 복호화 키를 생성한다. 그러므로 하나의 복호화 키로도 정보 보호의 수준에 따라 각 암호화 영상을 복호화할 수 있다. 또한 이진 무작위 위상과 무작위 위상 영상은 암호화 영상을 백색 잡음의 패턴과 유사하여 암호화 수준이 높은 장점을 가진다. 컴퓨터 실험과 고찰을 통하여 암호화의 적합함을 확인하였다.

주제어 : Hierarchical encryption, Walsh coding, Random phase encoding.

I. 서 론

현대 정보화 사회에서는 정보 통신의 발달에 따라 막대한 양의 정보가 점점 더 빠른 속도로 교환되고 있다. 또한 통신과 컴퓨터의 결합으로 새로운 형태의 경제와 문화 활동이 혁명적으로 발전하고 있고, 이런 발전이 우리 생활을 보다 편리하게 만들 뿐만 아니라, 새로운 가치 창조의 기회를 증가시켜서 경제적, 사회적 부가 막대하게 창출되고 있다. 하지만 빠른 속도의 기술발전에 대응하는 제도적, 기술적 장치의 미비로 인한 정보의 유출 때문에 또 다른 피해가 발생하고 있어서 정보의 보호가 매우 중요한 문제로 대두되며, 과거에는 정보 보호 문제가 주로 국가와 기업의 문제였으나, 현 정보 사회에서는 개인에게도 심각한 문제가 되며, 특히 인터넷을 통한 정보의 공유와 개방으로 인하여 정보에 대한 불법 침입이 새로운 사회적 문제로 부각되고 있다. 또한 정보를 기반으로 하는 산업의 발전으로 개인의 정보와 신용이 더욱 더 중요시되고, 여권, 신용카드, 은행 카드 등의 개인 신분증의 사용이 늘어나고 있다. 그러나 프린터, 스캐너 및 복사기 등의 컴퓨터 관련 장비들과 소프트웨어 기술의 발달로 화폐뿐만 아니라 각종 카드의 복제가 보다 정교하게 이루어지고 있다. 이에 따라 위조 방지 시스템에 관한 연구가 전 세계적으로 활발히 이루어지고 있지만, 아직까지 완벽한 보안 시스템은 개발되지 못하고 있다. 따라서 복제나 위조 방지에 관한 연구와 여러 가지 암호화 시스템 개발에 대한 연구가 활발히 진행되고 있다. 이 중 광 암호화 시스템은 광의 고속성과 병렬성을 이용할 수 있어서, 고속으로 대용량의 정보를 처리하는 데 적합하다. 광 암호화 시스템[1,2]은 주로 무작위 위상 마스크 키(random phase mask key)를 사용하여 원 영상을 암호화한다. 이러한 방법들 중에 위상 마스크를 이용한 대표적인 암호화 기법에는 이중 랜덤 위상 암호화(double random phase encryption) 기법[3]이 있다. 이 방법에서 입력 영상은 두 개의 랜덤 위상 마스크에 의해 암호화되며, 두 개의 랜덤 위상 마스크 중에서 하나는 입력 면에 위치되며, 다른 하나는 푸리에 면에 위치된다. 이 방법으로 암호화된 패턴은 백색 잡음(white noise)과 흡사하며, 암호화에서 사용한 랜덤 키에 대한 정보가 없이는 복원하기가 매우 어렵다. 그러나 복호화 과정에서 암호화된 데이터의 푸리에 변환과 푸리에 랜덤 위상 마스크의 복소공액이 서로 곱해진 후 역 푸리에 변환 후 복호화된 원 영상을 재생할 수 있다. 이 방법은 암호화된 패턴이 진폭과 위상으로 표현되는 복소함수이

† E-mail: dhseo@bada.hhu.ac.kr

기 때문에 광학적인 시스템으로 구성하기 위해서는 복소함수를 표현할 수 있는 영상 장치가 필요하며, 올바른 복호화를 위해서는 암호화 과정에서 사용된 랜덤 키의 복소공액이 필요하다는 단점이 있다. 그리고 암호화된 영상은 암호화시 사용한 복호화 키 영상을 가지고 전통적인 4-f 광 상관기나, 간섭계(interferometer),[4] 결합변환 상관기(joint transform correlator)[5]를 이용하여 원 영상을 재생한다. 또한 기존의 디지털 영상처리 시스템은 영상 신호의 세기를 검출해서 대량 복제와 위조가 가능한 반면에 광 암호화 시스템은 영상 신호를 위상 정보로 기록할 수 있기 때문에 인간의 시각이나 세기 검출기로는 위조가 불가능한 장점을 가지고 있다. 따라서 위상 정보는 무작위 위상 마스크 형태로 광 암호화 시스템에 이용되며, projection onto constraint set(POCS)[6,7]기술은 보통 위상 마스크(phase-only mask)를 설계하는 데 이용된다. 이러한 암호화 시스템을 정보의 중요성에 따라 계층적으로 접근을 허용하도록 함으로써 보다 효율적인 정보보호 방법이 현재 제시되고 있다. 기존의 계층적 보안 시스템[8]은 정보의 중요성이 높아질수록 입력 정보가 많아진다는 단점을 가지고 있다.

