ISSN: 1226-7244 (Print)
ISSN: 2288-243X (Online)
논문번호 14-03-05

j.inst.Korean.electr.electron.eng.Vol.18,No.3,328~334,September 2014
http://dx.doi.org/10.7471/ikeee.2014.18.3.328

OFB 블록 암호화 알고리즘의 광학적 시스템 구현

Optical System Implementation of OFB Block Encryption Algorithm

길 상 근*★

Sang-Keun Gil*★

Abstract

This paper proposes an optical encryption and decryption system for OFB(Output Feedback Block) encryption algorithm. The proposed scheme uses a dual-encoding technique in order to implement optical XOR logic operation. Also, the proposed method provides more enhanced security strength than the conventional electronic OFB method due to the huge security key with 2-dimensional array. Finally, computer simulation results of encryption and decryption are shown to verify the proposed method, and hence the proposed method makes it possible to implement more effective and stronger optical block encryption system with high-speed performance and the benefits of parallelism.

요 약

본 논문은 OFB(Output Feedback Block) 블록 암호화 알고리즘에 대한 광학적 암호화 및 복호화 시스템을 제안한다. 제안한 방식은 암호화 과정에 필요한 XOR 논리 연산을 구현하기 위해 이중 인코딩 기법을 사용한다. 또한, 제안된 암호화 시스템은 광 병렬처리의 특성상 데이터가 2차원으로 배열되어 매우 큰 암호키를 구현할 수 있기 때문에 기존의 전자적 OFB 방식보다 한층 더 암호강도가 증강된 암호화 시스템을 제공한다. 마지막으로, 제안한 방식을 검증하기 위해 컴퓨터 시뮬레이션을 통하여 암호화 및 복호화 과정을 보여준다. 그 결과, 제안한 광학적 OFB 암호화 시스템은 광학적인 고속성과 병렬성의 이점까지 포함하기 때문에 더욱 효율적이고 강력한 광학적 블록 암호화 시스템이 가능하다.

Key words : Optical encryption, OFB encryption, optical XOR logic operation, Dual-rail encoding, security system

Ⅰ. 서론

사람들은 요즘 시대를 흔히들 21세기 정보화 시대에 살고 있다고 말들을 한다. 사회 전반적인 혁신으로 휴대폰 혹은 집에서 PC로 각종 은행업무, 직장에서의 사무, 학교에서의 숙제, 온라인 행정처리 등등 정치, 경제, 산업, 인간관계까지 정보처리 및 관리가 가능해졌다. 이와 같이 우리 생활 속 깊숙이 자리 잡은 디지털 정보들은 목적에 따라 생산, 교환되어 유용한 정보로써 생활 곳곳에서 사용하고 있으며, 정보가 곧 중요한 자원중의 하나로써 의미를 가지게 되었다. 하지만 신문, 방송 등 각종 언론매체에서 개인의 중요한 신상정보들이 아주 손쉽게 내부적인 요인에 의해 유출되거나 혹은 외부적 해킹으로 정보를 가로채거나 악의적으로 파괴되는 일이 적지 않게 방송에서 보도되고 있는 상황이다. 따라서 최근에는 개인 정보의 유

* Dept. of Electronics Engineering, The University of Suwon
skgil@suwon.ac.kr TEL: 031-220-2598
★ Corresponding author : skgil@suwon.ac.kr
※ Acknowledgment
Manuscript received Jul, 23, 2014; revised Sep, 3, 2014 ; accepted Sep, 3. 2014

