工學碩士 學位論文

다중 복호화 키들을 이용한 실질적인 영상 워터마크

Practical image watermark using multi-level decoding keys

指導敎授 徐 東 煥

*2008*年 *6*月

韓國海洋大學校 大學院

電氣電子工學科

李 炯 錫

本 論文을 李炯錫의 工學碩士 學位論文으로 認准함

委員長 : 工學博士 張 樂 元 

委 員 : 工學博士 全 泰 寅 

委 員 : 工學博士 徐 東 煥 

*2008*年 *6*月

韓 國 海 洋 大 學 校 大 學 院

電氣電子工學科

李 炯 錫

목 차

그림 목차

<그림목차>

Practical image watermark using multi-level decoding keys

by Hyung-Seok, Lee

Department of Electrical & Electronics Engineering
The Graduate School of Korea Maritime University
Busan, Republic of Korea

Abstract

In this paper, we propose a practical image watermark method using multi-level decoding keys. The advantages of this method are that the multiple original images are decrypted by using multi-level decoding keys in the same watermark image and that the quality of reconstructed images are clearly enhanced based on the idea of Walsh code without any side lobe in the decoding process. The zero-padded original images, multiplied with random-phase patterns to each other, are Fourier transformed and their real-valued data denote encoded images in the embedding process. The multiplication between the spreaded encoded image and each of Walsh code image is used as a hidden image. Here, the spreaded hidden image is the same size and shape of the walsh code. A stego image is then made

from the linear superposition of the weighted hidden image and a cover image. Each of multi-level decoding keys is obtained by multiplying an imaginary part of the encoded image with Walsh code. The original image is simply reconstructed by the despread process of the product of the stego image and decoding key and its inverse-Fourier transform. The embedding process and the reconstruction process are performed digitally. Computer simulations are demonstrated that the efficiency of the proposed technique with multi-level decoding keys and a good robustness to the external attacks such as cropping.

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, 산업현장뿐만 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 시회불안에까지 영향을 미치고 있다. 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.[1-3]

광 암호화 시스템은 주로 공간영역이나 주파수영역에서 원 영상을 백색잡음 형태를 가지는 복소함수로 암호화한 후 4-f 광 상관기(correlator)[4-7]나 간섭계[8] 또는 결합 변환 상관기(joint transform correlator, JTC)[9-11]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.[12-14]

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. 또한 실질적인 광학적 보안 시스템 구현 및 네트워크를 통한 정보 전송을 위해서는 양의 값을 가지는 실수로 표현이 가능하여야 하며 특히 현재의 기술로 표현되는 SLM의 기록을 위해서는 양자화 과정이 필수적으로 필요하다.[15-17]

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

트 워터마크와 프래절 워터마크의 중간 형태인 세미프래절 워터마크는비의도적으로 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.[18-25]

본 논문에서는 하나의 워터마크된 영상에 서로 다른 다중 정보를 암호화하여 삽입하고 이를 다중 복호화 키들을 사용하여 원하는 정보만을 복원하는 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 변조 시키고 새로운 무작위 위상 영상들과 곱한 뒤 허수부를 취하여 생성한다. 이때 곱한 무작위 위상 영상들의 실수부에 왈시 코드(Walsh code)를 곱하여 복호화 키로 사용하고 삽입 영상과 커버

(cover) 영상에 각각 다른 왈시 코드 영상을 곱한 후 서로 더하여 삽입된 워터마크 영상(stego image)을 생성한다. 따라서 허가받지 않은 사용자가 위상 측정 방법 등을 통하여 암호화된 영상의 위상 값을 추출하더라도 복호화 키들의 정보 없이는 원 영상들의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하며 커버 영상에 왈시 코드를 곱하므로 복구 과정에서 커버 영상의 사이드 로브(side lobe) 성분이 제거되어 복원 영상의 해상도를 높일 수 있다.

Ⅱ. 암호화방법과 *Walsh code*

1. 이중 랜덤 위상 암호화 방법

1) 진폭형(Amplitude based method)

그림 1과 같이 암호화 할 원 영상의 입력 영상은 $f(x,y)$ 로 나타내며, 입력면의 랜덤 위상 함수와 푸리에 면의 랜덤 위상 함수를 각각 $\exp[j2\pi p(x,y)]$ 와 $\exp[j2\pi b(u,v)]$ 로 표기 한다. 이때 (x,y) 는 공간 영역의 좌표를 나타내고, (u,v) 는 푸리에 영역에서의 좌표를 나타낸다. 입력 영상 $f(x,y)$ 는 0 과 1사이의 값으로 규격화된 양의 실수 함수로 가정하며, $p(x,y)$ 와 $b(u,v)$ 는 서로 독립적이며, 이 또한 0과 1사이에서 균일하게 분포된 랜덤 함수라 가정한다. 진폭형 이중 랜덤 위상 암호화 방법은 간단하게 2단계로 처리된다. 먼저 첫 번째 입력 함수 $f(x,y)$ 와 입력 랜덤 위상 마스크 $\exp[j2\pi p(x,y)]$ 와 곱해진다. 즉, 입력 함수와 랜덤 위상의 곱은 $H(u,v)$ 의 푸리에 변환인 임펄스응답(impulse response) $h(x,y)$ 와 컨볼루션(convolution)이 된다. 이 처리과정은

$$\psi_A(x,y) = \{f(x,y)\exp[j2\pi p(x,y)]\} \otimes h(x,y), \qquad (1)$$

과 같다. 이때 ⊗는 컨볼루션(convolution) 연산을 의미한다. 이 암호화의 처리과정은 광학적 또는 전자적으로 구현 할 수 있다. 그러나 어떠한 경우든 암호화된 영상 $\psi_A(x,y)$는 진폭과 위상이 모두 표현될 수 있어야 한다.

암호화 영상 $\psi_A(x,y)$ 복원과정은 그림 1(b)와 같이 암호화된 영상을 푸

리에 변환한 뒤, 암호화 과정에서 사용한 랜덤 위상 함수의 복소공액을 곱해 준다. 그 다음으로 푸리에 역변환을 취하므로 원 영상을 복원 할 수 있다. 즉

$$f(x,y)\exp[j2\pi\phi(x,y)] = \mathcal{F}^{-1}\{\mathcal{F}\{f(x,y)\exp[j2\pi\phi(x,y)]\} \times H(u,v)\times H^{*}(u,v)\}. \quad (2)$$

이때 $\mathcal{F}\{\cdot\}$ 와 $\mathcal{F}^{-1}\{\cdot\}$ 는 각각 푸리에 변환과 역변환을 나타내며, 위첨자 $*$ 는 복소공액을 나타낸다. 원 영상의 복원은 CCD와 같은 세기 검출기로 사용하면 $|\exp[j2\pi\phi(x,y)]|^2=1$ 에 의하여 원 영상 $f(x,y)$ 를 복원 할 수 있다.

2) 위상형(Phase based method)

위상형 암호화 방법은 진폭형과 유사하며, 그림 1(a)의 입력 영상 $f(x,y)$ 대신 위상 변조 된 $\exp[j\pi f(x,y)]$ 를 입력한다. 이때 진폭형 암호화 방법에서 가정한 것과 동일하게 입력 영상 $f(x,y)$ 는 0과 1사이의 균일한 분포를 가지므로 위상 변조된 입력 영상 $\exp[j\pi f(x,y)]$ 는 $[0,\pi]$ 의 분포를 가진다. 위상형 암호화 영상 $\psi_P(x,\ y)$ 은

$$\psi_P(x,\ y) = \{\exp[j\pi f(x,y)]\times \exp[j2\pi\phi(x,y)]\}\otimes h(x,y), \quad (3)$$

으로 표현된다. 또한 광학적인 방법이나 전자적인 방법으로 구현 될 수 있으나 광학적인 시스템으로 구성하기 위해서는 복소함수를 표현할 수 있는 영상 장치가 필요하고, 올바른 복호화를 위해서는 암호화 과정에서 사용된 랜덤 키의 복소공액이 있어야 한다는 단점을 가기고 있기에 전자적으로 구현하는 경우가 광학적인 구현 방법보다 훨씬 더 간단하며, 우수한 성능을 발휘 한다.

복원 방법은 진폭형의 암호화 의 복원 방법과 동일하게 처리한다. 즉

$$\begin{aligned} &\exp[i\pi f(x,y)]\times \exp[i2\pi g(x,y)] \\ &= \mathcal{F}^{-1}\{\mathcal{F}\{\exp[i\pi f(x,y)]\times \exp[i2\pi g(x,y)]\}\times H(u,v)\times H^{*}(u,v)\}. \end{aligned} \tag{4}$$

수식(4)에서 $\exp[-i2\pi g(x.y)]$ 를 곱한 뒤 위상만을 추출하여 π 를 나누어서 원 영상 $f(x,y)$ 를 구할 수 있다.

