

스크램블 연산 및 위상 천이 디지털 홀로그래피 기반 영상 이중 암호화

(Double Encryption of Image Based on Scramble Operation and Phase-Shifting Digital Holography)

김 철 수^{1)*}
(Kim Cheol-Su)

요 약 본 논문에서는 스크램블 연산(Scramble Operation) 및 위상 천이 디지털 홀로그래피(PSDH; Phase Shift Digital Holography) 기반 영상 이중 암호화 방법을 제안한다. 암호화하고자 하는 영상을 스크램블 연산을 통해 디지털적으로 1차 암호화를 수행한 후, 위상 변조하고, 위상을 천이시킨 기준파와의 간섭을 통해 2차 암호화 정보를 얻는다. 복호화 과정은 암호화 과정의 역순으로 진행된다. 두 개의 암호화된 영상들을 적절하게 산술 처리하는 위상 천이 디지털 홀로그래피 기술을 통해 디지털적으로 1차 복호화하고, 위상 복조를 한 후, 스크램블 연산 시에 사용한 암호화 키 정보를 이용하여 원래의 영상을 복원한다. 제안된 암호화 방법은 스크램블 연산에 사용된 두 개의 키 정보와 위상 천이 디지털홀로그래피 기술에서 사용된 거리 정보, 광원의 파장 등의 정보를 모두 정확하게 알아야만 원래의 영상을 복원할 수 있다.

핵심주제어 : 스크램블 연산, 위상 천이 디지털 홀로그래피, 이중 암호화 기술, 위상 변조/복조, 이중 암호화 기술

Abstract In this paper, double encryption technology of image based on scramble operation and phase-shifting digital holography is proposed. For the purpose, we perform first encryption digitally using scramble operation for the to be encrypted image, and perform phase modulation to the first encrypted image. Finally, we get the secondary encryption information through the interference between the phase-shifted reference wave and phase modulated image. The decryption process proceeds in the reverse order of the encryption process. The original image is reconstructed by digitally decoding the two encrypted images through a phase shift digital holography technique that appropriately performs arithmetic processing, phase-demodulating and then using the encryption key information used in the scramble operation. The proposed cryptosystem can recover the original image only if both the key information used in the scramble operation, the distance information used in the phase shift digital holography technique, and the wavelength of the light source are known accurately.

* Corresponding Author : kcs6694@hanmail.net
Manuscript received July 10, 2018 / revised July 31, 2018 /
accepted August 8, 2018

1) 경주대학교 전기에너지컴퓨터공학과, 제1저자 및 교신저자

Key Words : Scramble Operation, Phase-Shifting Digital Holography, Phase Modulation/ Demodulation, Double Encryption Technology

1. 서론

현재 사회는 컴퓨터와 정보통신기술이 융합된 네트워크 사회로 다양한 정보의 유통으로 엄청난 양의 디지털 정보가 발생하고 있고, 정보가 갖는 가치가 사회의 중심 자원으로 이용되고 있는 상황이다. 이와 같은 디지털 정보는 네트워크를 통한 정보 공유 및 전송에는 상당한 이점이 있지만 쉽게 복제가 가능한 단점이 있기 때문에 디지털 정보의 역기능인 불법 복제나 유통을 방지하기 위한 많은 저작권 보호 및 정보보호 방법들이 제안되어 왔다[1-2]. 광학적인 정보 암호화 방법에는 두 개의 랜덤 위상 마스크를 이용하는 이중 랜덤 위상 부호화 방법, XOR 연산을 이용하는 암호화 방법, 편광원리를 이용한 암호화 방법, 그리고 디지털 홀로그래피를 이용한 암호화 방법 등이 있으며[3-6], 본 논문에서는 디지털 홀로그래피를 이용한 새로운 암호화 방법을 제안하고자 한다. 디지털 홀로그래피(Digital Holography)는 물체파(Object Wave)와 기준파(Reference Wave)의 간섭세기를 홀로그래픽 기록 매질 없이 CCD(Charge Coupled Device)카메라에 직접 실시간적으로 기록하고, 이들 간섭 정보를 디지털적으로 처리하여 원래의 물체 영상 정보를 복원하는 기술로써, 광축(On-Axis) 구조의 간섭계로부터 얻은 단일 간섭 정보에서는 0차 항 및 역역상(Inverse Image)이 항상 존재하기 때문에 복원되는 영상의 질(Quality)이 떨어지는 단점이 있다[7-8]. 이러한 문제점을 해결하기 위해 다양한 방법들이 연구되어 왔고, 그 방법들 중 하나가 기준파의 위상을 천이시켜 가면서 간섭세기를 여러 개 구한 후, 디지털 계산 처리과정과 프레즈넬 변환(Fresnel Transform)을 거쳐 복원하는 위상 천이 디지털 홀로그래피(Phase-Shifting Digital Holography; PSDH) 기법이다[9-13]. PSDH 기술을 이용하여 원래 물체 영상 정보를 완벽하게 복원하기 위해서는 3개 이상의 간섭 정

보를 이용해야 한다고 알려져 있다. 2개의 간섭 정보를 이용할 경우에는 기준파와 물체파와의 세기 비 및 간섭 패턴의 가시성(Visibility) 정보가 복원 영상의 성능을 결정하는 중요한 인자가 된다[10]. 즉, PSDH 기법은 CCD 카메라를 통해 간섭 세기를 얻게 되는데, 간섭 세기의 세기 대역이 CCD 카메라가 수용할 수 있는 세기 대역을 초과하게 되거나, 물체 영상의 밝기 정도에 따라 간섭 세기의 패턴과 세기 범위가 결정되면 재생되는 영상의 질에 상당한 문제점을 초래할 수 있기 때문이다. 그러므로 입력 영상의 밝기 정도에 상관없이 항상 일정하고, 균일한 간섭 세기 분포를 얻을 수 있는 방법이 필요하다.