출과 정보의 도용 등의 심각한 문제로 인한 사생활의 침해뿐만 아니라 정보의 불법 유출 및 수정으로 막대한 경제적인 손실을 당하지 않기 위하여 네트워크상에서 정보의 안정성에 대해 중요하게 인식하게 되었다. 하지만 지금과 같은 현실 속에서 기존의 디지털 암호화 기술은 컴퓨터 장비들의 향상으로 인해 다가오는 미래에서는 정보들을 보호할 수가 없게 되어 버릴 것이다. 또한 머지않아 정보의 용량뿐만 아니라 처리 속도 면에서도 그 한계를 드러낼 것이다. 이와 같은 문제를 해결하기 위해 1990년대 초부터 광학적 기술을 적용한 암호화, 복호화 보안 장치가 지속적으로 연구되어 왔다[1-8]. 이는 기존의 사용하였던 디지털적인 알고리즘을 대신하여 암호화 시스템을 광학적으로 구현하면 전자적 디지털 보안 기법에 비하여 정보의 크기, 처리 속도가 월등한 능력을 가지는 장점을 가지고 있기 때문에 기존의 디지털 보안 기법의 대안으로서 좀 더 복잡하고 빠른 광학적 암호화 기법들을 수행할 수 있다[9]. 이 중 대부분의 방법들은 홀로그래피 특성을 이용한 주파수 영역의 복소 함수를 다룸으로써 광학 시스템의 광축 정렬 문제나 외부 교란에 의한 시스템 성능 저하 등 민감한 단점을 지니고 있다. 또한 현재 연구되어 오는 대부분의 광학적 암호화 기법은 복소 함수 형태의 암호문을 생성하기 때문에 디지털 통신망을 이용해 암호문을 전달시키기 위해서는 디지털 데이터 변환 과정과 그 처리 시간이 요구된다. 이를 해결하기 위해서 디지털 처리 방식인 XOR 연산을 이용한 광 암호화 기법이 제안되었으며, 대표적인 방법으로는 광학적으로 빛의 편광 성분을 이용하여 XOR 연산을 하는 방법[10]과 이중 인코딩(dual-rail encoding) 기법을 사용하여 자유공간 광 연결 논리 XOR 연산을 기반으로 하는 암호화 방법[11]이 있다. 특징적으로 광학적으로 XOR 연산은 디지털 신호와도 잘 연동이 되어 광학적인 시스템 구현에도 간단하다는 장점을 가진다.

본 논문에서는 블록 암호화 기법의 대표적인 OFB(Output Feedback Block) 기법을 광학적인 XOR 연산을 이용하여 광 암호화 및 복호화를 수행하는 암호화 시스템을 제안하였다. 제안한 시스템의 성능을 확인하기 위해서 암호화 하고자 하는 원래의 256 gray level 영상을 디지털 정보 1 또는 0으로 이진화하여 암호화할 입력 데이터로 변환한 다음, 이중 인코딩 방식과 자유 공간 광 연결에 기반한 XOR 연산을 이용하여 암호화 및 복호화 시뮬레이션을 수행하였다.

II. 광학적 이중 인코딩 XOR 연산

이중 인코딩 방법은 이진 정보를 진수와 보수(complement)로 동시에 표현한 뒤 이들을 거울과 BS(Beam Splitter)를 이용하여 XOR 연산을 구현하는 방법이다[11]. XOR 연산을 풀어서 살펴보면 입력에 대한 진수 및 보수 표현과 AND 연산과 OR 연산의 세 개의 과정이 필요하다. 이 과정을 광학적으로 구현을 해보면 그림 1과 같다.

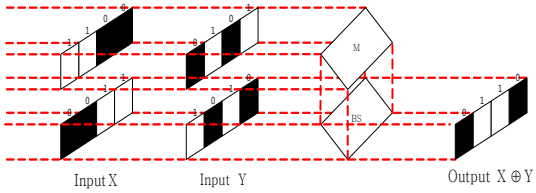


Fig. 1. Optical XOR operation using dual-rail encoding method

그림 1. Dual-rail encoding 기법을 이용한 광학적 XOR 연산

먼저 입력으로써 직렬과 병렬로 배치된 SLM(Spatial Light Modulator)에 진수 데이터와 보수 데이터를 표현한다. 여기서 논리 1은 빛이 통과되는 화소를 나타내고 논리 0은 빛이 통과하지 않는 화소를 나타낸다. 이러면 그림 1에서 보듯이 위와 아래에 위치한 두 쌍의 두 개의 직렬로 배열된 SLM들에 빛이 통과되면 각각 AND 연산이 수행되고, 이 통과된 두 개의 빛을 거울과 BS를 통하여 OR 연산을 수행하여 XOR 연산이 얻어진다. 간단히 XOR 연산을 수식적으로 살펴보면 다음과 같다.

