정보저장시스템학회논문집, 제 1 권 제 2 호, pp. 143~149

상보 데이터와 이진 진폭 마스크를 이용한 새로운 체적 홀로그램 암호화

A Novel Volume Hologram Encryption Using Complementary Data and Binary Amplitude Mask

김 현†, 김도형*, 이연호**
Hyun Kim, Do-Hyung Kim, and Yeon H. Lee

ABSTRACT

In this paper we propose a novel volume hologram encryption system with binary amplitude masks rather than phase masks, in which volume holograms can be securely recorded against the attacks by a third party. In our system, the encryption is done by multiplexing two volume holograms in such a way that an original binary data page is first stored as a volume hologram by interference with a binary amplitude mask and then the complementary data page is stored as another volume hologram by interference with the complementary binary amplitude mask over the first hologram. The operation principle of our system is explained with the well-known theory of recording and reading a volume hologram in a photorefractive material and the experimental results are presented. Experimental data show that our encryption system is protected from blind decryptions by randomly-generated incorrect amplitude masks.

Key Words : Volume Hologram, Encryption, Binary Amplitude Mask

기호설명

SLM: Spatial Light Modulator
CCD: Charge-Coupled Device

1. 서 론

최근 컴퓨터 기술의 발달과 스캐너, 복사기 등 광학 장비의 손쉬운 이용 때문에 신분증, 신용 카드, 지폐 등을 위조 혹은 불법 복제하는 일이 점차로 쉬워지고 있다. 이 때문에 2 차원 데이터의 보안 문제가 많은 관심을 끌게 되었고 이에 대한 산업계의 요구가 계속해서 증가하고 있다. 현재 신분증이나 카드 등에서 신원 확인을 위해 많이 쓰이고 있는 얼굴 사진 혹은 제품의 저작권 표시로 쓰이는 로고 등은 홀로그램(embossed hologram)을 부착함으로써 보호를 받는다. 그러나 이러한 홀로그램들은 스캐너, CCD(charge-coupled device) 카메라 등의 광학 입력 장치들을 이용하면 쉽게 읽힐 수가 있고 또한 복제가 가능해지므로 embossing hologram 기법은 보안에 취약하다고 할 수 있다. 이러한 이유로 지난 10 여년간 데이터 자체의 암호화뿐만 아니라 매질에 기록되는 데이터의 홀로그램을 암호화하기 위해서 다양한 광 암호화 기법들이 연구돼왔다[1-19].

광 암호화 기법들은 크게 두 가지로 분류할 수 있다. 첫째로, 원 데이터를 제 3 자가 알아볼 수 없는 노이즈 패턴 형태로 암호화시키는 기법이다. 2 차원 데이터를 stationary white noise 패턴으로 변경시켜 암호화를 수행하는 이중 랜덤 위상 인코딩 기법(double-random phase encoding technique)은 많은 연구가 진행돼왔다[1-3]. 위상 부호 암호화 기법(phase-encoded data encryption technique)에서는 원래의 2 차원 데이터(크기 정보)를 암호화를 수행하기에 앞서 먼저 위상 정보로 부호화하고 그런 다음 랜덤 위상 마스크들을 이용해 암호화시켰다[4-7]. 이진 데이터를 암호화시키기 위해 광 exclusive-OR 연산을 이용한 암호화 기법이 보고됐다[8]. 또한 광의

† 삼성전기 광 랩
E.Mail: harry5005.kim@samsung.com
* 성균관대학교 정보통신공학부
** 성균관대학교 정보통신공학부
논문접수일 (2005 년 4 월 6 일)

편광 성질을 이용해 데이터를 암호화시키는 기법이 보고됐다[9]. 이러한 기법에서 2 차원 데이터는 공간 광 변조기(spatial light modulator)를 통해 표시되었고 이러한 SLM 의 각 픽셀을 통과한 빛의 편광 상태가 랜덤 편광 마스크에 의해 랜덤한 편광 상태로 바뀌었다. 둘째로, 데이터 자체를 암호화하기 보다는 매질에 저장되는 데이터의 홀로그램을 암호화시키기 위한 여러 홀로그램 암호화 기법들이 제안됐다[10-17]. 이 경우 기준빔 경로 혹은 신호빔 경로에 랜덤 위상 마스크를 삽입함으로써 랜덤 위상 코드된 빔을 이용하여 기록되는 홀로그램들을 암호화시킬수 있었다.