본 논문에서는 암호화하고자 하는 입력 영상에 대해 랜덤하게 발생시킨 열 키 정보(Column Key Information)와 행 키 정보(Row Key Information)를 활용하여 각각 스크램블 연산(Scramble Operation)을 디지털적으로 처리하여 1차 암호화를 한 후[14], 이를 다시 위상 변조함으로써 균일한 크기를 갖는 잡음과 유사한 형태의 물체파를 만들었으며, 이를 위상 천이된 기준파들과 간섭시켜 랜덤 잡음 형태의 간섭 패턴을 얻는 2차 암호화 과정을 수행하였다. 이들 간섭 패턴은 CCD 카메라의 세기 대역(Intensity Range)을 벗어나지 않으므로 정확하게 디지털 값으로 변환할 수 있다.

복호화 과정은 암호화 과정의 역순으로 진행되는데, 2차 암호화된 두 개의 간섭세기 정보를 디지털 처리과정 및 역프레즈넬(Inverse Fresnel Transformation) 변환을 통해 1차 복원하고, 이를 위상 복조(Phase Demodulation)한 후, 다시 디스크램블 연산(Descramble Operation)을 통해 2차로 복원하게 된다. 그리고 복호화 과정에서는 1차 암호화 과정에서 사용된 두 개의 키 정보와 2차 암호화 과정에서 사용된 입력 평면과 CCD 카메라 사이의 거리 및 사용된 광원의 파장 정보 등을 정확하게 알아야만 왜곡 없이 원래의 물체

영상을 복원할 수 있다. 이 기술은 정보보호 분야뿐만 아니라 3차원 디스플레이 및 디지털 홀로그래피 그래픽 현미경 등에도 널리 사용이 되고 있으며, 추후 광고 또는 교육 서비스 분야에서도 많은 활용이 예상된다[15].

본 논문의 구성의 다음과 같다. 2장에서는 스크램블 연산 및 위상 천이 디지털 홀로그래피 기술에 대해 설명하고, 3장에서는 제안한 영상 이중 암호화 및 복호화 방법과 광학적 구성도에 대해 설명한다. 4장에서는 컴퓨터 모의실험을 통해 제안한 암호화 방법의 성능을 확인하고, 마지막으로 5장에서 결론을 맺도록 한다.

2. 본 론

2.1 스크램블 연산

입력영상의 암호화 과정은 2단계로 나뉘며, 입력영상의 1차 암호화를 수행하기 위해 랜덤하게 발생시킨 열 키 정보와 행 키 정보를 기반으로 두 번의 스크램블 연산을 입력영상에 적용한다. 두 번의 스크램블 연산을 거친 결과 영상은 원래의 영상과는 형태가 전혀 다른 랜덤 잡음과 유사한 형태를 갖는데, 이를 1차 암호화된 영상이라고 한다. 스크램블 연산을 통한 암호화 과정을 Fig. 2에 나타내었다. 테스트 영상을 가로 및 세로 방향으로 5개 블록으로 나눈 후, 이에 대한 열 키 정보와 행 키 정보를 랜덤하게 발생시키고, 두 키 정보에 기반하여 스크램블 연산을 함으로써 1차 암호화 하였다. 이들 두 개의 키 정보는 복호화 과정에서도 반드시 필요한 보안요소가 된다.

Fig. 1(a)는 5x5 블록으로 나뉘어진 테스트 영상을 나타내고, Fig. 1(b)는 랜덤하게 발생시킨 행 키 정보 기반으로 행 방향으로 스크램블된 테스트 영상을 나타내며, Fig. 1(c)는 Fig. 1(b)를 다시 열 키 정보를 기반으로 열 방향으로 스크램블한 테스트 영상을 의미한다. 두 번의 스크램블 연산을 거친 암호화된 영상은 원래의 테스트 영상과는 전혀 다른 형태의 영상을 가지는 것을 확인할 수 있다.

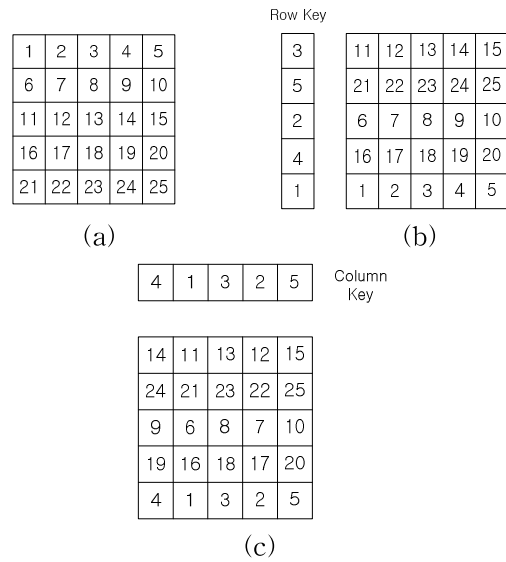


Fig. 1 Example of Scramble Operation Process. (a) Test Image, (b) Scrambled Test Image in Row Direction and (c) Scrambled Test Image in Row and Column Directions.