본 논문에서는 직교성의 특성을 가진 Walsh code[8-11]를 이용하므로 하나의 입력 정보만으로도 하위 정보는 특정한 정보에만 접근이 가능하며, 상위 정보는 더 많은 암호화 정보에 접근이 가능한 계층적인 암호화 방법을 제안하였다. 그리고 암호화의 수준을 높이기 위하여 이중 랜덤 위상 암호화 기법을 응용하였다. 제안한 암호화 방법은 공간영역에서 무작위 위상영상을 곱하여 푸리에 변환을 취하여, 직교성의 특성을 갖는 Walsh code 크기만큼 확장한 영상과 Walsh code로 만들어진 Walsh code 영상과 이진 무작위 위상 영상을 곱하여 암호화 영상을 만들었다. 이때 Walsh code의 크기에 따라 암호화 영상의 크기가 커지나, 계층성의 크기 증가와 복호화 키의 암호화 수준이 높아지며, 외부잡음과 절단성에 강하며, 원 영상 각각의 픽셀에 하나의 Walsh code를 확산시킴으로써 암호화 영상의 암호화 수준을 향상시켰다. 복호화 키는 암호화 영상에 사용된 Walsh code 영상과 이진 무작위 위상 영상을 곱한 영상을 키로 사용하였으며, 계층에 따라 복호화 키를 더하여 계층적인 복호화 키를 만들었다. 이때 직교성의 특성에 의하여 복호화 키를 더하여도 각 키의 원래 특성은 그대로 가지고 있다. 복호화 과정에서는 먼저 암호화 영상에 계층적인 복호화 키를 곱한다. 이때 전자에 사용된 Walsh code 영상과 복호화 키에 포함하고 있는 Walsh code가 동일할 경우 직교성의 특성에 의하여 코드 값들은 1로 변화되어 원 영상의 복원이 가능하나, 서로 다를 경우 0으로 되어 원 영상을 복원하지 못한다. 그리고 암호화 과정에서 원 영상을 Walsh code의 크기와 모양만큼 확산시킨 것에 동일한 크기와 영역만큼 비확산(despread) 과정을 거친 다음 다시 원영상의 크기에 맞게 조합한 후 그 영상을 푸리에 변환하여 원 영상을 복원한다. 컴퓨터 실험을 통하여 제안한 계층적 암호화 시스템의 타당성을 검증하였다.

II. Walsh coding 기법

Walsh code[9-11]는 1923년 Walsh에 의해 직교함수로 소개되었으며, 직교성은 서로 간섭을 주지 않으며, 코드 간에 상관관계가 매우 적은 것을 의미한다. Walsh code 생성법은 "Hadadmard matrix"에 의해 생성되며, 행렬은

$$H_{2N}=\begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix} \tag{1}$$

과 같이 정의된다. 이때 H_1은 1이며, N은 2의 거듭제곱수를 의미한다. 예를 들어 Hadamard 행렬을 이용한 4×4 행렬은

$$H_4=\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} w \\ w_1 \\ w_2 \\ w_3 \end{bmatrix} \tag{2}$$

과 같이 구현된다. 이때 모두 1의 값을 갖는 첫 번째 행을 제외한 두 번째 행부터 w_1, w_2, w_3으로 정의한다면, Hardamard 행렬의 각 행은

$$\frac{1}{T_L} w_i\, w_j{}^T = \begin{cases} 0 & , i \neq j \\ 1 & , i = j \end{cases} \tag{3}$$

의 특성을 갖는다. 이때 T_L은 Hadamard 행렬의 한 행의 크기이며, $w_j{}^T$는 w_j의 전치행렬을 나타낸다. 따라서 위 3개의 Walsh code(w_1, w_2, w_3)는 모두 직교성의 특성을 가지고 있다.

III. 제안한 계층적 암호화 방법

기존의 계층적 암호화 방법에서 하위 계층의 암호화 영상은 소수의 위상 마스크로 복원이 되며, 상위 계층의 암호화 영상은 다수의 위상 마스크로 복원이 가능하였다. 즉 이는 계층성이 높은 영상일수록 하위 영상보다 더 많은 위상 마스크를 필요로 한다. 따라서 본 논문에서 제안한 암호화 방법은 직교성을 갖는 Walsh code를 이용하여 생성한 Walsh code 영상과 무작위 위상 영상을 사용하여, 하나의 복원키 영상만으로 계층적인 암호화 영상의 복원을 가능하게 하였다.

암호화 과정은 각 원 영상에 무작위 위상 영상을 곱한 뒤 푸리에 변환한 후, Walsh code로 구성된 영상을 확장한 뒤, 또 다른 이진 무작위 위상 영상을 곱하여 암호화 영상을 생성하였다. 그리고 복호화 과정은 각 암호화에 사용된 Walsh code 영상과 이진 무작위 위상 영상을 이용하여 계층적인 복호화

키를 생성하였으며, 암호화 과정의 역순으로 처리함으로써 하나의 계층적인 복원키만으로 암호화 영상을 복원하였다.

3.1 암호화 방법

각각의 원 영상 $O_i(x,y)$와 컴퓨터로 발생시킨 무작위 영상 $r_i(x,y)$를 위상 변조하여 원 영상과 곱하여 푸리에 변환하면,

$$A_i(u,v) = \mathcal{F}\{O_i(x,y)\exp[j2\pi r_i(x,y)]\} \tag{4}$$

와 같이 표현된다. 이때 $\mathcal{F}\{\bullet\}$는 푸리에 변환, i는 영상의 수를 나타내며, $r_i(x,y)$은 $[0,1]$ 사이의 값을 가진다. 식 (4)에서 생성된 $A_i(u,v)$를 Walsh code의 크기에 맞게 확장을 시켜 $A_i'(u,v)$를 표현하면,