기존 홀로그램 기록 시스템에서 기준빔 경로에 서로 다른 위상 마스크들을 삽입하여 홀로그램들을 기록하는 경우 기록 매질의 동일한 체적에 서로 다른 2 차원 데이터들을 독립적으로 기록 또는 암호화할 수 있었다. 하지만, 이 경우 랜덤 위상 마스크 대신에 랜덤 이진 진폭 마스크들이 사용되면 복원 데이터들간의 crosstalk 잡음들 때문에 서로 다른 데이터의 홀로그램들을 동일한 체적에 기록할 수 없게 된다. 다시 말해서 기준빔 경로에서 랜덤 진폭 마스크들을 사용하는 경우 기록된 홀로그램은 임의의 크기 패턴을 갖는 기준빔에 의해 읽힐 수 있으므로 이 경우 기록된 체적 홀로그램은 암호화되어 있다고 말할 수 없다.

본 논문에서 랜덤 이진 진폭 마스크(random binary amplitude mask)들과 상보 데이터 페이지(complementary data page)들을 이용한 새로운 체적 홀로그램 암호화 시스템을 제안한다[18]. 제안 시스템에서 기준빔 경로에 삽입된 랜덤 이진 진폭 마스크를 이용해 기록 매질의 동일한 체적에 두 홀로그램들(원 데이터의 홀로그램과 상보 데이터의 홀로그램)을 중첩해서 기록함으로써 암호화를 수행하게 된다. 먼저, 랜덤 이진 진폭 마스크를 통과한 기준빔이 원 데이터를 통과한 신호빔과 기록 매질에서 간섭함으로써 첫 번째 홀로그램이 기록된다. 다음으로, 원 진폭 마스크의 상보 진폭 마스크를 통과한 기준빔이 원 데이터의 상보 데이터를 통과한 신호빔과 기록 매질에서 간섭함으로써 두 번째 홀로그램이 첫 번째 홀로그램과 중첩 기록된다. 제안 시스템의 암호화 원리가 잘 알려진 체적 홀로그래피 이론을 바탕으로 설명된다. 그런 다음 제안 시스템의 실험 결과들이 제시된다. 기록시 사용된 마스크 패턴과 다른 마스크 패턴들을 사용해 홀로그램을 읽는 경우 복원된 데이터의 비트 에러율을 측정함으로써 제안 시스템의 성능을 평가한다

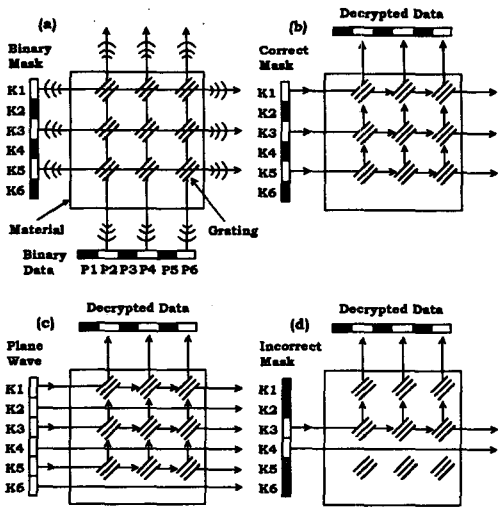

Fig. 1 Schematic diagram of holographic recording and reading in the conventional method. (a) Record of a binary data using a binary amplitude mask. Reads by the correct amplitude mask (b), plane wave (c), and randomly-generated amplitude mask (d). The original binary data is restored by any reference beam in the conventional method.

2. 암호화의 원리

2.1 기존 시스템에서 홀로그램 기록 및 판독

먼저, 기존 시스템에서 체적 홀로그램을 기록하고 읽는 과정이 잘 알려진 체적 홀로그래피 이론을 바탕으로 그림 1 의 구조도를 이용해 간단히 설명 되어진다. 그림 1(a)는 홀로그램을 기록하는 과정을 보여주며, 그림 1(b)-1(d)는 서로 다른 마스크를 사용해 기록된 홀로그램을 읽은 결과를 보여준다. 단순화를 위해 이진 데이터와 이진 진폭 마스크를 모두 일차원적으로 표시했다.그림 1(a)에서 대각선들은 M 개의 픽셀들로 구성된 신호빔 $\sum_{m=1}^{M} S_m(\vec{r})\exp[i\vec{k}_{sm}\cdot\vec{r}]$과 N개의 픽셀들로 구성된 기준빔 $\sum_{n=1}^{N} R_n(\vec{r})\exp[i\vec{k}_{rn}\cdot\vec{r}]$의 간섭에 의해 매질에 기록되는 체적 홀로그램 격자 $\Delta\varepsilon(\vec{r})$를 나타낸다.

$$\Delta\varepsilon(\vec{r}) = \beta\sum_{m=1}^{M} S_m(\vec{r})\exp[i\vec{k}_{sm}\cdot\vec{r}]\times\sum_{n=1}^{N} R_n^{*}(\vec{r})\exp[-i\vec{k}_{rn}\cdot\vec{r}], \quad (1)$$