2.2 위상 천이 디지털 홀로그래피

디지털 홀로그래피(Digital Holography)는 물체파와 위상 천이된 기준파 사이의 간섭 패턴을 CCD로 획득하고, 이들 간섭패턴을 컴퓨터로 디지털 처리하여 2차원 또는 3차원 영상을 복원하는 기술이다. 이 과정을 설명하기 위해 그림으로 나타내면 다음과 같다.

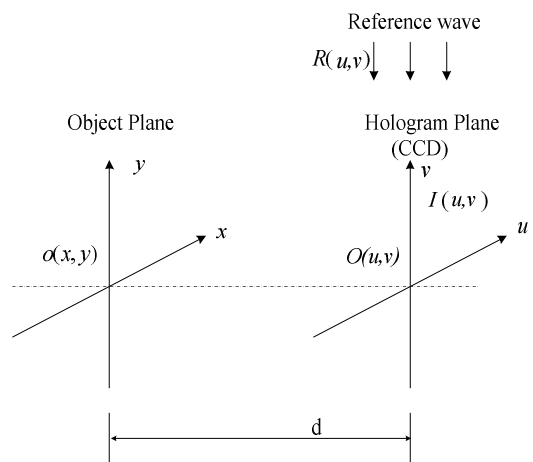


Fig. 2 Coordinate System in Digital Holography

(x, y) 평면의 임의의 물체로부터 반사된 물체파 함수를 $o(x, y)$ 라 하면, 물체로부터 d 만큼 떨어진 위치에서의 물체파는 프레즈넬 변환에 의해 $O(u, v)$ 로 표현되며 다음 식과 같다.

$$O(u, v) = \frac{\exp(ikd)}{i\lambda d} \iint o(x, y) \times \exp\left[i\pi \frac{(x-u)^2 + (y-v)^2}{d\lambda}\right] dx dy \quad (1)$$

여기서 $i = \sqrt{-1}$ 이고, λ 는 사용된 광원의 파장이며, k 는 파수(Wave Number)를 의미하며, d 는 프레즈넬 변환 거리이다. 홀로그램 평면에서 물체파 함수 $O(u, v)$ 와 기준파 함수 $R(u, v)$ 는 복소함수로 표현된다.

$$O(u, v) = |O(u, v)| \exp[i\phi_O(u, v)] \quad (2)$$

$$R(u, v) = |R(u, v)| \exp[i\phi_R(u, v)] \quad (3)$$

홀로그램 평면에서 물체파와 기준파는 서로 간섭을 일으키고, 그 간섭세기는 CCD카메라에 기록된다. 이때 기준파의 경로에 위상 천이기를 설치하여 기준파의 위상 값을 제어하면서 간섭 세기를 얻고, 이들 간섭 세기를 이용하여 디지털적으로 처리하면 홀로그램 평면에서의 물체파 함수 $O(u, v)$ 를 얻을 수 있다. 위상 천이기를 통과한 기준파 $R(u, v)\exp(j\theta)$ 와 물체파 함수 $O(u, v)$ 사이의 간섭 세기는 다음 식으로 표현된다.

$$\begin{aligned} I(u, v; \theta) &= |O(u, v) + R(u, v)\exp(i\theta)| \times \\ &= |O(u, v) + R(u, v)\exp(i\theta)|^* \times \\ &= I_O(u, v) + I_R(u, v) + 2|O(u, v)||R(u, v)| \times \\ &= \cos[\phi_O(u, v) - \phi_R(u, v) - \theta] \end{aligned} \quad (4)$$

여기서 $I_O(u, v) = |O(u, v)|^2$ 이고, $I_R(u, v) = |R(u, v)|^2$ 이다. 식 (4)에서 간섭세기 $I(u, v; \theta)$ 의 첫 번째항과 두 번째 항은 DC 성분을 나타내고, 세 번째 항에서 물체파 함수를 추출한 후, 역프레즈넬 변환을 수행하면 원래의 영상이 복원된다.

이를 위해서 위상 천이 디지털 홀로그래피 기술을 이용하는데, 이는 기존의 광축 구조를 갖는

디지털 홀로그래피 시스템의 기준파 경로에 위상 천이기를 설치하고, 기준파의 위상 값을 제어하면서 두 개 이상의 간섭세기를 구한 후, 그 세기 값들을 이용해서 물체파 함수 $O(u, v)$ 를 완벽하게 재생할 수 있는 기술이다. 기준파의 위상 천이 값 θ 를 0과 $\pi/2$ 로 각각 변화시켜 가면서 얻은 간섭세기를 간략히 표현하면

$$I_1 = I(u, v; 0) \quad (5)$$

$$I_2 = I(u, v; \frac{\pi}{2}) \quad (6)$$

와 같다. 위의 2 개의 간섭세기 만을 이용하는 2-단계 위상 천이 디지털 홀로그래피 방법에서는 다음 식을 이용해서 원래의 물체파 함수를 복원할 수 있다.