$$A_i'(u,v) = A_i[s_x(x-1)+\alpha, s_y(y-1)+\beta] \tag{5}$$

$$\text{where } \alpha = 1,2,3,\cdots,s_x,\ \beta = 1,2,3,\cdots,s_y$$

와 같으며 여기서 s_x와 s_y는 각각 Walsh code 영상의 크기에 맞게 확장시키기 위한 요소의 최대값이며 α와 β는 확장 요소로 사용된다. 여기서 Walsh code 영상과 이진 무작위 위상 영상을 곱하여 암호화 영상을 생성한다. 이때 서로 직교성을 가지게 하기 위해 Walsh code 영상은 원 영상의 개수만큼 각각 독립적으로 생성되어야 한다. 따라서 암호화 영상 $E_i(u,v)$는

$$E_i(u,v) = A_i'(u,v)\, W_i \exp[j\pi R_2(u,v)] \tag{6}$$

와 같이 얻을 수 있다. 이때 W_i는 Walsh code를 이용하여 생성한 Walsh code 영상이며, $R_2(u,v)$는 0과 1의 값을 가진다. 이때 원 영상에 곱해진 무작위 위상 영상 $\exp[j2\pi r_i(x,y)]$와 이진 무작위 위상 영상 $\exp[j\pi R_2(x,y)]$는 암호화된 패턴을 백색 잡음의 형태와 유사하게 만들어 주며, 또한 이진 무작위 위상 영상은 복호화 키의 암호화 수준을 높이는 역할을 한다.

제안한 방법은 원 영상을 공간 영역에서 무작위 위상 영상을 곱하고, 주파수 영역에서 이진 무작위 위상 영상을 곱한 이중 랜덤 위상 암호화 영상의 기본적인 틀에 Walsh code를 첨가함으로써 원 영상의 크기가 Walsh code의 크기만큼 확산된 암호화 영상을 생성하였다. 기존의 이중 랜덤 위상 암호화 영상은 이진 무작위 영상만으로 암호화 영상의 복원이 가능하였으나, Walsh code의 크기만큼 확산되어 있기 때문에, 그 확산된 부분만큼 비확산 과정이 필요하다. 따라서 복호화 시 Walsh code의 크기와 Walsh code의 대응 모양을 알아야 원 영상을 복원할 수 있다. 그림 1은 제안한 계층적 암호화 방법의 블록 다이어그램를 나타낸 것이다.

3.2 복호화 방법

제안한 방법으로 암호화된 영상은 암호화 과정에서 사용된

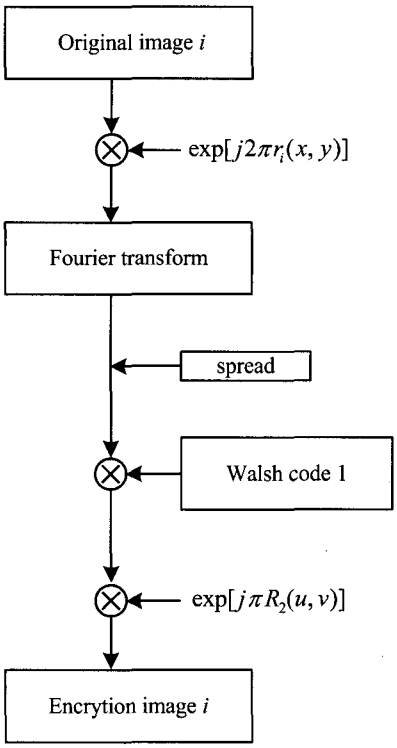


그림 1. 제안한 계층적 암호화 방법의 블록 다이어그램.

2개의 무작위 위상 마스크와 계층적인 복호화 키에 의하여 복호화 할 수 있다. 계층적 복호화 키는

$$L_1 = W_1\exp[j\pi R_2(u,v)] \tag{7}$$

$$L_2 = (W_1+W_2)\exp[j\pi R_2(u,v)]$$

$$L_3 = (W_1+W_2+W_3)\exp[j\pi R_2(u,v)]$$

와 같이 Walsh code 영상을 계층적인 수준에 따라 위 식과 같이 더함으로써 차별적인 암호화 영상에 접근이 가능하다. 예를 들어 상위 계층의 복호화 키 L_3을 사용할 때 3번째 암호화 영상의 확산된 복호화 영상 D_{S3}'는

$$\begin{aligned} D_{S3}' &= E_3 L_3 \\ &= A_3'(u,v)\, W_3 \exp[j\pi R_2(u,v)] \\ &\quad \times (W_1+W_2+W_3)\exp[j\pi R_2(u,v)] \\ &= A_3'(u,v)(W_1+W_2+W_3)\, W_3\, (\exp[j\pi R_2(u,v)])^2 \\ &= A_3'(u,v)(W_1W_3+W_2W_3+W_3W_3)\,(\exp[j\pi R_2(u,v)])^2 \\ &= A_3'(u,v) \end{aligned} \tag{8}$$

와 같이 나타난다. 식 (8)에서 R2(u, v)의 값이 0 혹은 1의 값을 나타내므로 이진 위상 영상의 제곱$(\exp[j\pi R_2(u,v)])^2$은 1이며, 수식 (3)의 Walsh code의 직교성 특성에 의하여

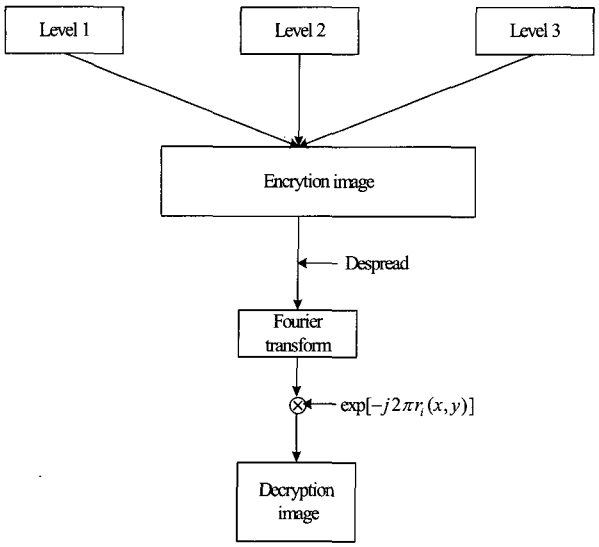


그림 2. 제안한 복호화 방법의 블록 다이어그램.