여기서 β는 홀로그램 격자 세기와 관계되는 상수를, $\vec{r}=(x,y,z)$ 는 위치 벡터를 각각 나타내고, $\vec{k}_{sm}$, $\vec{k}_{rn}$ 는 각각 신호빔과 기준빔의 파동 벡터를 나타낸다. 이 경우 신호빔 경로에는 기록할 이진 데이터가 삽입되어지고 기준빔 경로에는 이진 진폭 마스크가 삽입되어진다. 그림 1 에서 체적 홀로그램 격자들이 공간적으로 분리돼 있지만 실제 실험(그림 3)에서는 빔들이 렌즈에 의해 매질로 포커스 되어지므로 격자들은 공간적으로 겹쳐질 것이다. 또한 이러한 기록된 체적 홀로그램 격자들은 interpixel crosstalks 가 없도록 Bragg selectivity 를 만족시키면서 각도적으로 분리된다고 가정한다.

그림 1(b)-1(d)는 기존 방법에서 홀로그램을 읽은 결과를 보여준다. 굴절률의 변조가 약하고 대역폭이 좁다고 가정하는 *Born* 근사화 영역에서 복원빔 $\sum_{n=1}^{N}P_n(\vec{r})\exp[i\vec{k}_{pn}\cdot\vec{r}]$ 에 의해 회절되는 빔 $D(\vec{r})$ 은 다음과 같이 표현되어진다[19].

$$D(\vec{r})=\beta\iiint_V\left\{\frac{\exp[ik_{pn}|\vec{r}-\vec{r}'|]}{|\vec{r}-\vec{r}'|}\sum_{m=1}^{M}S_m(\vec{r})\exp[i\vec{k}_{sm}\cdot\vec{r}]\times\sum_{n=1}^{N}R_n^*(\vec{r})\exp[-i\vec{k}_{rn}\cdot\vec{r}]\sum_{n=1}^{N}P_n(\vec{r})\exp[i\vec{k}_{pn}\cdot\vec{r}]\right\}d^3\vec{r}', \quad (2)$$

여기서 V 는 매질에서 체적 홀로그램 격자가 차지하는 부피를 나타낸다.

이 경우 기록할 때와 동일한 맞는 진폭 마스크(b), 평면파(c), 랜덤 발생된 틀린 마스크(d)가 각각 기준빔 경로에서 복원빔으로 쓰일 경우 기록된 이진 데이터의 홀로그램은 임의의 진폭 마스크를 가지고 읽힐 수 있음을 보여준다. 위의 식 (2)로부터 알 수 있듯이 기록시 기준빔 경로에서 쓰였던 마스크 정보 $\sum_{n=1}^{N}R(\vec{r})\exp[i\vec{k}_{rn}\cdot\vec{r}]$ 를 정확히 아는 경우 원래의 이진 데이터가 완전하게 복원되어진다. 또한 평면파 - 모든 픽셀들을 *ON* - 를 복원빔으로 사용하는 경우 이러한 마스크의 전체 픽셀 중 절반(*N*/2 개)이 원래 랜덤 이진 마스크의 *ON* 픽셀들과 일치할 것이고 이러한 *ON* 픽셀들을 통과한 빔들은 식 (2)에서 회절을 할 수 있게 된다. 따라서 원래의 이진 데이터가 완벽히 복원되어진다. 반면에 랜덤 발생된 틀린 마스크를 사용하는 경우에는 확률적으로 *ON* 픽셀들의 절반(*N*/4 개)이 기록시 사용된 마스크 패턴의 *ON* 픽셀들과 일치할 것이고 이러한 픽셀들을 통과한 빔들은 기록된 홀로그램으로부터 회절을 할 수 있게 되고 따라서 원래의 이진 데이터가 약하게 읽혀질 것이다.

2.2 제안 시스템에서 홀로그램 암호화 및 복호화

그림 2 는 새로이 제안된 체적 홀로그램 암호화 시스템에서 기록 및 복원을 설명하기 위한 구조도이다. 암호화할 원래 이진 데이터를 그림 1(a)에서처럼 이진 진폭 마스크를 통과한 기준빔과 간섭시켜 첫 번째 홀로그램(실선 대각선)으로 기록한 후, 상보 데이터 $\sum_{m=1}^{M}S_m^c(\vec{r})\exp[i\vec{k}_{sm}^c\cdot\vec{r}]$ (reversed data)를 그림 2(a)에서처럼 상보 마스크(reversed mask)를 통과한 기준빔 $\sum_{n=1}^{N}R_n^c(\vec{r})\exp[i\vec{k}_{rn}^c\cdot\vec{r}]$과 간섭시켜 두 번째 홀로그램(점선 대각선)으로 중첩 기록한다. 이 경우 기록된 체적 홀로그램 격자는 다음과 같이 표현할 수 있다.