$$O'(u, v) = \frac{1}{2R(u, v)^*} [(I_1 - I_O - I_R) + j(I_2 - I_O - I_R)] \quad (7)$$

이렇게 구해진 복소함수 $O'(u, v)$ 를 디지털적으로 역프레즈넬 변환을 하면 원래의 물체파 함수와 거의 유사한 $o'(x, y)$ 를 복원할 수 있으며, 다음 식으로 표현된다.

$$\begin{aligned} o'(x, y) &= \frac{\exp(ik(-d))}{i\lambda(-d)} \times \\ &= \frac{\exp(ik(-d))}{i\lambda(-d)} \exp\left[\frac{ik}{2d}(x^2 + y^2)\right] \times \\ &= \text{FFT2D}\left\{O'(u, v)\exp\left[\frac{ik}{2(-d)}(u^2 + v^2)\right]\right\} \end{aligned} \quad (8)$$

여기서 FFT2D는 2차원 푸리에 변환 연산을 의미한다.

3. 제안한 영상 이중 암호화 방법

본 논문에서 제안하는 스크램블 연산 및 PSDH 기반 영상 이중 암호화 및 복호화 과정은 2단계로 이루어지며, 두 과정의 블록도는 Fig. 3과 같다.

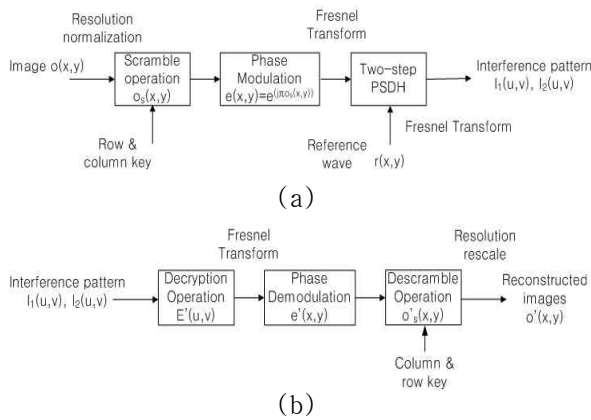


Fig. 3 Block Diagrams for (a) Image Encryption and (b) Decryption Process

암호화 과정은 입력 영상 $o(x,y)$ 에 대해 해상도 정규화(Resolution Normalization)를 거친 후, 행 및 열 키 정보를 기반으로 한 스크램블 연산을 통해 1차 암호화 과정을 수행한다. 1차 암호화된 영상 정보인 $o_s(x,y)$ 는 위상 변조되어 $e(x,y) = e^{j\pi o_s(x,y)}$ 가 된 후, 2-단계 PSDH기법에 의해 위상제어기가 장착된 기준파 함수 $r(x,y)$ 와의 간섭을 통해 2개의 간섭세기 $I_1(u,v)$ 와 $I_2(u,v)$ 를 얻는데, 이것이 최종 2차 암호화 영상이 된다. 암호화 과정에서 스크램블 연산을 통해 잡음 형태의 영상으로 암호화한 후, 이를 다시 위상 변조 함수로써 입력 영상의 밝기 정도에 무관한 일정한 세기의 물체파를 만들 수 있으며, 기준파와의 간섭 패턴 또한 항상 일정한 세기 대역을 갖게 할 수 있어 상용 CCD 카메라로도 간섭 패턴의 정보를 정확한 디지털 값으로 변환할 수 있게 된다.

복호화 과정은 암호화 과정의 역과정이라고 할 수 있으며, 2 개의 간섭세기 정보로부터 식 (7)을 적용하여 1차 암호화된 영상 정보 $E'(u,v)$ 를 얻는다. 그리고 프레즈넬 변환과 위상 복조화를 수행하여 $e'(x,y)$ 를 구한 후, 암호화 시에 사용한 행 및 열 키 정보와 디스크램블 연산을 통해 최종 복원된 원 영상 $o'(x,y)$ 을 얻을 수 있게 된다. 제안한 방법에서 2차 암호화 정보인 간섭 세기를 얻는 광학적 실험 구성도는 Fig. 4와 같다.

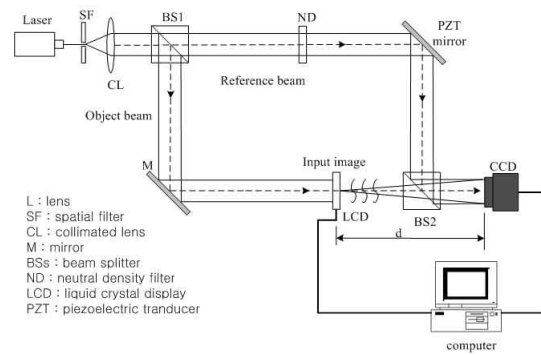


Fig. 4 Optical Schematic Diagram for Implementing the PSDH

그림에서 LCD에 올려지는 입력 영상은 1차 암호화된 후, 위상 변조된 정보이며, 이 위상 변조된 영상 정보와 PZT(Piezoelectric Transducer) Mirror에 의해 위상이 제어된 기준파가 간섭을 일으키고, 그 간섭 세기가 CCD에 기록된다. 이 간섭 세기 정보가 2차 암호화된 영상 정보인 것이다. 간섭 실험에서 사용된 광원의 파장, LCD의 스펙(Specifications), 그리고 입력 평면과 CCD 사이의 거리 등이 2차 암호화 키 정보에 해당한다고 할 수 있다. 기준파의 세기는 ND(Neutral Density) 필터에 의해 세기가 제어되며, 위상은 PZT Mirror에 의해서 제어된다. 그리고 입력 평면과 CCD 카메라 사이의 프레즈넬 변환 거리(d)도 보안요소가 된다.