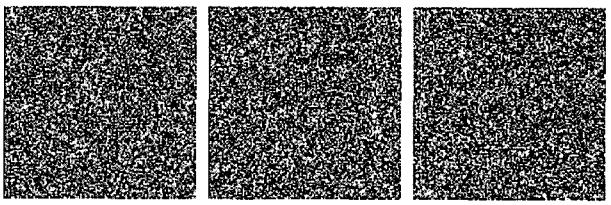
$W_1W_3=0$, $W_2W_3=0$, $W_3W_3=1$의 값을 나타내므로 $W_1W_3+W_2W_{3+}W_3W_3$의 값은 1이 된다. 따라서 비확산 과정을 통하여 i가 3인 암호화 영상 E_3의 비확산 영상 $A_3(u,v)$를 구할 수 있으며 동일한 방법으로 i가 1과 2인 각각의 암호화 영상 E_1과 E_2의 비확산 영상 $A_1(u,v)$과 $A_2(u,v)$를 구할 수 있다. 따라서 하위 계층의 복호화 키 L_1은 W_1W_i에 의하여 i가 1인 암호화 영상 E_1만 원 영상으로 복원이 가능하며, 중간 계층의 복호화 키 L_2는 i가 1 또는 2인 암호화 영상 E_1과 E_2만 원 영상 복원이 가능하다. 또한 Walsh code의 크기가 증가할수록 암호화 영상의 크기는 증가하나, 더 높은 상위 계층의 복호화 키를 생성할 수 있다. 식 (4)에서 영상 $A_i'(u,v)$는 확산된 영상 때문에 Walsh code의 크기 및 Walsh code의 대응 모양만큼 다시 비확산 과정이 필요하다. 따라서 비확산 영상 D_{Di}'는

$$D_{Di}'(u,v)=\sum_{u'=0}^{M-1}\sum_{v'=0}^{N-1}D_{Si}'(u',v')\exp\left[-j2\pi\left(\frac{u'u}{M}+\frac{v'v}{N}\right)\right] \tag{9}$$

과 같이 표현할 수 있다. 이때 M,N은 Walsh code를 이용하여 생성한 영상의 한 블록 크기이며, u, v와 u', v'는 동일한 영역인 주파수 영역에서의 변수이며, $u=0$, $v=0$일 때 확산된 영상 D_S'의 한 블록만큼 비확산 과정이 처리된다. 그리고 위 식(9)의 과정을 블록 개수만큼, 즉 원 영상의 크기만큼, 반복적 처리하여 조합하면 원 영상의 크기인 영상 $A_i(u,v)$를 구할 수 있다. 이 영상은 식 (4)의 암호화 과정을 역방향으로 처리함으로써 원 영상은

(a) (b) (c)

그림 3. 계층적 암호화를 위한 원 영상들 (128×128). (a) 하위 원 영상 (Lena), (b) 중간 원 영상 (Baboon), (c) 상위 원 영상 (Ship).



(a) (b) (c)

그림 4. 컴퓨터로 발생 시킨 무작위 영상들 (128×128). (a) 하위 무작위 영상, (b) 중간 무작위 영상, (c) 상위 무작위 영상.

$$\begin{aligned} O_i(x,y) &= \mathcal{F}^{-1}\{D_{Di}'(u,v)\}\exp[-j2\pi r_i(x,y)] \\ &= \mathcal{F}^{-1}\{A_i(u,v)\}\exp[-j2\pi r_i(x,y)] \\ &= O_i(x,y)\exp[j2\pi r_i(x,y)]\exp[-j2\pi r_i(x,y)] \\ &= O_i(x,y) \end{aligned} \tag{10}$$

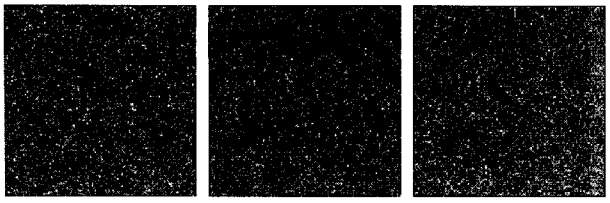
와 같이 복호화할 수 있다. 따라서 최상위 계층의 복호화 키는 모든 암호화 영상을 원 영상으로 복원할 수 있으며, 하위 계층의 복호화 키는 동일한 Walsh code 영상이 포함된 암호화 영상만 원 영상으로 복원할 수 있다. 그림 2는 복호화 과정의 블록다이어그램을 나타낸 것이다.

IV. 실험 및 고찰

4.1 컴퓨터 실험

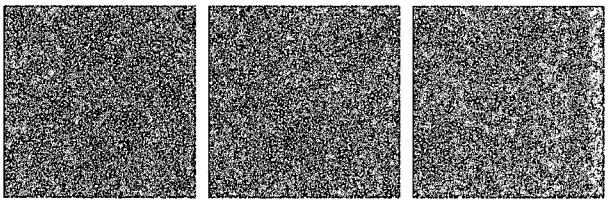
본 논문의 타당성을 검증하기 위해 컴퓨터 모의실험을 수행하였다. 3개의 계층을 수행하기 위하여 3개의 원 영상을 사용하였으며, 원 영상은 그림 3과 같이 128×128의 크기를 가진다. 그림 4는 원 영상의 암호화 수준을 높이기 위해 0과 1 사이의 임의의 값을 갖는 무작위 영상(128×128)이다. 그림 5는 그림 4의 영상을 위상 변조시켜 원 영상과 곱하여 푸리에 변환한 영상이다.