$$\Delta\varepsilon(\vec{r})=\frac{\beta}{2}\sum_{m=1}^{M}S_m(\vec{r})\exp[i\vec{k}_{sm}\cdot\vec{r}]\times\sum_{n=1}^{N}R_n^*(\vec{r})\exp[-i\vec{k}_{rn}\cdot\vec{r}]+\frac{\beta}{2}\sum_{m=1}^{M}S_m^c(\vec{r})\exp[i\vec{k}_{sm}^c\cdot\vec{r}]\times\sum_{n=1}^{N}R_n^{c*}(\vec{r})\exp[-i\vec{k}_{rn}^c\cdot\vec{r}], \quad (3)$$

여기서 $S_m(\vec{r})+S_m^c(\vec{r})=1$ 이고 $R_n(\vec{r})+R_n^c(\vec{r})=1$ 이다.

위에서처럼 상보 관계의 두 이진 진폭 마스크를 이용해 중첩 기록한 홀로그램들을 복원빔 $\sum_{n=1}^{N}P_n(\vec{r})\exp[i\vec{k}_{pn}\cdot\vec{r}]$ 을 사용해 읽는 경우 *Born* 근사화 영역에서 회절되는 빔은 다음과 같이 표현되어질 것이다.

$$\begin{aligned}D(\vec{r})&=\iiint_V\left\{\frac{\exp[ik_{pn}|\vec{r}-\vec{r}'|]}{|\vec{r}-\vec{r}'|}\Delta\varepsilon(\vec{r})\times\sum_{n=1}^{N}P_n(\vec{r})\exp[i\vec{k}_{pn}\cdot\vec{r}]\right\}d^3\vec{r}'\\&=\frac{\beta}{2}\iiint_V\left\{\frac{\exp[ik_{pn}|\vec{r}-\vec{r}'|]}{|\vec{r}-\vec{r}'|}\sum_{m=1}^{M}S_m(\vec{r})\exp[i\vec{k}_{sm}\cdot\vec{r}]\times\sum_{n=1}^{N}R_n^*(\vec{r})\exp[-i\vec{k}_{rn}\cdot\vec{r}]\sum_{n=1}^{N}P_n(\vec{r})\exp[i\vec{k}_{pn}\cdot\vec{r}]\right\}d^3\vec{r}'\\&+\frac{\beta}{2}\iiint_V\left\{\frac{\exp[ik_{pn}|\vec{r}-\vec{r}'|]}{|\vec{r}-\vec{r}'|}\sum_{m=1}^{M}S_m^c(\vec{r})\exp[i\vec{k}_{sm}^c\cdot\vec{r}]\times\sum_{n=1}^{N}R_n^{c*}(\vec{r})\exp[-i\vec{k}_{rn}^c\cdot\vec{r}]\sum_{n=1}^{N}P_n(\vec{r})\exp[i\vec{k}_{pn}\cdot\vec{r}]\right\}d^3\vec{r}',\end{aligned} \quad (4)$$

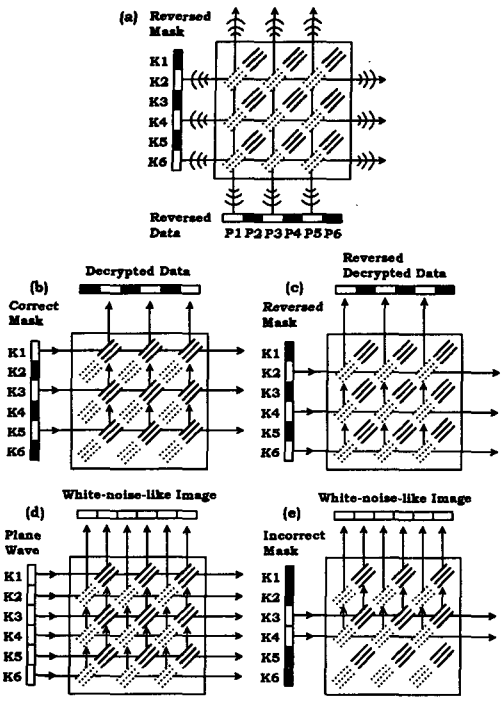

Fig. 2 Schematic diagram of our encryption system. (a) Solid lines, hologram of the original data; dotted lines, hologram of the reversed data. Reads by the correct amplitude mask (b) and the reversed mask (c). Plane wave (d) and randomly-generated incorrect mask (e) produce white-noise-like patterns.