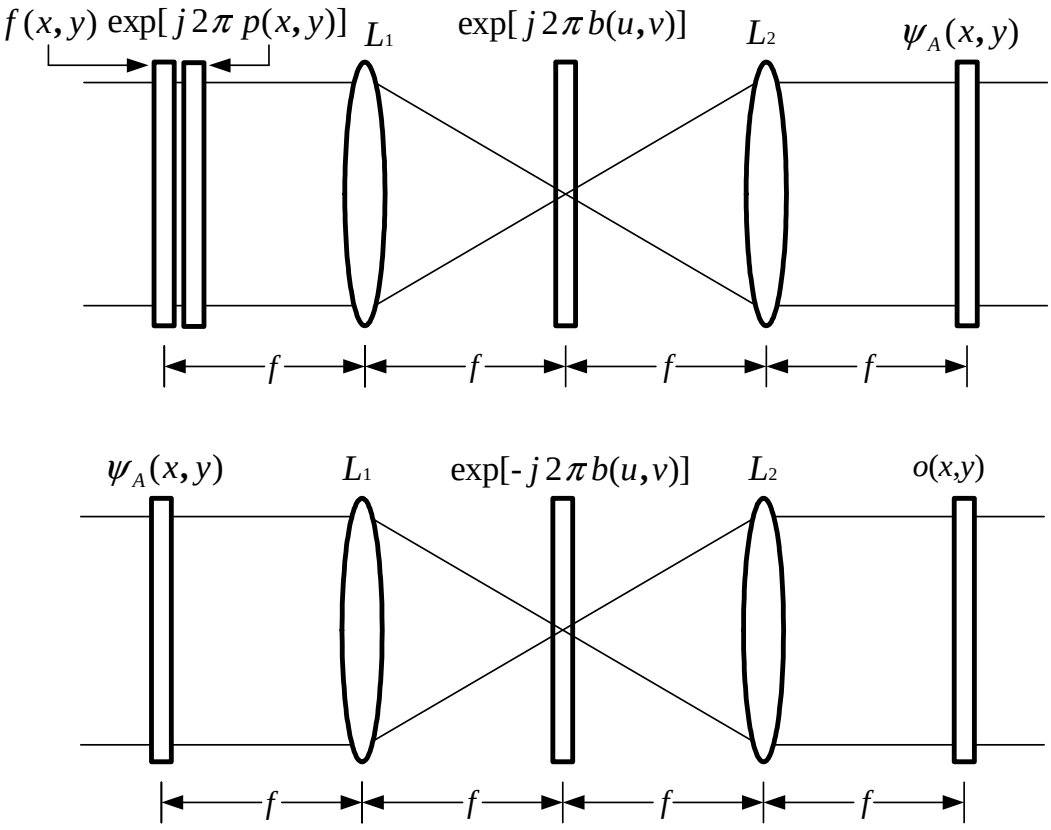


그림 1. 진폭형 이중 랜덤 위상 암호화 방법: (a)암호화 과정, (b)복호화 과정

Fig. 1. Amplitude-based double random phase encoding method : (a) Encryption process, (b) Decryption process

2. 계층적 암호화 방법

계층적 암호화 시스템은 Chia H.a Yen 이 직렬 위상 마스크(Cascaded phase-only mask)를 이용하여 계층적 보안 시스템을 제안 하였다.

광 구성도는 그림 2와 같으며, 입력 평면 I에 위상 마스크(phase-only mask)를 두고 초점 거리 $L/2$ 의 거리를 두고 푸리에 렌즈, 출력 평면 O 를 두었다.

입력 평명 (x, y) , 출력 평면 (u, v) 로 각각 정의 하면, 입력 평면 $U_I(x, y)$ 와 출력 평면 $U_O(u, v)$ 의 빛의 분포는

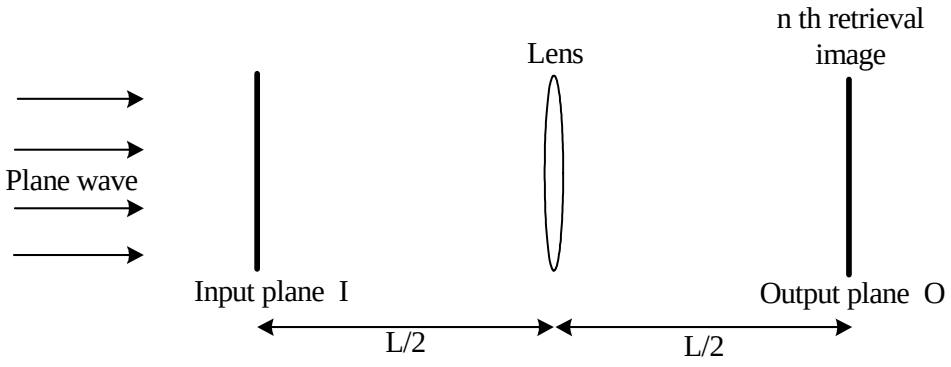


그림 2. 기본 광 구성도

Fig. 2. Optical setup of the basic architecture.

$$U_I(x.y) = A_I(x.y)P_I(x.y) = A_I\exp[j\Phi_I(x.y)],$$
$$P_I(x.y) = \exp[j\Phi_I(x.y)], \tag{5}$$

$$\begin{aligned} U_O(u, v) &= A_O(u, v)P_O(u, v) \\ &= A_O\exp[j\Phi_O(u, v))], \\ P_O(u, v) &= \exp[j\Phi_O(u, v)], \end{aligned} \tag{6}$$

이며, 이때 A_I와 A_O는 U_I와 U_O의 진폭 세기이며, Φ_I와 Φ_O는 각 각 U_I와 U_O의 위상을 나타낸다. 입력 영상 U_I와 출력 영상 U_O의 관계는

$$U_O(x.y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} U_I(x.y)G(x.y)\times\exp[j\frac{2\pi}{\lambda L}(xf_x.yf_y)]\,\mathrm{d}x\,\mathrm{d}y. \tag{7}$$

나타난다.

하나의 원 영상(original image)의 최적 위상 마스크(the optimized phase-only mask)는 그림 3.의 블록 다이어그램과 같이 POCS 알고리즘으로 정의 되며, 처리 과정은 다음과 같은 4 단계로 이루어진다. (1) 주어진 결과 영상 패턴 $U_O(u, v)$를 역 푸리에 변환에 의해 유사한 광 투과 함수를 찾는다. (2) 균일한 위상 마스크를 위해 진폭 투과 $A_I(x, y)$를 고정 시킨다. (3) 새로운 출력 회절 패턴을 위해 출력 영역에 적용한다. (4) 위상 마스크나 회절 영상이 변하지안을 때까지 1에서 3까지의 과정을 반복한다.

최적 위상 마스크 $P_I(x, y)$로 나타내며, POCS 알고리즘을 사용하여 n 위상 마스크 $P_{I,i}(x, y)$를 찾는다. 이때 i=1, …, n. 이다. 계층적인 보안 시

스템을 구성하기 위해 이웃 한 두 최적 위상 마스크 $P_{I,i}(x,y)$ 와 $P_{I,i-1}(x,y)$ 로부터 유사한 n 위상을 계산하여 n 위상 키(phase key)를 생성한다. i 번째 위상 키 K_i 는 이웃한 다른 두 최적 위상 마스크의 위상이며, 수식 (8)에 나타내었다.

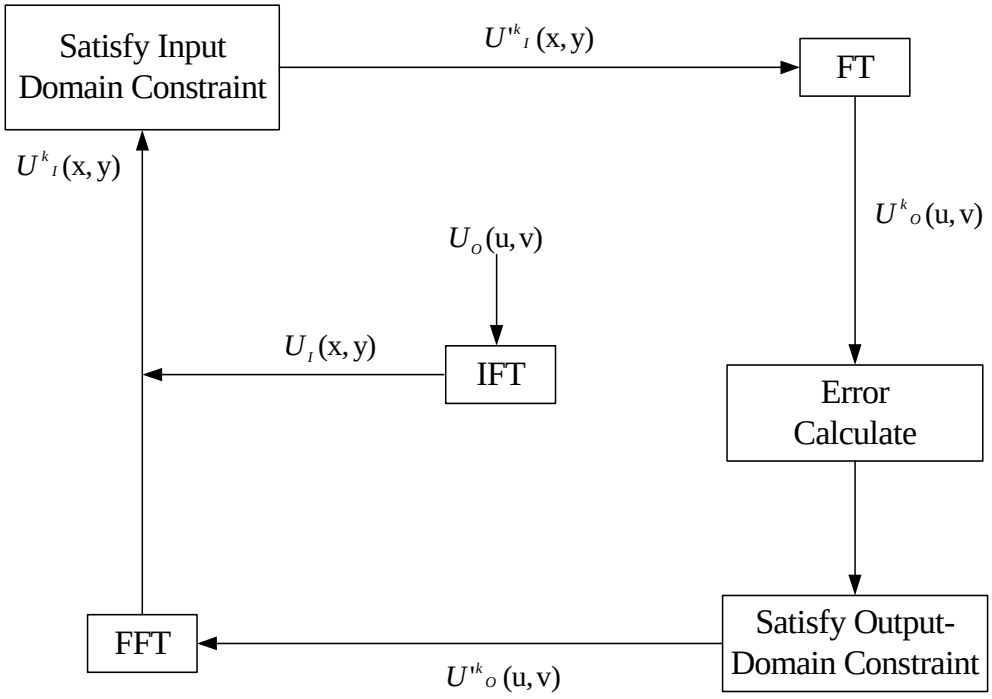


그림 3. 반복 알고리듬의 블록 다이어그램

Fig. 3. Block diagram of the iterative algorithm.