위의 1차 암호화 과정에서 사용된 스크램블 연산과 위상 변조 방법을 통해 물체파 함수의 크기를 일정하게 해 주고, 간섭패턴의 가시성을 높여주는 역할도 동시에 하도록 하였다. 최종 암호화 영상은 CCD 카메라를 통해 얻어지며, 1차 암호화 과정에서 사용된 행 및 열 키 정보뿐만 아니라 2차 암호화 과정에서 실험에 사용된 광원 및 CCD 카메라 등의 스펙들과 프레즈넬 거리 등이 또한 보안요소가 되며, 이러한 보안요소 정보들을 모두 알아야만 복호화 과정에서 정확한 물체파 함수를 복원할 수 있다.

4. 컴퓨터 모의실험 결과 및 고찰

본 논문에서 제안한 스크램블 연산 및 PSDH 기반 영상 이중 암호화 및 복호화 방법의 성능을 평가하기 위해 컴퓨터 시뮬레이션을 수행하였다. 시뮬레이션에 사용된 물체 영상은 256x256 크기의 명암도 영상(Gray Image)과 이진 영상(Binary Image)이며, 이를 Fig. 5에 나타내었다.

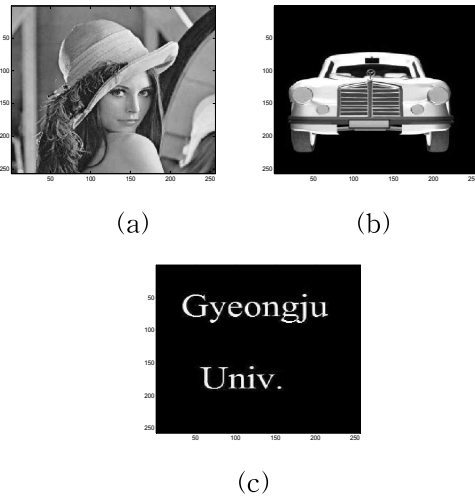


Fig. 5 Original Object Images; (a) Lena Image, (b) Car Image, and (c) Binary Image

이들 영상은 입력 평면의 전 영역을 차지하는 Lena 명암도 영상(256-Gray-Level), 중앙의 일부를 차지하는 Car 명암도 영상(256-Gray-Level), 그리고 중앙을 중심으로 균형있게 배치된 이진 영상으로 다양한 밝기와 형태를 가진다고 볼 수 있다. 또한 시뮬레이션에 사용된 광 실험 조건은 광원이 514nm의 Ar레이저이고, CCD 카메라의 화소 크기는 15.6μm x 15.6μm 이며, 영상 평면과 CCD 카메라 사이의 거리(d)는 300nm로 하였다. 먼저, 암호화 과정은 Fig. 3(a)의 블록도 순서대로 스크램블 연산을 통해 입력 영상에 대한 1차 암호화된 영상을 구하였고, 위상 변조 과정을 거친 후, 2-단계 PSDH 기술을 이용하여 2차 암호화된 2 개의 영상을 얻었다. 2차 암호화 과정에서 적용한 2-단계 PSDH 기술에서는 물체파와 기준파 사이의 세기 비에 따라 간섭 패턴의 시각성(Visibility)이 달라지고, 이에 따라 CCD 카메라로 정확하게 간섭 패턴 정보를 디지털로 변환할 수 없는 상황이 발생할 수 있어 최

종적으로 복원되는 물체 영상의 성능이 달라지게 되는 문제점 지니고 있다.

이 문제를 해결하기 위해 1차 암호화된 영상 정보를 위상으로 변조함으로써 입력 영상의 종류나 형태에 상관없이 항상 일정한 크기의 물체파를 생성하도록 하였고, 다양한 물체 영상에 대해 물체파와 기준파 사이의 세기 비 변화에 따른 최종적으로 복원되는 영상의 성능을 시뮬레이션을 통해 평가하였다. 성능평가에 사용된 비용함수는 원래의 물체파 함수 $o(x,y)$ 와 복원된 물체파 함수 $o'(x,y)$ 사이의 RMSE(Root Mean Square Error)이며, 다음과 같이 표현된다.

$$RMSE = \sqrt{\frac{1}{MN} \sum_{m=1}^M \sum_{n=1}^N [o(m,n) - o'(m,n)]^2} \tag{9}$$

여기서 $o(m,n)$ 과 $o'(m,n)$ 은 $o(x,y)$ 와 $o'(x,y)$ 를 이산적으로 표현한 함수이다. 기준파와 물체파 사이의 세기 비 변화에 따른 RMSE 성능을 Fig. 6에 나타내었다.