여기서 첫 번째 항은 원래 이진 데이터의 홀로그램으로부터 회절되는 빔의 세기를, 두 번째 항은 상보 이진 데이터의 홀로그램으로부터 회절되는 빔의 세기를 각각 나타낸다

그림 2(b)-2(e)는 상보 관계의 두 마스크(이진 진폭 마스크와 이의 상보 마스크)를 사용해 중첩 기록한 홀로그램들을 읽은 결과를 보여준다. 기록시 사용한 마스크와 동일한 마스크(상보 마스크)를 사용해 중첩 기록된 홀로그램들을 읽는 경우 원래 데이터(상보 데이터)가 완전하게 복원되어진다는 것이 그림 2(b)(그림 2(c))에서 보여진다. 이것은 원래의 진폭 마스크를 사용해 중첩 기록된 홀로그램들을 읽으면 이러한 마스크를 사용해 기록된 첫 번째 홀로그램으로부터 단지 회절이 발생하고(식 (4)의 첫 번째 항) 상보 마스크를 사용해 읽으면 이번에는 단지 두 번째 홀로그램으로부터 회절이 발생하기 때문이다(식 (4)의 두 번째 항).

반면에 그림 2(d)-2(e)에서 보듯이 평면파 혹은 랜덤 발생된 틀린 마스크를 사용해 홀로그램들을 읽는 경우 단지 white-noise 같은 패턴이 출력에서 얻어진다. 이것은 평면파 혹은 틀린 마스크를 복원빔 $\sum_{n=1}^{N} P_n(\vec{r})\exp[i\vec{k}_{pn}\cdot\vec{r}]$ 으로 사용하는 경우 확률적으로 이러한 마스크의 패턴 $P_n(\vec{r})$ 중 절반이 기록시 사용된 원래의 이진 진폭 마스크 패턴 $R_n(\vec{r})$ 와 동일한 패턴이 되고 나머지 절반은 상보 마스크 패턴 $R_n^c(\vec{r})$ 와 동일한 패턴이 되기 때문이다. 다시 말해서 이러한 마스크들의 *ON* 픽셀들을 통과한 빔들 중 절반은 첫 번째 홀로그램으로부터 회절하고 나머지 절반은 두 번째 홀로그램으로부터 회절해서 전체적으로 white-noise 같은 패턴이 출력에서 얻어지게 된다.

3. 실험 결과

이진 진폭 마스크와 이의 상보 마스크를 이용한 새로이 제안된 체적 홀로그램 암호화 시스템은 그림 3 에서 보여진 실험 장치도에서 수행되어진다. 먼저, 파장 515nm 의 Ar 이온 레이저 빔이 확대되고 다음으로 확대된 레이저 빔이 각각 신호빔과 기준빔으로 나뉘어진다. 신호빔은 첫 번째 공간 광 변조기 SLM1 - 2 차원 이진 데이터 페이지를 표시한다 - 을 통과한 후 초점 길이 *260mm* 의 렌즈 L1 에 의해 $BaTiO_3$ crystal 로 포커스된다. 비슷하게, 기준빔은 SLM2 - 2 차원 이진 진폭 마스크를 통과한다 - 를 통과한 후 렌즈 L1 과 동일한 초점 길이의 렌즈 L2 에 의해 약하게 crystal 로 포커스된다. 이 경우 기준빔은 crystal 에서 신호빔과 보다 잘 간섭을 일으키도록 crystal 뒤쪽 2cm 에서 포커스된다. 렌즈 L3 와 L4 는 실험에서 복원되어지는 데이터를 모아서 CCD 로 보내주는 역할을 하며 CCD 에서 검출된 데이터는 frame grabber 에 의해 8 비트(256 그레이 스케일)의 디지털 정보로 변환되어진다.

실험에서 사용된 공간 광 변조기 SLM1 과 SLM2 는 동일한 진폭형 SLM 으로서 *18um×18um* 의 피치를 갖는 400×600 픽셀들로 이루어진다. 실험에서 신호빔 경로에 삽입된 SLM1 은 이진 데이터(이미지)로서 사용되어진 United States Air Force(USAF) resolution chart 를 표시했다. 기준빔 경로에 삽입된 SLM2 는 그림 3 에서 보듯이 체크무늬 패턴의 마스크를 표시하도록 40×60 셀들로 그룹화됐다. 실험에서 SLM 들에 의해 표시되어지는 이진 데이터 혹은 이진 마스크의 intensity contrast 는 125 라고 측정되어졌고 기준빔과 신호빔의 빔 세기들은 각각 20.4 mW/cm^2, 1.7 mW/cm^2