$$K_i = \frac{P_{I,i}(x,y)}{P_{I,i-1}(x,y)} = \exp\{j[\Phi_{I,i}(x.y) - \Phi_{I,i-1}(x.y)]\}. \quad (8)$$

K_i 는 i 번째 위상키이며, 입력 평면 I 에 평면파가 입사되면, 출력 평면 O 에 n 번째 위상키는

$$\begin{aligned} U_{O,n}(f_x, f_y) &= FT\{K_1 \times K_2 \times \cdots \times K_n\}, \\ &= FT(\exp\{j[\Phi_{I,}1(x,y) - \Phi_{I,0}(x.y) \\ &+ \Phi_{I,2} - \Phi_{I,1}(x.y)(x.y) + \cdots \\ &+ \Phi_{I,n}(x.y) - \Phi_{I,n-1}(x.y)]\}), \\ &= FT\{\exp[j\Phi_{I,n}(x.y)]\}, \\ &= FT\{P_{I,n}(x,y)\}, \end{aligned} \quad (5)$$

나타난다. 이때 모든 i, 와 $\Phi_{I,i}(x,y) = 0$ 일때 $A_{I,i}(x,y) = 1$ 이다.

빛이 자유공간에서 일정한 거리 d_i 만큼 전파한다면 그림 4와 같으며, 두 광파면 U_I 와 $U_{I,i}$ 의 관계는

$$\begin{aligned} U_{I,i}(x_i, y_i) &= \int\int U(x,y)\exp\left\{j\frac{k}{2d_i}[(y-y_i)^2 + (x-x_i)^2]\right\} \mathrm{d}x\,\mathrm{d}y, \\ &= U(x.y) \otimes \exp\left\{j\frac{k}{2d_i}[(x_i^2 + y_i^2)]\right\}. \end{aligned} \quad (6)$$

와 같이 표현 되며, 이때 $k = 2\pi/\lambda$, λ 는 파장, 그리고 $\otimes$는 컨볼루션 (convolution) 연산자를 의미한다.

그림 4와 같이 입력 평면 I 에서 거리 d_i 만큼 떨어진 위상 키(phase

key) K_i' 는

$$
\begin{aligned}
K_1' &= K_1 \otimes h(-d_1), \\
K_2' &= [K_2 \otimes h(-d_1)\,\overline{K_1'} \otimes h(-((d_2-d_1)), \\
K_3' &= \{[K_3 \otimes h(-d_1)]\,\overline{K_1'} \otimes h(-((d_2-d_1)) \times K_2'\} \otimes h(-((d_3-d_2)), \\
&\vdots \\
K_n' &= (\cdots\{[K_n \otimes h(-d_1)]\,\overline{K_1'} \otimes h(-((d_2-d_1)) \times \overline{K_2'}\} \otimes h(-((d_3-d_2))\cdots \\
&\quad \times \overline{K_{n-1}'} \otimes h(-((d_n-d_{n-1})).
\end{aligned}
\tag{7}
$$

와 같으며, $\overline{K_1'}$ 는 K_1' 의 복소 공액(complex conjugate)을 의미 한다.

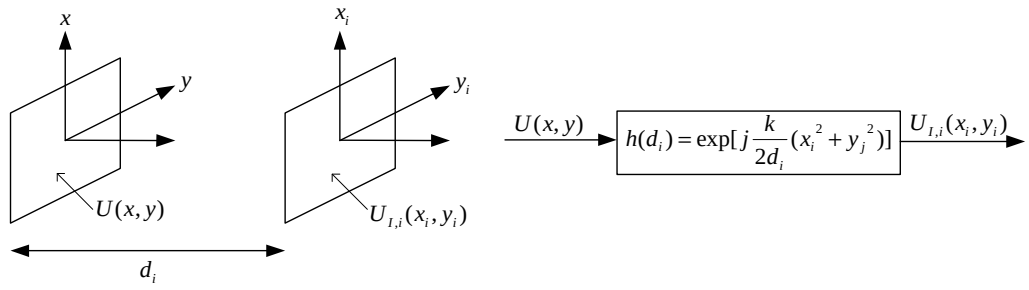


그림 4. 자유 공간 d_i 이동에 따른 구조와 연산

Fig. 4. Schematic and operation representation of the space distance d_i .

i 번째 반복 목표 영상(target image)의 출력 평면 O 는

$$\begin{aligned} U_{0,i}(u,v) &= FT\{[(\cdots(k_i' \otimes h(d_i - d_{i-1}) \times K_{i-1}') \\ &\quad \otimes h(d_{i-1} - d_{i-2}) \cdots \times K_1'] \otimes h(d_1)\}, \\ &= FT\{K_i\}, \\ &= FT\{\exp[j\Phi_{I,i}(x.y)]\}, \\ &= FT[P_{I,i}(x.y)]. \end{aligned} \tag{8}$$

로 표현된다. 이때 모든 i 에서 $A_{I,i}(x.y)=1$ 이다. 그리고 그림 5와 같이 n 위상 키(phase keys) 와 n 거리 변수의 정보는 n번째 목표 영상을 출력할 수 있으며, 모든 정보를 가지지 않은 불법 사용자는 목표 영상 재생이 불가능하다.

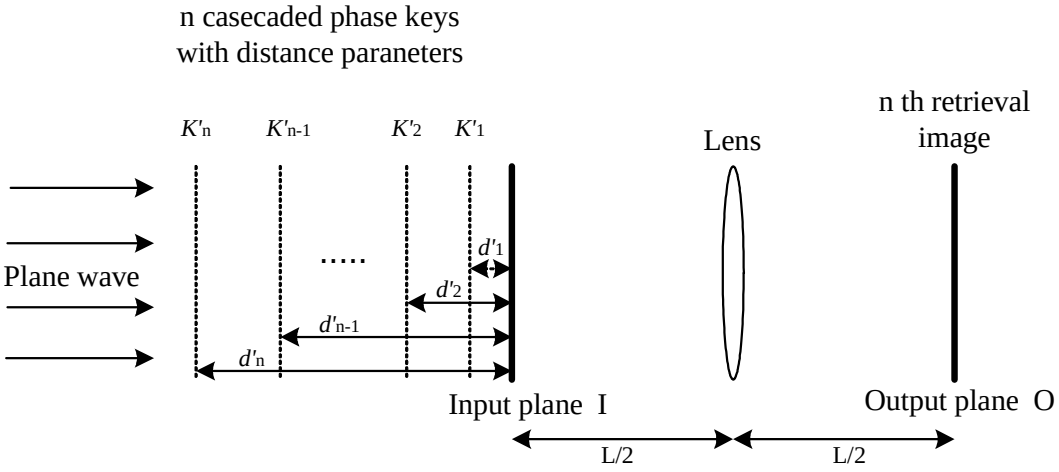


그림. 5. 개선된 광 구성도

Fig. 5. Advanced optical setup.

2. Walsh code

왈시 코드는 1923년 J. L. Walsh에 의해 직교함수로 소개 되었으며, 직교성은 서로 간섭을 주지 않으며, 코드 간에 상관관계가 매우 적은 것을 의미한다.[24-25]

왈시 코드 생성법은 “Hadamard Matrix"에 의해 생성되며, 행렬은

$$H_{2N}=\begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix}. \tag{9}$$

와 같이 정의 된다. 이때 H_1 은 1이며, N은 2의 거듭제곱수를 의미한다.

예를 들어 Hadamard 행렬을 이용한 4×4 행렬은

$$H_2=\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} W \\ W_1 \\ W_2 \\ W_3 \end{bmatrix}. \tag{10}$$

와 같이 구현 되며, 이때 모두 1의 값을 갖는 첫 번째 행을 제외한 두 번째 행부터 W_1, W_2, W_3 로 정의 된다. Hadamard 행렬의 각 행은

$$\frac{1}{T_L}\sum[W_i \times W_j^T]=\begin{cases} 0, & i \neq j \\ 1, & i=j \end{cases} \tag{11}$$

의 특성을 갖는다. 이때 T_L 는 Hadamard 행렬의 행 크기이며, W_j^T 는

W_j 전치행렬(Transposed)을 나타낸다. 위 수식(11)과 같이 3개 Walsh-code (W_1, W_2, W_3)는 모두 직교성의 특성을 가지고 있다.