그림 6은 각각의 원 영상에 대입할 Walsh code 영상으로, Hardamard 행렬을 64×64로 생성한 뒤, 행의 크기가 64인 Walsh code를 8×8 영상으로 대응시켰으며, 모두 1의 값인 코드의 첫 번째 행을 제외한 63개의 행을 이용하여, 원 영상



(a) (b) (c)

그림 5. 원 영상과 무작위 위상영상 곱의 푸리에 변환 영상들 (128×128). (a) 하위 변환 영상, (b) 중간 변환 영상, (c) 상위 변환 영상.



(a) (b) (c)

그림 6. Walsh code 영상들 (1024×1024). (a) 하위 Walsh code 영상, (b) 중간 Walsh code 영상, (c) 상위 Walsh code 영상.

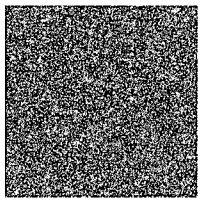
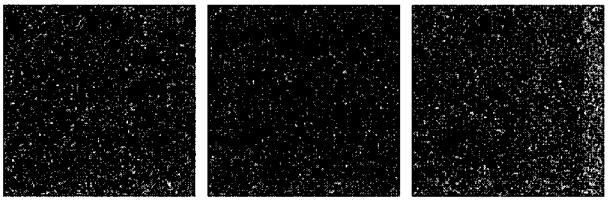


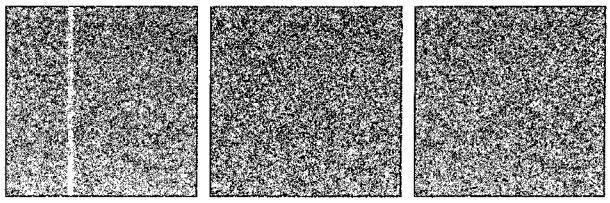
그림 7. 이진 무작위 영상 (1024×1024).



(a) (b) (c)

그림 8. 암호화 영상들 (1024×1024). (a) 하위 암호화 영상, (b) 중간 암호화 영상, (c) 상위 암호화 영상.

의 각 픽셀*크기만큼 임의의 Walsh code로 Walsh code 영상(1024×1024)을 표현하였다. 이때 원 영상들의 동일한 픽셀 위치에는 서로 다른 Walsh code를 사용하였으며, 만약 중복성이 허용되면, 복원할 때 서로 간섭을 주어 원 영상의 복원이 어렵게 된다. 그리고 Walsh code의 크기와 Walsh code를 대응시킨 모양 정보는 복호화 시 또 다른 복원 정보로 사용된다. 그림 7은 Walsh code 영상의 암호화 정도를 높이기 위해 사용된 이진무작위 영상을 나타내며, 이를 위상 변조한 후 Walsh code 영상과 곱하여 복호화 키로 이용한다. 그림 8(a)는 그림 5(a)의 영상을 각 픽셀 8×8만큼 확산시킨 후 그



(a) (b) (c)

그림 9. 복원 키 영상. (a) 하위 영상, (b) 중간 영상, (c) 상위 영상 (1024×1024).

(a) (b) (c)

그림 10. 하위 영상을 이용한 각 암호화 영상의 복원 영상들 (128×128).

(a) (b) (c)

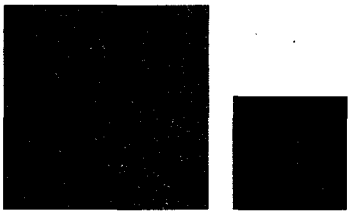
그림 11. 중간 영상을 이용한 각 암호화 영상의 복원 영상들 (128×128).

림 6(a)의 Walsh code 영상과 그림 7(a)의 이진 무작위 영상을 위상 변조시킨 이진 무작위 위상 영상을 곱하여 생성한 암호화 영상(1024×1024)이다. 동일한 방법으로 그림 8(b)와 그림 8(c)를 만들었다. 즉, 그림 8(a)의 암호화 영상은 그림 3(a)의 원 영상 정보와 그림 6(a)의 Walsh code 영상 정보를 포함하고 있으며, 그림 8(b)와 그림 8(c) 역시 동일한 위치의 원 영상 정보와 Walsh code 영상의 정보를 가지고 있다.

그림 9는 계층적 복호화 키를 나타낸 것이다. 그림 9(a)는 하위 계층의 복호화 키로 그림 6(a)의 Walsh code 영상 정보를 가지고 있으며, 그림 9(b)는 그림 6(a)의 Walsh code 영상과 그림 6(b)의 Walsh code 영상을 더한 후 이진 무작위 위상영상을 곱한 중간계층의 복호화 키이다. 즉, 그림 9(b)는 그림 8(a)와 그림 8(b)의 암호화 영상에 사용된 두 개의 Walsh code 영상 정보를 가지고 있다. 그리고 그림 8(c)는 그림 6의 모든 Walsh code 영상을 더한 후 이진 무작위 위상 영상을 곱하여 생성된 최 상위 계층의 복호화 키이다. 그림 10, 그림 11 그리고 그림 12는 그림 9의 하위 계층, 중간 계층 그리고 상위 계층의 복호화 키를 이용하여 각각의 암호화 영상을 복호화한 복원 영상이다. 하위 계층의 복호화 키는

(a) (b) (c)

그림 12. 상위 영상을 이용한 각 암호화 영상의 복원 영상들 (128×128).