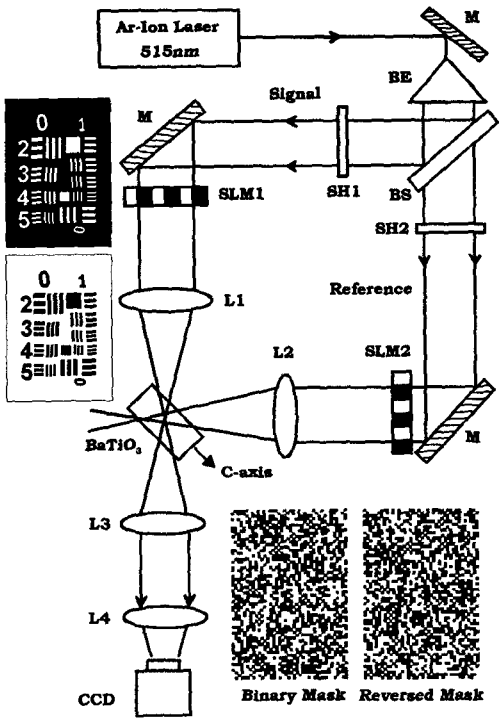

Fig. 3 Experimental setup. SLM's, Spatial Light Modulators; CCD, Charge-Coupled Device; BE, Beam expander; BS, Beam splitter; L's, Lenses; M's, Mirrors; SH's, Shutters.

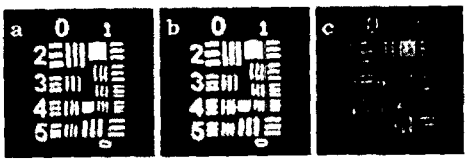

Fig. 4 Experimental results in the conventional method. Hologram read by the correct amplitude mask (a), plane wave (b), and randomly-generated incorrect mask (c).

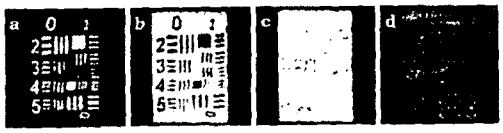

Fig. 5 Experimental results in our system. Hologram read by the correct amplitude mask (a), the reversed mask (b), plane wave (c), and randomly-generated incorrect mask (d).

라고 측정되어졌다.

또한 7.0 초의 홀로그램 격자 기록 시간내에서 Bragg 회절빔들의 세기를 동일하게 만들기 위해 첫 번째와 두 번째 홀로그램을 각각 4.5 초, 2.5 초씩 기록했다. 그림 4 는 USAF resolution chart 의 홀로그램을 단지 랜덤 이진 진폭 마스크만를 사용해 기록하는 기존 방법에서 홀로그램을 읽은 결과를 보여준다. 기존 방법으로 기록된 홀로그램은 임의의 기준빔 (맞는 진폭 마스크, 평면파, 랜덤 발생된 틀린 진폭 마스크)에 의해 읽혀진다는 것이 그림 4(a)-4(c)에서 보여진다. 이 경우 맞는 마스크 혹은 평면파를 가지고 홀로그램을 읽으면 원래 이진 데이터가 완전하게 복원되어졌고 설령 마스크 정보를 전혀 모르는 사람이 틀린 마스크를 사용해 홀로그램을 읽더라도 원래 이진 데이터가 약하게 복원되어질 수 있었다.

그림 5 는 새로이 제안된 시스템에서 수행되어진 체적 홀로그램 암호화 및 복호화의 실험 결과들을 보여준다. 먼저, USAF chart 가 랜덤 이진 진폭 마스크를 사용해 crystal 에 첫 번째 홀로그램으로 기록됐고 다음으로 상보 USAF chart 가 상보 이진 마스크를 사용해 첫 번째 홀로그램 위에 중첩 기록됐다. 맞는 마스크(상보 마스크)를 사용해 중첩 기록된 홀로그램들을 읽는 경우 원래 USAF chart(상보 USAF chart)가 복원되어진다는 것이 그림 5(a)(그림 5(b))에서 보여진다. 그러나 이 경우 평면파 혹은 랜덤 발생된 틀린 마스크를 사용해 기록된 홀로그램을 읽으면 단지 white-noise 패턴이 출력에서 나타난다는 것이 그림 5(c)-5(d)에서 보여진다. 이러한 실험 결과들은 새로이 제안된 암호화 기법으로 홀로그램을 기록하면 기록된 홀로그램이 안전하게 암호화되어진다는 것을 보여주며 또한 단지 맞는 마스크 혹은 상보 마스크를 사용하는 경우에만 홀로그램을 제대로 읽을 수 있음을 보여준다. 그림 5(a)-5(d)의 데이터에서 측정된 raw 비트 에러율은 각각 8.3×10^{-3}, 9.7×10^{-3}, 6.1×10^{-1}, 2.9×10^{-1} 였다. 여기서 비트 에러율은 CCD 에 의해 캡쳐된 원래 데이터와 비교해 동일한 CCD 에 의해 캡쳐된 70×100 픽셀의 복원 데이터 중 에러난 픽셀들의 개수로서 정의되어진다.