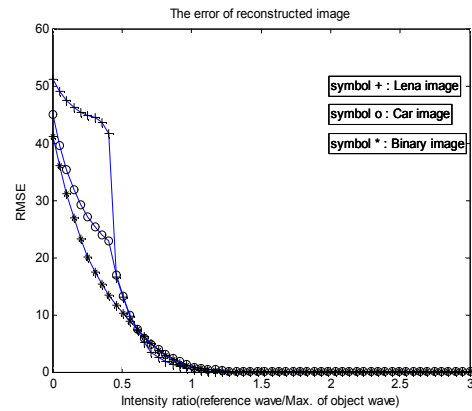


Fig. 6 RMSE Performance of Reconstructed Images according to the Intensity Ratio Variation between Reference Wave and Maximum of Phase Modulated Object Wave in 2-Step PSDH Technology.

세 개의 입력 영상에 대해 스크램블 연산 및 2-단계 PSDH 기법을 이용한 1차 및 2차 암호화

영상에 대한 시뮬레이션 결과를 Fig. 7에 나타내었다.

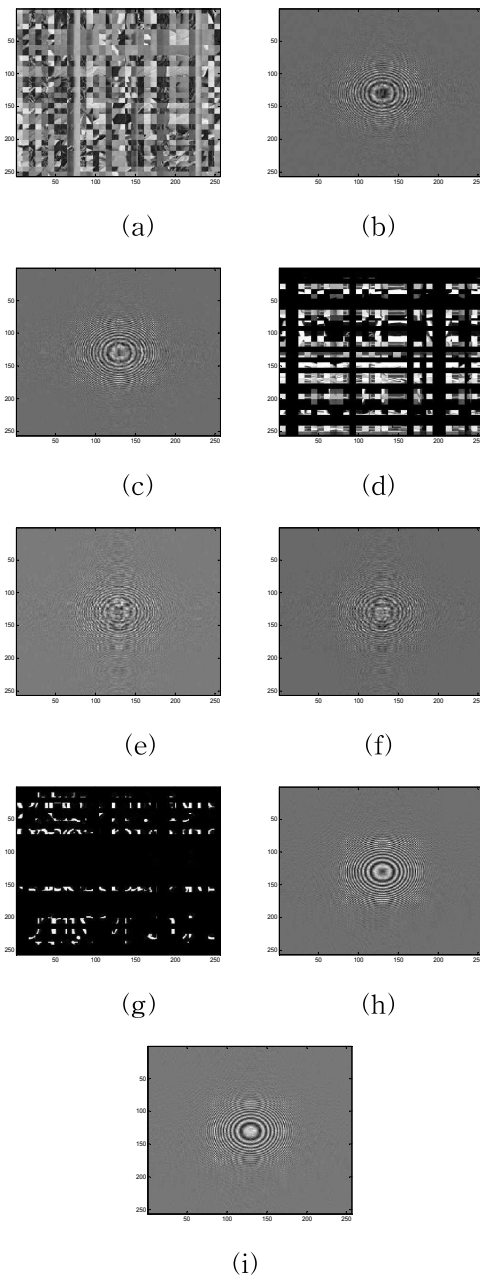


Fig. 7 Encrypted Images; (a) 1st Encrypted Lena Image, (b) and (c) are 2nd encrypted Lena Image, (d) 1st Encrypted Car Image, (e) and (f) are 2nd encrypted Car Image, (g) 1st Encrypted Binary Image, (h) and (i) are 2nd encrypted Binary Image.

1차 암호화를 위해 스크램블 연산에 사용된 블록의 크기는 8 화소(Pixels)이며, 랜덤하게 발생시킨 행 및 열 방향의 키 정보 32개를 각각 사용하여 암호화를 수행하였는데, 블록의 크기를 좀더 작게 하면 거의 잡음과 같은 형태의 암호화 정보를 얻을 수 있을 것으로 예상된다. 2차 암호화는 1차 암호화 영상 정보를 위상 변조하여 2-단계 PSDH 기법으로 암호화를 하였는데, 위상 변조로 인하여 입력 영상의 크기가 모두 균일하므로 영상에 상관없이 유사한 형태의 암호화 영상을 얻을 수 있었다.

복호화 과정은 암호화 과정의 역순인 Fig. 3(b)의 블록도 순서대로 진행된다. 두 개의 2차 암호화된 영상 정보를 식 (7)에 대입하여 디지털 처리한 후, 프레즈넬 변환을 통해 1차 복호화를 수행한다. 1차 복호화된 영상 정보를 위상 복조한 후, 디스크램블 연산을 수행하면 최종적으로 원래의 영상을 복원할 수 있게 된다. 복호화 과정에서는 암호화 과정에서 사용된 똑같은 암호화 요소 정보들(행 및 열 키 정보, 광원 파장, CCD 카메라 화소크기, 입력 평면과 CCD 카메라 사이의 거리)들을 사용해야만 원래의 입력 영상정보를 복원할 수 있다.