왈시 코드의 매핑 방법은 수식(10)에서 생성된 행의 크기가 4인 code를 그림 6과 같이 2×2영상에 가로 방향으로 우선적으로 맵핑하여 왈시 코드 영상을 만들었다. 원 영상의 첫 번째 각 픽셀 값이 그림 7과 같이 40, 80, 160이라고 가정을 하였다.

1	-1
1	-1

(A)왈시 코드 1 W_1

1	1
-1	-1

(b)왈시 코드 2 W_2

1	-1
-1	1

왈시 코드 3 W_3

그림 6. 왈시 코드 영상 매핑

Fig. 6. Mapping of Walsh code image.

40	

(a) Image 1 I_1

80	

(b) Image 2 I_2

160	

(c) Image 3 I_3

그림 7. 각 원 영상의 픽셀 값

Fig. 7. Pixel value of original image, respectively.

각 픽셀의 세기를 왈시 코드 행의 크기로 나눈 뒤 원 영상을 왈시 코드 영상에 확산하면 그림 8과 같다. 이때 원 영상의 한 픽셀이 4개의 픽셀로 증가된다. 복호화 키는 그림 9와 같이 왈시 코드 영상을 계층적으로 더하여 계층적인 복호화 키를 정의 한다. 각 계층적 복호화 키를 이용하여 각각의 암호화된 영상을 곱하면 , 그림 10, 그림 11, 그림 12와 같다.

그림 10, 11, 12는 확산된 영상이므로 원 영상을 확산한 영역만큼 다시 비확산(Despread)을 취하여 원 영상의 각 픽셀 값을 구 할 수 있다. 하위계층의 복호화 키 K_1 은 암호화 영상에 사용된 동일한 왈시 코드가 포함된 암호화영상 E_1 만 복원이 가능하며, 동일한 왈시 코드가 포함되지 않은 두 번째, 세 번째 암호화 영상은 직교성의 특성에 의하여, 비확산 처리 과정을 거쳐 영(zero)의 값을 갖으며, 상위계층의 복호화 키 K_3 는 암호화에 사용된 모든 Walsh-code의 정보를 가지고 있으므로 모든 암호화 영상의 복원이 가능하다. 그리고 직교성의 특성에 의하여, 복호화 키를 만들 때 각 왈시 코드를 더하여도 각각의 왈시 코드 정보의 특성을 가지고 있다.

10	-10		
10	-10		

(a) $E_1 = I_1 \times W_1$

20	20		
-20	-20		

(b) $E_2 = I_2 \times W_2$

40	-40		
-40	40		

(c) $E_3 = I_3 \times W_3$

그림 8. 확산된 각 원 영상과 왈시 코드영상의 곱 영상

Fig. 8. Multiplication image an spreaded original image and Walsh code image, respectively.

1	-1
1	-1

(a) $K_1 = W_1$

2	0
0	-2

(b) $K_2 = W_1 + W_2$

3	-1
-1	-1

(c) $K_3 = W_1 + W_2 + W_3$

그림 9. 계층적인 복호화 키 : (a) 하위 계층의 복호화 키, (b) 둥간 계층의 복호화 키, (c) 상위 계층의 복호화 키

Fig. 9. Hierarchical decryption key : (a) low level decryption key, (b) middle level decryption key, (c) high level decryption key.

10	10		
10	10		

(a) $E_1 \times K_1$

20	-20		
20	-20		

(b) $E_2 \times K_1$

40	40		
-40	-40		

(c) $E_3 \times K_1$

그림 10. 각 암호화 영상을 하위 계층의 복호화 키 K_1 으로 복원

Fig. 10. Decryption of encryption image using low level decryption key K_1, respectively.

10	10		
10	10		

(a) $E_1 \times K_2$

40	0		
0	40		

(b) $E_2 \times K_2$

80	0		
0	-80		

(c) $E_3 \times K_3$

그림 11. 각 암호화 영상을 중간 계층의 복호화 키 K_2 로 복원

Fig. 11. Decryption of encryption image using middle level decryption key K_2, respectively.

30	10		
-10	10		

(a) $E_3 \times K_3$

60	-20		
20	20		

(b) $E_2 \times K_3$

120	40		
40	-40		

(c) $E_3 \times K_3$

그림 12. 각 암호화 영상을 복호화 키 K_3 로 복원

Fig. 12. Decryption of encryption image using high level decryption key K_3, respectively.

Ⅲ. 제안한 워터마크 및 복호화 방법

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 로브를 제거하는 시스템을 제안하였다.

제안한 삽입 영상들은 원 영상들을 제로 패딩하고 무작위 위상 영상을 곱하여 푸리에 변환 후 이 변환된 영상들의 실수부를 확산 및 위상 변조 시키고 새로운 무작위 위상 영상들과 곱한 뒤 허수부를 취하여 생성한다. 이때 곱한 무작위 위상 영상들의 실수부에 왈시 코드를 곱하여 복호화 키로 사용하고 삽입 영상과 커버 영상에 각각 다른 왈시 코드 영상을 곱한 후 서로 더하여 삽입된 워터마크 영상을 생성한다. 따라서 허가받지 않은 사용자가 위상 측정 방법 등을 통하여 암호화된 영상의 위상 값을 추출하더라도 복호화 키들의 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 공간필터를 두어서 원 영상들을 복원함으로써 왈시 코드에 의해 사이드 로브를 제거된 해상도가 높은 복원 영상을 얻을 수 있다. 그리고 다중 복호화 키들을 이용하여 원하는 정보의 영상만을 복원이 가능하다.

1 삽입된 워터마크 영상 생성

삽입할 제로 패딩된 원 영상들 $f_i(x,y)$, 무작위 위상 영상 $\exp[jn(x,y)]$, 여

기서 $n(x,y)$는 정규화 된 $[0,2\pi]$사이 값을 가진다. 먼저 입력 영상을 무작위 영상을 위상 변조하여 곱하고 푸리에 변환을 하면 푸리에 면에 균일하게 분포된다. 그 식은

$$O_i(\zeta,\eta) = FT\{f_i(x,y)\exp[jn(x,y)]\}, \tag{20}$$

로 표현되고 여기에서 $FT\{\bullet\}$는 푸리에 변환을 의미한다. 원 영상들을 제로 패딩과 푸리에 변환을 하고 얻은 $O_i(\zeta,\eta)$에서 실수 부분만 갖는 암호화된 영상들을 $E_i(\zeta,\eta)$로 표현되고 선형적이며 $[-1,1]$ 사이의 값을 갖는다. 이 영상들을 다시 왈시 코드의 크기에 맞게 확장 시켜 $A_i(\zeta,\eta)$로 표현하면,

$$A_i(\zeta,\eta) = E_i[s_x(\zeta-1)+\alpha, s_y(\eta-1)+\beta] \tag{21}$$
$$where\ \ \alpha = 1,2,3,\cdots,s_x,\ \ \beta = 1,2,3,\cdots,s_y$$

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 더한 식은,

$$\exp[j2\pi r_h(\zeta,\eta)] = \exp[j2\pi\{A_i(\zeta,\eta)+r_i(\zeta,\eta)\}], \tag{22}$$

와 같이 표현되며 여기서 $r_h(\zeta,\eta)$는 삽입 영상들에 들어가는 암호화 산술 연산키이며 계층적으로 들어갈 영상의 수만큼 만들 수 있다. 그리고 $r_i(\zeta,\eta)$는 무작위 위상 영상들로 삽입 영상의 암호화 수준을 향상 시키고 복호화 키로도 사

용된다. 이 또한 계층적으로 들어갈 영상의 수만큼 만들 수 있다. 삽입 영상들과 복호화 키들는

$$\begin{aligned}\tilde{h}(\zeta,\eta) &= Im\{\exp[j2\pi r_h(\zeta,\eta)/K]\} \\ &= \sin[2\pi r_h(\zeta,\eta)/K] \\ \tilde{k}(\zeta,\eta) &= W_j Re\{\exp[2\pi r_i(\zeta,\eta)/K]\} \\ &= W_j \cos[2\pi r_i(\zeta,\eta)/K],\end{aligned} \tag{23}$$

와 같고 여기에서 $Im\{\bullet\}$, $Re\{\bullet\}$. 그리고 정수 K는 각각 허수부와 정수부 그리고 가시성을 조절하는 연산자로 복구 영상의 해상도를 높이고 스테고 영상과 커버 영상 사이의 PSNR을 높이는데 사용된다. 계층적으로 암호화하고 복호화를 위해 왈시 코드 영상을 곱하고 이 암호화키 영상과 커버 영상을 더한 스테고 영상은

$$S(\zeta,\eta) = \alpha W_i \tilde{h}(\zeta,\eta) + W_k C(\zeta,\eta), \tag{24}$$

와 같고 여기에서 $C(\zeta,\eta)$는 커버 영상으로 $[0,1]$ 사이의 값을 갖고 $S(\zeta,\eta)$는 숨겨진 영상과 커버 영상이 선형적으로 중첩되어진 스테고 영상이다. 그리고 α는 숨긴 영상을 커버 영상에 최대한 영향을 줄이기 위해 조절하는 연산자이다. W_i와 W_k는 왈시 코드를 이용하여 생성한 왈시 코드 영상이며 $[0,1]$ 사이의 값을 갖는다. 여기서 i와 k는 영상의 수이고 서로 같지 않다.