(a) (b)

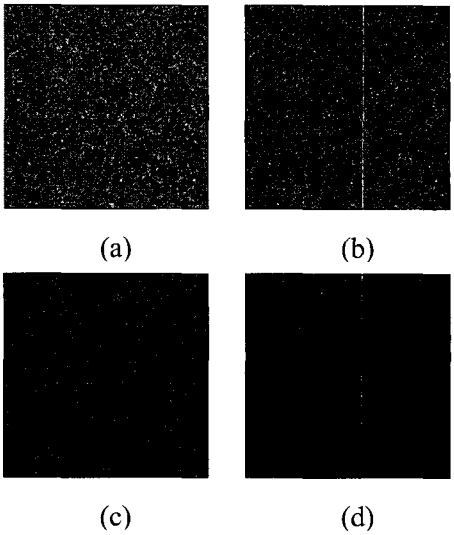
그림 13. 잘못된 정보로 복원한 결과 영상. (a) 비확산의 크기가 다를 때 복원 영상 (256×256), (b) 복호화 키 영상 다를 때 복원 영상 (128×128).

그림 10과 같이 암호화 영상인 그림 8(a)만 원 영상 복원이 가능하며, 중간 계층의 복호화 키는 그림 11과 같이 그림 8(a)와 그림 8(b)만 원 영상 복원이 가능하다. 그리고 상위 계층의 복호화 키는 그림 12와 같이 암호화 영상 모두 원 영상 복원이 가능하다. 따라서 그림 10에서 그림 12를 통하여 직교성의 특성을 지닌 Walsh code 영상을 계층에 따라 서로 더하여도 Walsh code의 원 정보는 간섭되거나 손실되지 않음을 알 수 있다. 또한 하나의 복호화 키만으로도 복호화 키에 포함된 동일한 Walsh code 영상으로 암호화된 영상은 원 영상 복원이 가능함을 알 수 있다.

4.2 복호화에 대한 고찰

비확산의 크기와 거짓 복호화 키에 대한 고찰

그림 13(a)는 비확산의 잘못된 크기 정보(4×4)로 암호화 영상을 복원한 영상이며, 그림 13(b)는 거짓 Walsh code 영상을 사용하여 복호화한 영상으로 원 영상복원이 불가능함을 알 수 있다. 따라서 원 영상을 복원하기 위해서는 Walsh code의 크기와 대응할 때의 모양의 정보를 알고 있어야 복원이 가능하며, 잘못된 정보로 복원하였을 경우, 원 영상의 크기와 모양을 제대로 복원하지 못하였으며, 거짓 복호화 키를 사용하였을 경우 역시 원 영상을 복원할 수 없었다. 따라서 암호화 영상에 사용된 Walsh code 영상과 확산 크기와 모양의 정보, 그리고 이진 무작위 위상 영상의 정보가 모두 있어야 원 영상의 복원이 가능하다.



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

그림 14. (a) 25%, (b) 50%, (c) 75%, (d) 90% 무작위로 절단된 암호화 영상 (128×128).

암호화된 영상의 손실에 대한 고찰

푸리에 영역에서 암호화된 영상의 정보 손실에 대한 실험을 하였다. 손실에 따른 정량적 지표로 PSNR(Peak Signal to Noise Ratio)[12]은

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{b}{rms}\right)(\mathrm{dB}) \tag{11}$$

와 같이 나타낼 수 있다. 이때 b는 원 영상인 입력 평면에서의 가장 큰 수이며, rms는 복원 영상과 절단된 암호화 영상의 복원 영상과의 root mean square이다. 그리고 암호화 영상의 손실이 없는 복원영상과 손실된 암호화 영상의 복원영상과의 상호관련성을 측정하는 상관 계수(correlation coefficient; CC)[13]는

$$\mathrm{CC} = \frac{\mathrm{cov}(\mathrm{E},\mathrm{E}')}{\mathrm{S_E}\,\mathrm{S_{E'}}} \tag{12}$$

와 같으며, 이때$\mathrm{cov}(\mathrm{E},\mathrm{E}')$는 손실이 없을 때의 복원 영상 E와 손실된 암호화 영상의 복원 영상 E'간의 공분산을 의미하여, $\mathrm{S_E}$와 $\mathrm{S_{E'}}$는 각각의 복원 영상 E와 E′의 표준편차를 나타낸다. 그림 14(a), (b), (c), (d)는 무작위로 각각 25%, 50%, 75%, 90% 절단된 암호화 영상이며, 그림 15(a), (b), (c), (d)는 무작위로 각각 25%, 50%, 75%, 90% 절단된 암호화 영상의 복원 영상이다.

이때 무작위 방향으로 각 25%의 절단된 암호화 영상은 암호화 영상의 75%가 일치하는 데이터이며, 각 절단된 부분은 영으로 처리하였으며, PSNR 수치는 각 16.882, 10.774, 7.2878, 5.6644로 다소 떨어지나, 상관계수(CC)는 각각 0.9903, 0.9713, 0.9160, 0.7972로 상당히 높게 나타났다. 이는 Walsh code로 생성된 각각의 블록 별로 비확산 과정을 취한 후 복원 영상

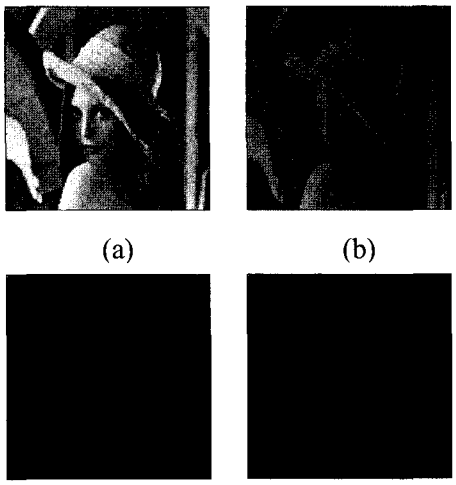


그림 15. (a) 25%, (b) 50%, (c) 75%, (d) 90% 무작위로 절단된 암호화 영상에 대한 복원 영상 (128×128).