Fig. 8은 복호화 과정에서 입력 평면과 CCD 카메라 사이의 거리 정보만 암호화 시와 다를 경우, 복원되는 세 개의 입력영상을 나타내었고, Fig. 9는 열 방향 키 정보만 암호화 시와 다를 경우, 복원 영상이며, Fig. 10은 거리 정보 및 열 방향 키 정보가 암호화 시와 다를 경우, 복원되는 세 개의 영상들을 나타내었다. 그리고 Fig. 11은 복호화 과정에서 암호화 요소들이 암호화 과정에서의 값들과 모두 같을 경우 복원 되는 세 개의 영상을 나타냈었다. 시뮬레이션 결과로부터 입력 평면과 CCD 사이의 거리정보와 열 방향 키 정보만 틀려도 원래의 입력 영상 정보와 전혀 다른 영상들이 복원됨을 확인 할 수 있고, 암호화 및 복호화 과정의 보안 요소들이 모두 같을 경우에만 원래의 입력 영상을 완벽하게 복원할 수 있음을 확인하였다. 이와 같이 제안된 스크램블 연산 및 2-단계 PSDH 기반 영상 이중 암호화 방법은 입력 영상에 대해 위상 변조를 통해 간섭을 시키므로 항상 일정한 형태의 가시성이

좋은 간섭무늬를 생성시킬 수 있고, 기존의 3-단계 및 4-단계 PSDH 방법에 비해 암호화를 위해 획득해야 하는 간섭무늬의 수가 적기 때문에 컴퓨터 프로세서 및 데이터의 전송 관점에서 보면 더 효율적이라고 할 수 있다.

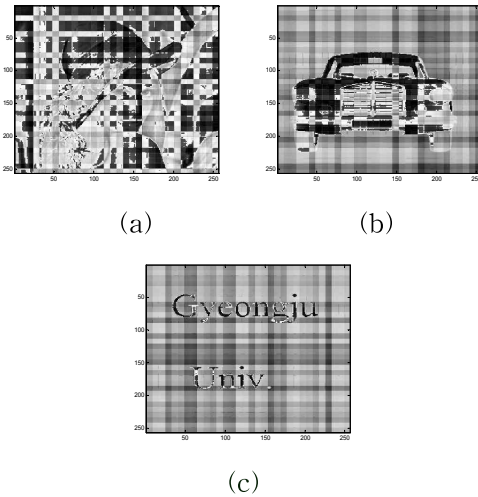


Fig. 8 The Decrypted Three Images, When $d(=295nm)$ is Different from that of the Encryption Process.

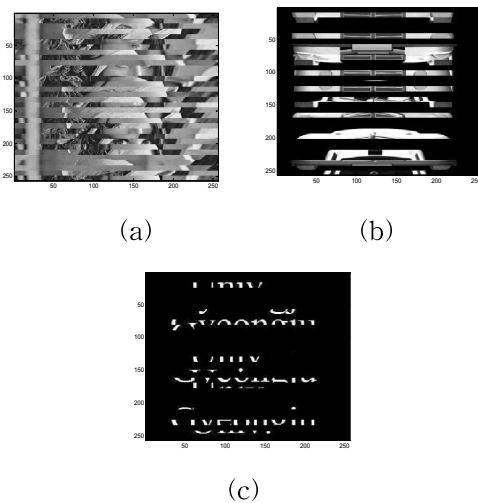


Fig. 9 The Decrypted Three Images, When Row Direction Key is Different from That of the Encryption Process.

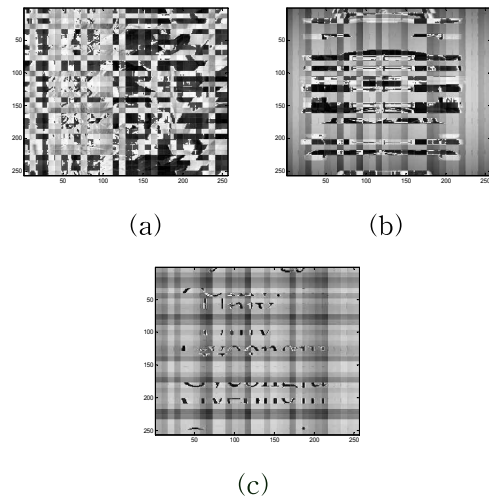


Fig. 10 The Decrypted Three Images, When $d(=295nm)$ and Row Direction Key are Different from Those of the Encryption Process.

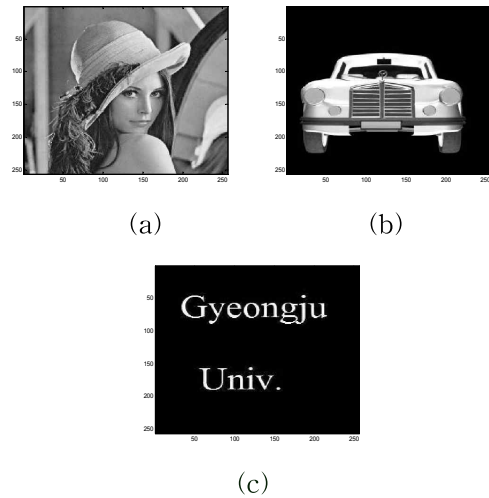


Fig. 11 The Decrypted Three Images, When $d(=300nm)$ and Row Direction Key are the Same as Those of the Encryption Process.