제안한 방법은 원 영상을 공간 영역에서 제로 패딩하고 무작위 위상 영상을 곱하여 푸리에 변환을 한다. 여기서 얻어진 영상의 실수 값을 무작위 영상

과 더하여 암호화 수준을 높이고 실수 값의 영상을 복호화 키로 사용하고 허수 값의 영상은 커버 영상과 더하여 스테고 영상을 만든다. 그리고 삽입 영상과 복호화 키에 왈시 코드를 첨가 하므로 영상의 크기가 왈시 코드의 크기만큼 확산된 암호화 영상 생성하였다. 기존의 이중 랜덤 위상 암호화 영상은 무작위 영상만으로 암호화 영상의 복원이 가능 했으나, 왈시 코드의 크기만큼 확산이 되어, 그 확산된 부분만큼 비확산 처리과정 이 필요하다. 그래서 왈시 코드의 크기와 모양을 알아야 원 영상을 복원 할 수 있고 커버 영상에 왈시 코스를 곱해서 복구 과정에서 커버 영상의 정보를 제거하여 복원 영상의 사이드 로브(side lobe)가 제거된다. 그림 13은 본 논문에서 제안한 암호화 방법의 블록 다이어그램이다.

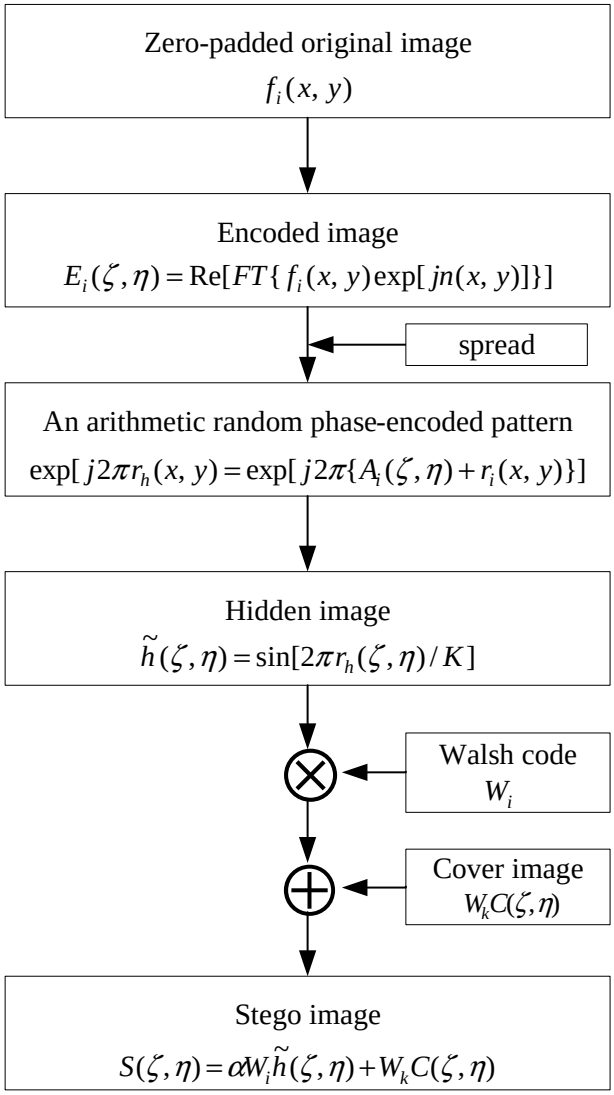


그림 13. 제안한 워터마크 방법의 블록 다이어그램

Fig. 13. The block diagram of proposed watermark method.

2 복호화 방법

그림 14는 본 논문에서 제안한 복호화 방법의 블록 다이어그램이다.

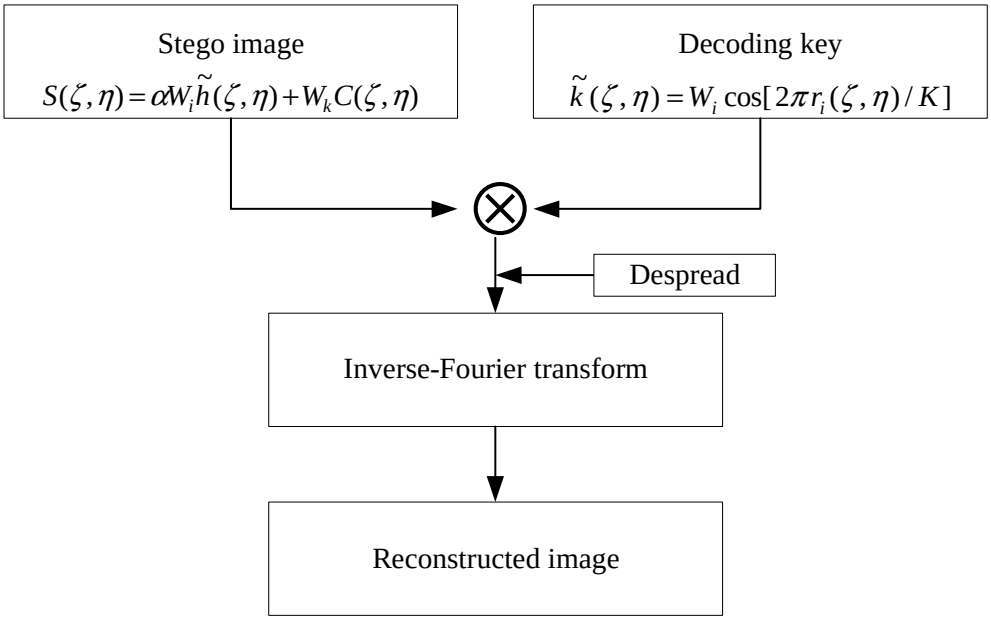


그림 14. 제안한 복호화 방법의 블록 다이어그램

Fig. 14. The block diagram of proposed decryption method.

제안한 복호화 방법은 원 영상을 얻기 위해 스테고 영상과 복호화 키들을 곱하고 비확산을 거친 후 역 푸리에 변환을 하면 원점에 대칭하는 원하는 원 영상들을 얻을 수 있다. 우선 스테고 영상과 복호화 키들과의 곱에서 얻어진 수식을 다음과 같이 전개하면

$$\tilde{k}(\zeta,\eta)H(\zeta,\eta) = W_j\cos\left[2\pi r_i(\zeta,\eta)/K\right]\left\{\alpha W_i\sin\left[2\pi r_h(\zeta,\eta)/K\right] + W_k C(\zeta,\eta)\right\} \quad (25)$$

$$= \alpha W_i W_j \sin\left[2\pi r_h(\zeta,\eta)/K\right]\cos\left[2\pi r_i(\zeta,\eta)/K\right]$$

$$+ W_j W_k C(\zeta,\eta)\cos\left[2\pi r_i(\zeta,\eta)/K\right]$$

$$= \frac{\alpha}{2} W_i W_j \sin\left[2\pi\{r_h(\zeta,\eta) - r_i(\zeta,\eta)\}/K\right]$$

$$+ \frac{\alpha}{2} W_i W_j \sin\left[2\pi\{r_h(\zeta,\eta) + r_i(\zeta,\eta)\}/K\right]$$

와 같이 표현할 수 있으며 여기에서 W_iW_j는 왈시 코드 영상의 곱으로 $i=j$ 일 경우 $W_iW_j=1$이 되고 $i\neq j$일 경우에는 $W_iW_j=0$가 된다. 이때 $W_jW_k=0$ 이 되기 때문에 커버 영상이 제거되어 복원 영상에 큰 사이드 로브가 제거된다. 식 (22)와 (25)를 테일러 공식에 의해 정리하면

$$\frac{\alpha}{2}\sin\left[2\pi\{r_h(\zeta,\eta) - r_i(\zeta,\eta)\}/K\right] + \frac{\alpha}{2}\sin\left[2\pi\{r_h(\zeta,\eta) + r_i(\zeta,\eta)\}/K\right] \quad (26)$$

$$= \frac{\alpha}{2}\sin\left[2\pi E(\zeta,\eta)/K\right] + \frac{\alpha}{2}\sin\left[2\pi\{E(\zeta,\eta) + r_i(\zeta,\eta)\}/K\right]$$

$$= \frac{\alpha}{2}\left\{2\pi E(\zeta,\eta)/K - \frac{[2\pi E(\zeta,\eta)/K]^3}{3!} + \frac{[2\pi E(\zeta,\eta)/K]^5}{5!} - \Lambda\right\}$$

$$+ \frac{\alpha}{2}\left\{\begin{array}{l} 2\pi\{E(\zeta,\eta) + r_i(\zeta,\eta)\}/K - \dfrac{[2\pi\{E(\zeta,\eta) + r_i(\zeta,\eta)\}/K]^3}{3!} \\ \quad + \dfrac{[2\pi\{E(\zeta,\eta) + r_i(\zeta,\eta)\}/K]^5}{5!} - \Lambda \end{array}\right\}$$

$$\approx \frac{2\alpha\pi}{K}E(\zeta,\eta) + \frac{2\alpha\pi}{K}r_i(\zeta,\eta),$$