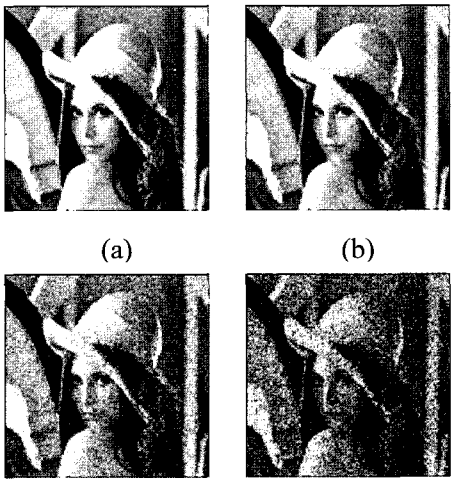


그림 16. (a) 25%, (b) 50%, (c) 75%, (d) 90% 무작위로 절단된 암호화 영상에 대한 정규화된 복원 영상 (128×128).

을 얻기 때문이며 정규화 과정을 취함으로써 암호화 영상의 90% 이상을 절단하여도 복원 영상은 육안으로 식별이 가능함을 알 수 있다. 따라서 그림 16과 같이 정규화 과정을 취함으로써 암호화 영상의 90% 이상을 손실하여도 복원 영상은 육안으로 식별이 가능하다. 그러나 무작위 방향으로 임의의 값을 가지는 거짓 데이터가 각 25% 입력되면 각각의 Walsh code의 크기만큼의 블록 별로 비확산 과정에 의하여 원 영상 복원이 어렵게 된다. 따라서 암호화 영상의 절단에는 강하나, 무작위 방향으로의 거짓 데이터에는 복원이 거의 불가능함을 알 수 있다. 그림 14부터 그림 16을 통하여 임의로 절단된 암호화 영상의 복원력은 u축 방향으로 암호화 영상을 절단하였을 경우의 복원력보다 더 강인함을 알 수 있다. 또한 이것은 복호화 시 비확산 과정을 취하므로 전체적

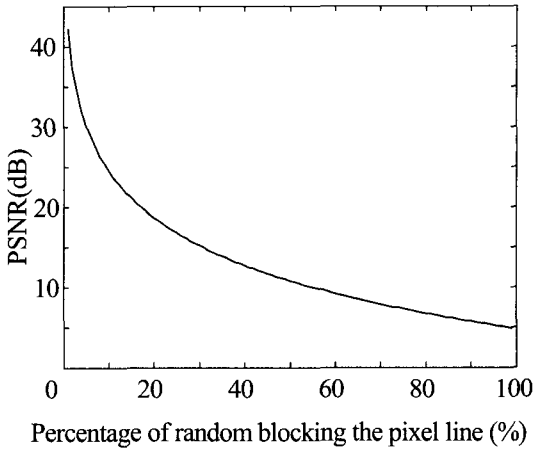


그림 17. 무작위 픽셀 절단에 따른 PSNR.

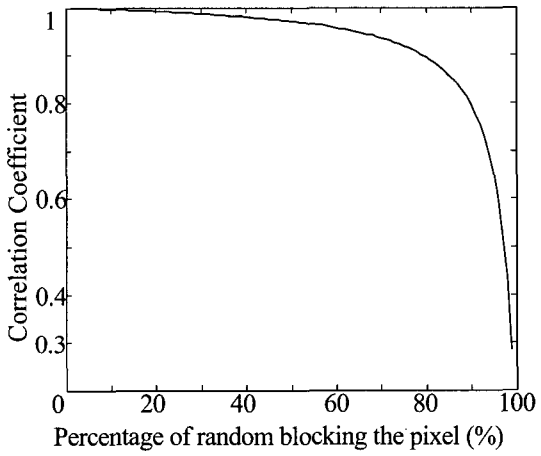


그림 18. 무작위 픽셀 절단에 따른 상관 계수.

인 복원 값은 떨어지나 원 영상과의 분포도는 비슷함을 알 수 있다. 그림 17과 그림 18은 무작위로 암호화 영상을 절단하였을 경우의 PSNR과 상관계수(CC)를 나타낸 것이다.

V. 결 론

본 논문에서는 직교성의 특성을 지닌 Walsh code를 이용하여 계층적 영상 암호화 시스템을 제안하였다. 기존의 계층적 암호화는 하위 계층의 정보는 적은 복호화 키를 사용하나, 상위 계층의 정보일수록 더 많은 복호화 키를 사용하여야 한다는 단점을 가지고 있다. 그러나 Walsh code를 도입함으로써 하나의 키만으로도 정보의 수준에 따라 계층적 구분이 가능하다. 암호화는 먼저 각각의 원 영상에 무작위 위상 영상을 곱하여 푸리에 변환을 취한 후 이진 무작위 위상 영상을 곱한 Walsh code 영상에 확산을 시켜 각각의 암호화 영상을 얻었다. 이때 무작위 위상 영상과 이진 무작위 위상 영상은 암호화 영상을 백색 잡음의 형태로 만들어 암호화 수준을 높이는 역할을 한다. 원 영상은 Walsh code의 행 크기