다음으로, 맞는 진폭 마스크의 일부분만을 사용하여 복호화를 시도함으로써 제안 시스템의 성능을 조사했다. 그림 6(a)는 맞는 마스크 정보 중 일부분만 - 100%, 85%, 25%, 2% - 을 사용해 홀로그램을 읽는 경우 복원되어지는 데이터에서 수평선 (그림 6(b)에서 화살표에 의해 보여진다.) 상의 CCD 픽셀들의 그레이 스케일 값을 보여준다. 이 경우 2% 미만의 맞는 마스크 정보(우리의 실험

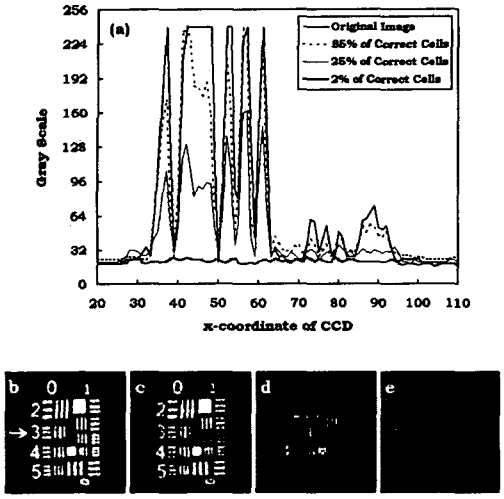

Fig. 6 (a) Horizontal scans of the images restored by partial use of the correct amplitude mask: (b) 100%, (c) 85%, (d) 25%, (e) 2%.

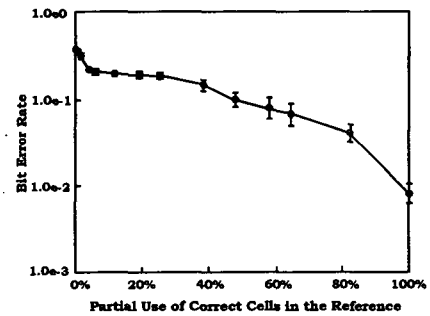

Fig. 7 Measured bit error rates of the images restored by partial use of the correct amplitude mask.

조건에서 전체 2400 개의 셀들 중 48 개의 셀)만을 사용해 홀로그램을 읽으면 복원되어지는 데이터는 알아볼 수 없었다. 기록시 사용된 마스크 정보를 모르는 누군가가 시행 착오(trial and error) 기법으로 2%의 맞는 진폭 마스크 정보를 알아내려고 시도한다면 이는 $(1/2)^{48} \approx 3.6\times10^{-15}$ 의 복호화 확률에 대응할 것이다.

그림 7 은 그림 6 에서 보여진 것처럼 맞는 마스크 정보 중 일부분만을 사용해 홀로그램을 읽는 경우 복원되어지는 데이터의 비트 에러율을 나타낸다.다음으로, 제안 시스템에서 전체 2400 개의 셀들로 구성된 이진 진폭 마스크에서 틀린 셀들의 비율을 늘리면서 홀로그램을 읽는 경우 복호화 결과를 조사했다.

마스크에서 서로 다른 틀린 셀들의 비율 (0%, 15%, 30%, 50%) 을 사용해 복호화를 시도할 때 복

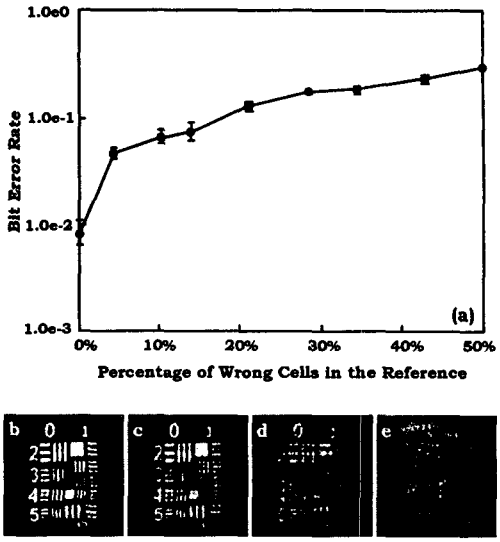

Fig. 8 (a) Measured bit error rates of the images restored for different ratios of wrong cells in the mask: (b) 0%, (c) 15%, (d) 30%, (e) 50%.

원되어지는 데이터는 그림 8(b)-8(d)에서 보여지며 이 때 측정된 비트 에러율은 그림 8(a)에서 보여진다. 이 경우 틀린 셀들 (reversed 패턴에 해당)의 비율이 증가할수록 복원 데이터는 점점 white-noise 패턴에 가까워지며 따라서 측정되어지는 비트 에러율이 증가함을 볼 수 있다.