로 감소된 암호화 영상을 얻을 수 있다. 식 (21)에서 영상 $A_i(\zeta,\eta)$는 확산된 영상이기 때문에 왈시 코드의 크기 및 왈시 코드의 대응 모양만큼 다시 비확산 과정이 필요하다. 따라서 비확산 영상은

$$D_{Di}'(\zeta,\eta)=\sum_{u'=0}^{M-1}\sum_{v'=0}^{N-1}D_{Si}'(\zeta',\eta')\exp[-j2\pi(\frac{\zeta'\zeta}{M}+\frac{\eta'\eta}{N})], \tag{27}$$

과 같이 표현할 수 있다. 이때 M,N은 왈시 코드를 이용하여 생성한 영상의 한 블록 크기이며, 그리고 $u=0$, $v=0$ 일 때 확산된 영상 D_{Si}' 한 블록의 비확산 처리 과정이 된다. 그리고 위 식(27)의 과정을 블록 계수만큼, 즉 원 영상의 크기만큼, 반복적 처리하여 조합을 하면, 원 영상의 크기를 구할 수 있다. 식 (25)를 식 (27)의 과정을 반복한 후 다음과 같이 역-푸리에 변환을 한다.

$$\begin{aligned} IFT\{D_{Di}'(\zeta,\eta)\}&=IFT\left[\frac{2\alpha\pi}{K}E_i(\zeta,\eta)\right]+IFT\left[\frac{2\alpha\pi}{K}r_i(\zeta,\eta)\right] \\ &=e'(x,y)+r'(x,y). \end{aligned} \tag{28}$$

그러면 간단하게 $e'(x,y)$, $r'(x,y)$는 각각 $IFT\{(2\alpha\pi/K)E(\zeta,\eta)\}$, $IFT\{(2\alpha\pi/K)r_i(\zeta,\eta)\}$ 로 같다.

CCD 평면상에 복구된 영상 $R_{CCD}(x,y)$는

$$\begin{aligned} R_{CCD}(x,y)&=|e'(x,y)+r'(x,y)|^2 \\ &=|e'(x,y)|^2+e'(x,y)r'(x,y)^*+e'(x,y)^*r'(x,y)+|r'(x,y)|^2 \end{aligned} \tag{29}$$

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

$$+ e'(x,y) r'(x,y)^* + e'(x,y)^* r'(x,y) + |r'(x,y)|^2$$

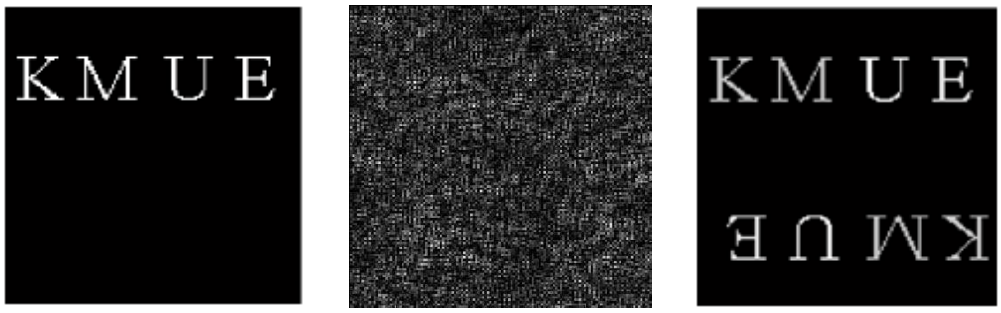
$$= \left(\frac{2\alpha\pi}{K} \right)^2 [O_i'(x,y)]^2 + e'(x,y) r'(x,y)^* + e'(x,y)^* r'(x,y) + |r'(x,y)|^2$$

와 같이 표현된다. 여기서 $\exp[jn'(x,y)]$ 는 $Re[FT\{\exp[jn(x,y)]\}]$의 역-푸리에 변환 결과이며, $O_i'(x,y)$는 $Re[FT\{O_i(x,y)\}]$의 역-푸리에 변환의 결과로 실질적인 복구 패턴이다. 또한 식 (29)에서, $e'(x,y)r'(x,y)^* + e'(x,y)^* r'(x,y)$와 $|r'(x,y)|^2$은 화이트 잡음과 같은 형태로 매우 작은 값으로 각각 복구 영상의 실수부와 허수부 그리고 결과 면에 무작위 분산된다. 그러므로 복구된 영상이 출력이 가능하다. 우리는 지수 부분을 작은 값으로 만들기 위해 K를 사용하였다.

Ⅳ 실험 및 고찰

1. 실험

본 논문에서는 타당성을 검증하기 위해 제안한 방법으로 컴퓨터 모의실험을 통해 수행하였다. 4개의 계층을 수행하기 위하여 4개의 원 영상을 사용하였으며 사용한 영상들을 그림 15에 나타내었고 영상 크기는 128×128이다. 그림 15(a)는 복원할 원 영상 $f_i(x,y)$로 64×64 픽셀 크기의 'K'와 'M', 'U', 'E'를 제로 패딩하고 더하여 사용하였고 이진 값을 가진다. 그림 15(b)는 그림 15(a)를 푸리에 변환하여 실수부 갖는 암호화 된 영상 $E_i(\zeta,\eta)$이고 그림 15(c)는 그림 15(b)를 역-푸리에 변환하여 복구한 영상이다.



(a) (b) (c)

그림 15. 컴퓨터 실험 결과 (128×128): (a) 제로 패딩된 원 영상 $f_i(x,y)$, (b) 암호화된 영상 $E_i(\zeta,\eta)$, (c) 복구 영상

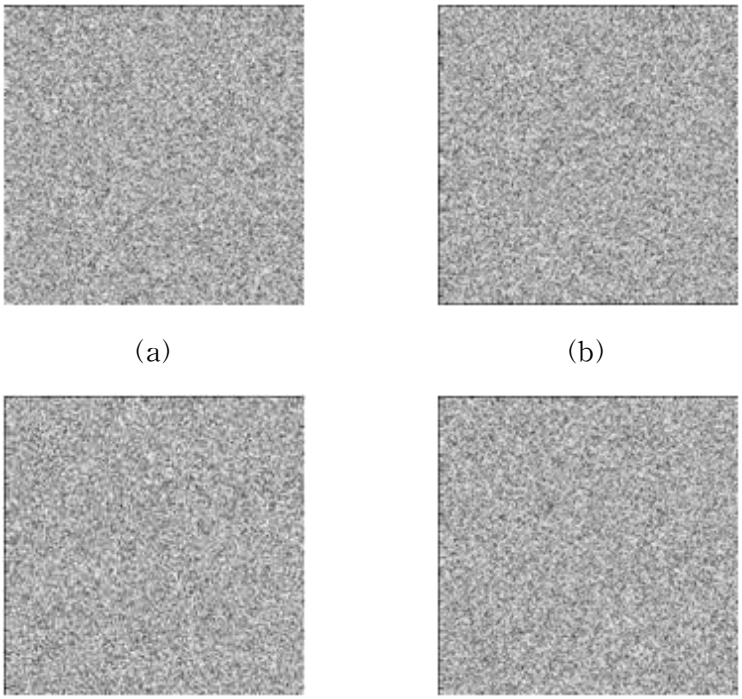
Fig. 15. Computer simulation results (128×128): (a) zero-padded the original image $f_i(x,y)$, (b) encoded image $E_i(\zeta,\eta)$, (c) reconstructed image

그림 16은 각각 커버 영상 $C(\zeta,\eta)$, 암호화된 영상과 왈시 코드 영상으로부터 만들어진 삽입 영상 $\alpha W_i\tilde{h}(u,v)$, 그리고 워터마크 영상 $S(\zeta,\eta)$이다. 영상들의 크기는 각각 1024×1024이다. 여기서 α값과 K값은 각각 0.5와 100으로 하였다. 삽입 영상에 상용된 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 임의의 왈시 코드로 왈시 코드 영상(1024×1024)을 만들었다. 이때 숨김 영상들의 동일한 픽셀 위치에는 서로 다른 왈시 코드를 사용하였으며, 만약 중복성이 허용되면, 복원할 때 서로 간섭을 주어 원 영상의 복원이 어렵게 된다. 그리고 왈시 코드의 크기와 왈시 코드를 대응시킨 모영 정보는 복호화 시 또 다른 복원 정보로 사용된다.