만큼 증가한다는 단점이 있으나, 이는 코드의 특성상 필수 부가결한 요소이며, Walsh code의 크기 증가는 암호화 수준을 높이며, 계층의 수 또한 증가하는 장점이 있다. 복호화는 각각의 암호화된 영상에 Walsh code와 이진 무작위 영상으로 생성된 계층적 복호화 키를 곱한 뒤, Walsh code 영상을 생성할 때와 동일한 크기와 모양으로 비확산 과정을 수행한 후 푸리에 변환을 통하여, CCD로 원 영상을 복원하였다. Walsh code는 동일한 코드가 입력되면 1이 되며, 다른 코드가 입력되면 0이 되는 직교성의 특성에 의해 여러 Walsh code를 동시에 합하여도, 각각 하나의 코드 특성은 상쇄되거나 첨가되지 않는 장점을 가진다. 따라서 단 한 개의 계층적 복호화 키만으로도 상위 계층의 키는 하위 계층의 정보보다 더 많은 코드의 정보를 입력할 수 있다. 최상위 계층의 복호화 키는 모든 암호화 영상을 복원할 수 있으나, 하위 계층의 복호화 키는 암호화 과정에서 사용된 동일한 Walsh code 영상이 포함된 암호화 영상에만 접근이 가능하다. 그리고 Walsh code의 정보뿐만 아니라 원 영상의 확산된 크기와 모양의 정보를 알아야 원 영상의 복원이 가능하다. 따라서 기존의 계층적 암호화 방법보다 좀더 효율적인 계층적 암호화 방법을 제안하였으며, 암호화 수준도 더욱 향상시켰다. 그리고 컴퓨터 실험을 통하여 제안한 계층적 암호화 방법의 타당성을 고찰하였다. 현재 사용되는 광학장비의 성능개선과 위상 정보를 정확히 표현할 수 있는 SLM이나 식각 기술의 개발 등을 통하여 제안한 계층적 암호화 방법의 성능은 더 나아질 것이라 생각된다.

감사의 글

이 논문은 2005년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임 (KRF-2005-003-D00253)

참고문헌

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

[2] B. Javidi and E. Ahouzi, "Optical security system whth Fourier plan encoding," *Applied Optics*, vol. 37, no. 26, pp. 6247-6255, 1998.

[3] B. Javidi, G. Zhang, and J. Li, "Encrypted optical memory using double-random phase encoding," *Applied Optics*, vol. 36, no. 5, pp. 1054-1058, 1997.

[4] E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optolectronic information encryption with phase-shifting interferometry," *Applied Optics*, vol. 39, no. 14, pp. 2313-2320, 2000.

[5] R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," *Optical Engineering*, vol. 35, No. 9, pp. 2464-2469, 1996.

[6] J. W. Goodman, *Introduction to Fourier Optics*, 2nd ed., McGraw-Hill, New York, 1996.

[7] C. H. Yen, H. T. Chang, H. C. Chien, and C. J. Kuo, "Design of caseaded phase Keys for a hierarchical security system," *Applied Optics*, vol. 41, no. 29, pp. 6128-6314, 2002.

[8] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 2nd ed., Prentice-Hall, Upper Saddle River, 2002.

[9] P-L. Lin, "Robust transparent image watermarking system with spatial mechnisms," *The Journal of Systems and Software*, vol. 50, pp. 107-116, 2000.

[10] N. Nikolaidis and L. Pitas, "Robust image watermarking in the spatial domain," *Signal Processing*, vol. 66, no. 3, pp. 384-403, 1998.

[11] A. B. Sewaif, M. Al-Muall, and H. Al-Ahmad, "2-D Walsh coding for robust digital image watermarking," *Proc. IEEE ISSPIT 2004*, pp. 302-305, 2004.

[12] S. Kishk and B. Javidi, "Information hiding technique with double phase encoding," *Applied Optics*, vol. 41, no. 26, pp. 5462-5470, 2002.

[13] G. Situ and J. Zhang, "A lensless optical security system based on computer-generated phase only masks," *Optics Communications*, vol. 232, pp 115-122, 2004.

Hierarchical Image Encryption System Using Orthogonal Method

Nam-Jin Kim

School of Information & Communication, Kyungpook National University, Daegu 702-701, Korea

Dong-Hoan Seo†, and Sung-Geun Lee

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

†*E-mail : dhseo@bada.hhu.ac.kr*

Chang-Mok Shin, Kyu-Bo Cho, and Soo-Joong Kim

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

(Received March 16, 2006, Revised manuscript June 2, 2006)

In recent years, a hierarchical security architecture has been widely studied because it can efficiently protect information by allowing an authorized user access to the level of information. However, the conventional hierarchical decryption methods require several decryption keys for the high level information. In this paper, we propose a hierarchical image encryption using random phase masks and Walsh code having orthogonal characteristics. To decrypt the hierarchical level images by only one decryption key, we combine Walsh code into the hierarchical level system. For encryption process, we first perform a Fourier transform for the multiplication results of the original image and the random phase mask, and then expand the transformed pattern to be the same size and shape of Walsh code. The expanded pattern is finally encrypted by multiplying with the Walsh code image and the binary phase mask. We generate several encryption images as the same encryption process. The reconstruction image is detected on a CCD plane by a despread process and Fourier transform for the multiplication result of encryption image and hierarchical decryption keys which are generated by Walsh code and binary random phase image. Computer simulations demonstrate that the proposed technique can decrypt hierarchical information by using only one level decryption key image and it has a good robustness to the data loss such as random cropping.

OCIS Codes : 070.0070, 0702590, 100.1160, 120.5060.