5. 결론

본 논문에서는 스크램블 연산 및 PSDH 기반 영상 이중 암호화 방법을 제안하였다. 제안한 암호화 방법은 2 단계를 거쳐 진행되며, 행 및 열

방향 스크램블 연산을 통해 1차 암호화되고, 1차 암호화된 영상 정보를 위상 변조 한 후, 2-단계 PSDH 기법에 의해 기준파와 간섭 무늬를 CCD 카메라로 획득함으로써 2차 암호화를 수행하였다. 복호화 과정은 암호화 과정의 역순으로 진행하면 되는데, 암호화 시에 사용된 많은 키 정보들을 정확하게 사용했을 때에만 원래의 영상을 복원할 수 있음을 컴퓨터 모의실험을 통해 확인하였다. 그리고 영상 정보를 위상 변조함으로써, 입력 영상의 형태에 상관없이 항상 일정한 형태의 물체파 및 간섭 패턴을 생성할 수 있는 장점이 있다. 제안된 방법은 디지털 처리 및 광 실험을 통한 두 번의 암호화 과정을 거치면서 사용된 키 정보가 많아서 보안능력이 한층 더 강화된 방법이라고 할 수 있다. 추후 연구는 한 번의 간섭 패턴 획득으로 원래의 영상을 복원할 수 있는 PSDH 방법에 대한 연구가 진행되어야 할 것으로 판단되며, 이와 같은 연구결과들은 암호화 분야뿐만 아니라 표면의 미세 두께 측정을 통한 반도체 기관 불량 검출 및 광학 현미경 제작에도 많은 기여가 예상된다.

References

- [1] Kim, T. H., Shin, H. D., and Park, S. H., "Software Protection Strategy through Digital Rights Management: Two Cases of Korean Firms," *Journal of Internet Electronic Commerce Research*, Vol. 9, No. 1, pp. 359-379, 2009.
- [2] Han, H. H., and Chang, H. S., "The Behavioral Model of Digital Music Piracy on the Web," *Journal of Information Systems*, Vol. 16, No. 1, pp. 135-158, 2007.
- [3] Refregier, P., and Javidi B., "Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding," *Opt. Lett.*, Vol. 32, No. 7, pp. 767-769, 1995.
- [4] Han, J. W., Park, C. S., Ryu, D. H., and Kim, E. S., "Optical Image Encryption Based on XOR Operations," *Opt. Eng.*, Vol. 38, No. 1, pp. 47-54, 1999.
- [5] Mogensen, P. C., and Gluckstad, J., "A Phase-Based Optical Encryption System with Polarisation Encoding," *Opt. Commu.*, Vol. 173, pp. 187-183, 2000.
- [6] Javidi, B., and Nomura, T., "Securing Information by Use of Digital Holography," *Opt. Lett.*, Vol. 25, No. 1, pp. 28-30, 2000.
- [7] Kreis, T. M., and Juptner, W. P. O., "Suppression of the DC Term in Digital Holography," *Opt. Eng.*, Vol. 36, No. 8, pp. 2357-2360, 1997.
- [8] Chen, G. L., Lin, C. Y., Kuo, M. K., and Chang, C. C., "Numerical Suppression of Zero-Order Image in Digital Holography," *Opt. Express*, Vol. 15, No. 14, pp. 8851-8856, 2007.
- [9] Yamaguchi I., "Phase-Shifting Digital Holography", *Opt. Lett.*, Vol. 22, No. 16, pp. 1268-1270, 1997.
- [10] Liu, J. P., Poon, T. C., Jhou, G. S., and Chen, P. J., "Comparison of Two-, Three-, and Four-Exposure Quadrature Phase-Shifting Holography," *Appl. Opt.*, Vol. 50, No. 16, pp. 2443-2450, 2011.
- [11] Zhang, S., and Zhou, J., "A New Estimation Method for Two-Step-only Quadrature Phase-Shifting Digital Holography," *Opt. Commu.*, Vol. 335, No. 1, pp. 183-188, 2015.
- [12] Yang, T. D., Kim, H. J., Lee, K. J., Kim, B. M., and Choi, Y., "Single-Shot and Phase-Shifting Digital Holography Microscopy Using a 2-D Grating," *Optics Express*, Vol. 24, No. 9, pp. 9480-9488, 2016.
- [13] Kim, C. S., "Double Encryption of Digital Hologram Based on Phase-Shifting Digital Holography and Digital Watermarking," *Journal of the Korea Industrial Information Systems Research*, Vol. 22, No. 4, pp. 1-9, 2017.

- [14] Kim, C. S., "Digital Image Watermarking Technique Using Scrambled Binary Phase Computer Generated Hologram in Discrete Cosine Transform Domain," *Journal of Korea Multimedia Society*, Vol. 14, No. 3, pp. 403-413, 2010.
- [15] Poon, T. C., "Digital Holography and Three-Dimensional Display: Principles and Applications," Springer, 2006.



김철수 (Kim Cheol-Su)

- 정회원
 - 경북대 전자공학과 공학사
 - 경북대 전자공학과 공학석사
 - 경북대 전자공학과 공학박사
 - Univ of Connecticut 방문교수
- 경주대학교 전기에너지컴퓨터공학과 교수
- 관심분야 : 광신호처리, 3D 디스플레이, 광암호화, 워터마킹, 뇌-컴퓨터인터페이스 등