(a) (b) (c)

그림 16. 컴퓨터 실험 결과 (1024×1024): (a) 커버 영상 $C(\zeta,\eta)$, (b) 삽입 영상 $\alpha W_i\tilde{h}(u,v)$, (c) 워터마크 영상 $S(\zeta,\eta)$

Fig. 16. Computer simulation results (1024×1024): (a) cover image $C(\zeta,\eta)$, (b) embedded image $\alpha W_i\tilde{h}(u,v)$, (c) watermark image $S(\zeta,\eta)$

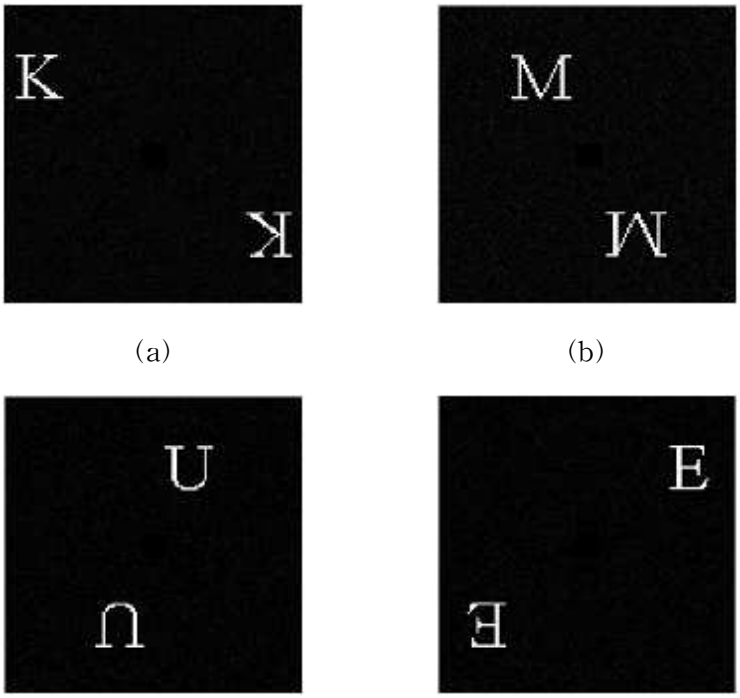


(a) (b)

(c) (d)

그림 17. 컴퓨터 실험 결과 : (a) 'K' 복호화 키 영상, (b) 'M' 복호화 키 영상 (c) 'U' 복호화 키 영상. (d) 'E' 복호화 키 영상

Fig. 17. Computer simulation results : (a) 'K' Decoding key image (1024×1024), (b) 'M' Decoding key (1024×1024), (c) 'U' Decoding key (1024×1024), (d) 'E' Decoding key (1024×1024).



(a) (b)

(c) (d)

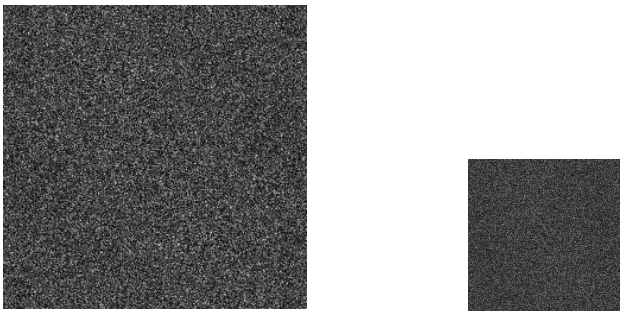
그림 18. 컴퓨터 실험 결과 : (a) 'K' 복호화 키로 복원한 영상, (b) 'M' 복호화 키로 복원한 영상 (c) 'U' 복호화 키로 복원한 영상. (d) 'E' 복호화 키로 복원한 영상

Fig. 18. Computer simulation results : (a) Decryption image with 'K' decoding key (128×128), (b) Decryption image with 'M' decoding key (128×128), (c) Decryption image with 'U' decoding key (128×128), (d) Decryption image with 'E' decoding key(128×128).

복호화 과정에서 스테고 영상과 복호화 키 영상을 곱하여 비확산 시킨 후 역-푸리에 변환을 하면 복구된 영상을 얻을 수 있다. 그림 17 (a)~(d)는 각각 'K', 'M'과 'U', 'E' 복호화 키 영상(1024×1024)들이다. 그리고 그림 18 (a)~(d)는 각각 그림 17의 복호화 키들을 이용해 복원한 'K', 'M'과 'U', 'E'의 복원 영상들이다. 하나의 워터마크 영상에서 원하는 영상의 복호화 키를 사용하여 복구가 가능하고 큰 사이드 로브가 제거된 복구 영상을 얻을 수 있다.

2. 고찰

1) 비확산의 크기와 거짓 복호화 키에 대한 고찰



(a) (b)

그림 19. 잘못된 정보로 복원한 결과 영상 : (a) 비확산의 크기가 다를 때 복원 영상 (256×256) (b) 복호화 키 영상 다를 때 복원 영상 (128×128)

Fig. 19. Reconstructed images with incorrect information : (a) incorrect order of keys, (b) Decryption key image with inaccuracy.

그림 19(a)는 비확산의 잘못된 크기의 정보(4×4)로 암호화 영상을 복원한 영상이며, 그림19(b)는 거짓 왈시 코드를 사용하여 복원한 영상으로 원 영상복

원이 불가능 하였다. 따라서 원 영상을 복원하기 위해서는 왈시 코드의 크기와 매핑 할 때의 모양의 정보를 알고 있어야 복원이 가능하면, 잘못된 정보로 복원 하였을 경우, 원 영상의 크기와 모양을 제대로 복원 하지 못하였으며, 거짓 복호화 키를 사용하였을 경우 역시 원 영상을 복원 할 수 없었다. 따라서 암호화 영상에 사용된 왈시 코드영상과 코드의 매핑 크기와 모양의 정보, 그리고 무작위 위상 영상의 정보가 모두 있어야 원 영상의 복원이 가능하다.

2) 스테고 영상의 손실에 대한 고찰

손실에 따른 정력적 지표로 PSNR(Peak Signal to Noise Ratio)은

$$\mathrm{PSNR} = 20*\log 10\left(\frac{1}{rms}\right) \quad (dB) \tag{18}$$

과 같다. 이때 b는 입력 신호의 가장 큰 수이며, rms 는 root mean square 이다. 그림 20은 α와 K 값의 변화에 따른 커버 영상과 워터마크 영상 사이의 PSNR을 구한 것이다. 그림 20에서 보는 바와 같이 α 값이 커질수록 K 값이 적을수록 손실이 커진다는 것을 알 수 있다. 본 논문에서는 α와 K 값은 각각 0.2와 100으로 선택하여 36.1 $[dB]$에서 모의실험을 실행 하였다.

그림 21 (a), (b), (c)는 x축 방향으로 각각 25%, 50%, 75% 차단한 워터마크 영상이며, 그림 22, 그림 23, 그림 24는 각각 x축 방향으로 25%, 50%, 75% 차단된 워터마크 영상의 복원 영상이다. 이번 모의실험을 통해서 워터마크 영상이 블록이 되더라도 영상이 복원됨을 알 수 있었다.

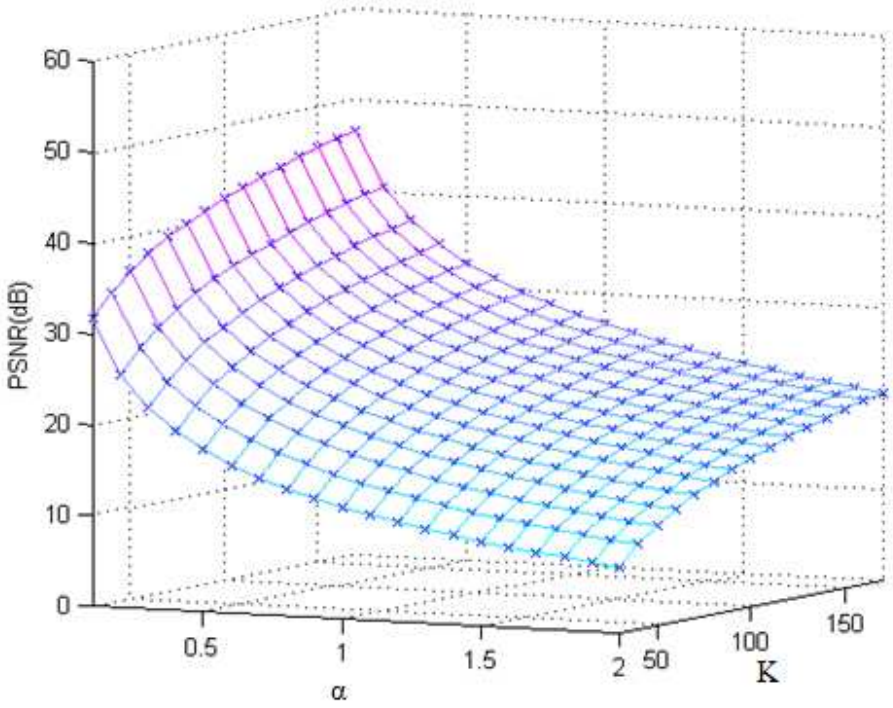


그림 20. α와 K 값의 변화에 따른 커버 영상과 워터마크 영상 사이의 PSNR

Fig. 20. PSNR for both the cover image and the watermark image based on the value of α and K.