4. 결 론

본 논문에서 상보 데이터와 상보 이진 진폭 마스크를 이용한 새로운 체적 홀로그램 암호화 시스템을 제안했다. 제안 암호화 시스템에서 기록된 체적 홀로그램은 평면파 혹은 랜덤 발생된 진폭 마스크를 사용해 복원을 시도하는 blind decryption 로부터 안전하게 보호되어진다는 것이 실험적으로 보여졌다. 또한 맞는 마스크 정보 중 제한된 일부분만을 사용해 홀로그램을 읽거나 혹은 전체 마스크에서 틀린 셀들의 비율을 늘리면서 홀로그램을 읽는 경우 복원되어지는 데이터의 비트 에러율이 측정되어졌다. 전체 2400 개의 셀들로 구성된 이진 진폭 마스크를 이용한 본 실험에서 맞는 마스크 정보 중 2%미만의 영역만을 단지 이용하거나 전체 마스크 중 틀린 셀들의 비율이 30%를 넘어서면 복원 되어진 데이터는 알아 볼 수가 없거나 질이 크게 떨어졌다. 새로이 제안된 시스템은 위상 마스크보다 제작이 훨씬 용이하고 휴대가 간편한 이진 진폭 마스크를 사용하므로 제안 시스템은

위상 마스크를 이용한 시스템들에 비해 실제 수행 시 장점이 있을 수 있다.

후 기

This work was supported by the Advanced Materials and Process Research Center at Sungkyunkwan University (grant R12-2002-057-02002-0).

참고문헌

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

[2] G. Unnikrishnan, J. Joseph, and K. Singh, 1998, "Optical encryption system that uses phase conjugation in a photorefractive crystal ," Appl. Opt. Vol .37, No.35, pp.8181-8186.

[3] T. Nomura, S. Mikan, Y. Morimoto, and B. Javidi, 2003, "Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator ," Appl. Opt. Vol.42, No.8, pp.1508-1514.

[4] L. G. Neto and Y. Sheng, 1996, "Optical implementation of image encryption using random phase encoding ," Opt. Eng. Vol.35, No.9, pp.2459-2463.

[5] L. G. Neto, 1998, "Implementation of Image Encryption using the Phase-Contrast Technique," Proc. SPIE 3386 pp.284-290.

[6] P. C. Mogensen and J. Gluckstad, 2000, "Phase-only optical encryption ," Opt. Lett. Vol.25, No.8, pp.566-568.

[7] X. Tan, O. Matoba, T. Shimura, K. Kuroda, and B. Javidi, 2000, "Secure optical storage that uses fully phase encryption ," Appl. Opt. Vol.39, No.35, pp.6689-6694.

[8] S. Fukushima, T. Kurokawa, and Y. Sakai, 1991, "Image Encipherment Based on Optical Parallel Processing Using Spatial Light Modulators," IEEE Photon. Tech. Lett. Vol.3, No.12, pp.1133-1135.

[9] X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, 2001, "Secure optical memory system with polarization encryption," Appl. Opt. Vol.40, No.14, pp.2310-2315.

[10] E. Tajahuerce and B. Javidi, 2000, "Encrypting three-dimensional information with digital holography," Appl. Opt. Vol.39, No.35, pp.6595-6601.

[11] T. F. Krile, M. O. Hagler, W. D. Redus, and J. F. Walkup, 1979, "Multiplex holography with chirp-modulated binary phase-coded reference-beam masks," Appl. Opt. Vol.18, No.1, pp.52-56.

[12] J. E. Ford, Y. Fainman, and S. H. Lee, 1990, "Array interconnection by phase-coded optical correlation," Opt. Lett. Vol.15, No.19, pp.1088-1090.

[13] C. Denz, G. Pauliat, G. Roosen, and T. Tschudi, 1991, "Volume hologram multiplexing using a deterministic phase encoding method," Opt. Commun. Vol.85, No. 2, pp.171-176.

[14] H. Lee and S. K. Jin, 1993, "Experimental study of volume holographic interconnects using random patterns," Appl. Phys. Lett. Vol.62, No.18, pp.2191-2193.

[15] J. F. Heanue, M. C. Bashaw, and L. Hesselink, 1995, "Encrypted holographic data storage based on orthogonal-phase-code multiplexing," Appl. Opt. Vol.34, No.26, pp.6012-6015.

[16] S. Lai, 1996, "Security holograms using an encoded reference wave," Opt. Eng. Vol.35, No.9, pp.2470-2472.

[17] B. Wang, J.-Y. Chang, W.-C. Su, and C.-C. Sun, 2004, "Optical security using a random binary phase code in volume holograms," Opt. Eng. Vol.43, No.9 pp.2048-2052.

[18] Hyun Kim, 2004, Storage and Encryption of Multiple Volume Holograms, PhD Thesis, Sungkyunkwan University, pp.68-107.

[19] H. J. Coufal, D. Psaltis, and G. T. Sincerbox, 2000, Holographic Data Storage, Springer-Verlag, pp.30-35.