(a) (b) (c)

그림 21. 절단에 따른 스테고 영상 : (a) 25%. (b) 50%. (c) 75%.

Fig. 21. For the block, the occluded stego image : (a) 25%. (b) 50%. (c) 75%.

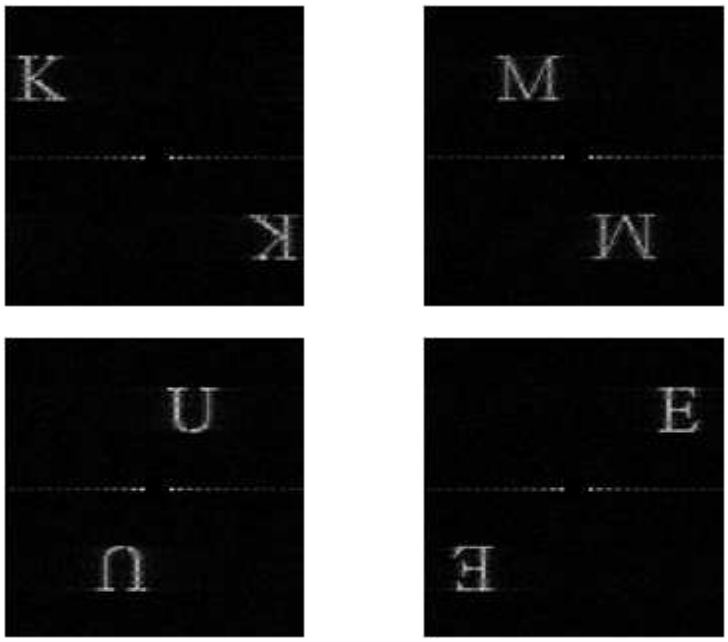


그림 22. 25% 절단된 스테고 영상에 대한 복원 영상들

Fig. 22. For 25% the block, the reconstruction image by the occluded stego image

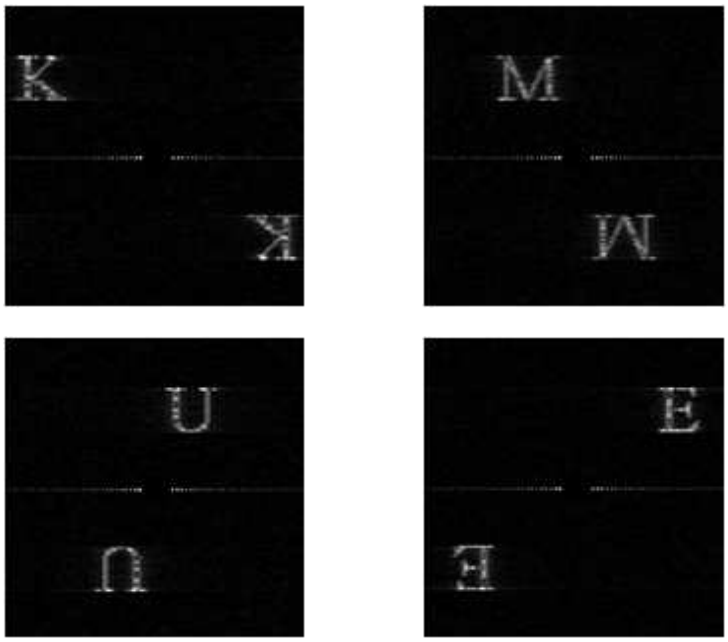


그림 23. 50% 절단된 스테고 영상에 대한 복원 영상들

Fig. 23. For 50% the block, the reconstruction image by the occluded stego image

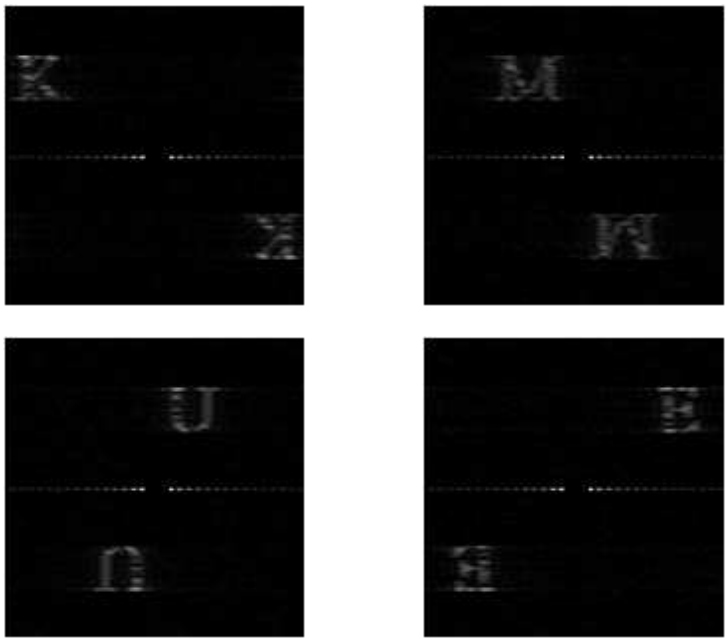


그림 24. 75% 절단된 스테고 영상에 대한 복원 영상들

Fig. 24. For 75% the block, the reconstruction image by the occluded stego image

Ⅴ. 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 필수부가결한 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 0 이 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.

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.

참 고 문 헌

[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] H. Naor and A. Shamir, "Visual cryptography," Advanced in Cryptography Eurocrypto'94, vol. 950, no. 7, pp. 1-12, 1995.

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

[5] 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.

[6] 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.

[7] B. Javidi, G. Zhang, and Jian Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification," Opt. Eng., vol. 35, no. 9, pp. 2506-2512, 1996.

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

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

[10] T. Nomura and B. Javidi, “Optical encryption system with a binary key code,” Appl. Opt., vol. 39, no. 26, pp. 4783-4787, 2000.

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

[12] 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.

[13] B. Javidi, A. Sergent, and E. Ahouzi, “Performance of double phase encoding encryption technique using binarized encrypted images,” Opt. Eng., vol. 37, no. 2, pp. 565-570, 1998.

[14] 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.

[15] C. H. Yeh, H. T. Cahng, 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, Oct. 2002

[16] Nam-Jin Kim, Dong-Hoan Seo, and Sung-Geun Lee, Chang-Mok Shin, Kyu-Bo Cho, and Soo-Joong Kim, "Hierarchical Image Encryption System Using Orthogonal Method," Optical Society of Korea, Volume 17, Number 3, June 2006.

[17] J. D. Gaskill, "Linear System Fourier Transforms and optics," Chap 4

[18] Sheng Huang and Jian Kang Wu, "Optical Watermarking for Printed Document Authentication," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 2, NO. 2, pp. 164-173, JUNE 2007.

[19] David Abookasis, Ofir Montal, Ohad Abrannson, and Joseph Rosen, “Watermarks encrypted in a concealogram and deciphered by a modified joint-transform correlator," APPLIED OPTICS, Vol. 44, No. 15, pp. 3019-3023, 20 May 2005.

[20] Guohai Situ, Jingjuan Zhang, "Image hiding with computer-generated phase codes for optical authentication," Optics Communications 245 pp. 55-65, 2005.

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

[22] Hsuan T. Chang and Chung L. Tsan, "Image watermarking by use of digital holography embedded in the discrete-cosine-transform domain," APPLIED OPTICS Vol. 44, No. 29, pp. 6211-6219, 10 October 2005.

[23] P-L. Lin, "Robust Transparent Image Watermarking System with Spatial Mechnisms," *The Journal of Systems and software*, vol. 50, pp. 107-116, Oct. 2000.

[24] N. Nikolaidis, and L. Pitas, "Robust Image Watermarking in the Spatial domain," *Signal processing*, vol. 66, no. 3, pp. 384-403, Oct. 1998.

[25] Kyu-Bo Cho, Dong-Hoan Seo, and Soo-Joong Kim, "Practical Image Hiding Method Using a Phase Wrapping Rule and Real-Valued Decoding Key," Optical review, Vol. 14, No. 3 (2007).