$$X \oplus Y = X\overline{Y} + \overline{X}Y \tag{2.1}$$

앞에서 말한 연산 과정을 주어진 입력들에 대해서 이중 인코딩 방법은 1 개의 이진 정보에 대해 진수와 보수로 구성된 2 개의 화소를 한 쌍으로 인코딩하는 방식이다. 연산하고자 하는 두 개의 이진 데이터는 광학적으로 공간상에 이중 인코딩되어 다음과 같이 표현할 수 있다.

$$a(x,y) = \overline{X}(x,y) + Y(x-a,y-b) \tag{2.2}$$

$$b(x,y) = Y(x,y) + \overline{Y}(x-a,y-b) \tag{2.3}$$

(2.2)식과 (2.3)식을 AND 연산과 OR 연산을 수행하면

$$c(x,y)=a(x,y)\bullet b(x,y)=\overline{X}\bullet Y+Y\bullet \overline{X}=X\oplus Y \quad (2.4)$$

이 되며, 결과는 XOR 연산의 논리식과 같다. 여기서 •은 AND 연산을 +는 OR 연산을 나타내며, ⊕는 XOR 연산을 표시한다.

III 제안한 OFB 암호화의 광학적 시스템

그림 2는 OFB 암호화 알고리즘의 블록도이다. 암호화키를 초기에 어떤 임의의 값과 연산한 뒤에 다음 평문과 XOR 연산을 하여 암호문을 얻고 똑같은 암호화 과정으로 복호화 하는 시스템이다. 이 방식은 블록 암호화 방식중의 CBC(Cipher Block Chaining)모드, CFB(Cipher feedback)모드, ECB(Electronic CodeBook)모드의 단점을 보안한 방식으로 평문의 패턴이 보이지 않고 오류가 발생했을 때 전체 암호문 블록에게 영향을 미치지 않은 블록 암호화 알고리즘으로 초기 설정은 다음과 같다.

$$I_0=IV \quad (3.1)$$

$$O_i=E_k(I_{i-1}),\qquad 2\le i\le m \quad (3.2)$$

여기서 $I_0=IV$는 초기값(initial value)을 나타내고 E_k는 암호화키에 의한 암호화 과정을 나타낸다. i-번째 평문 P_i에 대해서 OFB의 암호화 방식은 다음과 같다.

$$C_i=P_i\oplus O_i,\qquad 1\le i\le m \quad (3.3)$$

여기서 ⊕는 XOR 연산을 말한다. 복호화 수식은 다음과 같다.

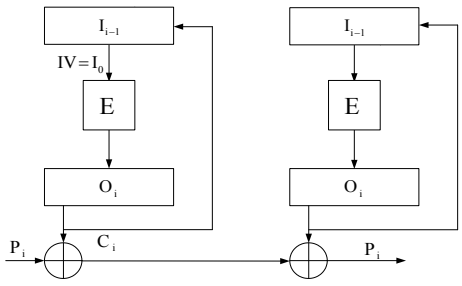


Fig. 2. Block diagram of OFB encryption algorithm
그림 2. OFB 암호화 알고리즘의 블록도

$$R_i=C_i\oplus O_i=P_i,\qquad 1\le i\le m \quad (3.4)$$

CBC, CFB 방식의 오류 전파의 해결책으로 나오게 된 OFB 알고리즘은 위성통신 암호화에 쓰이며 오류 전파가 전체 암호화 시스템에 미치지 않는 반면에 별도의 동기화 기법을 사용해야 한다. CFB 방식과 비교해 보았을 때 초기의 임의의 값과 암호화키를 연산하여 평문과 XOR 연산을 한 값을 넘겨주는 것이 아니라 초기값과 암호화키의 연산값만 넘겨주어 각각의 독립적인 암호화를 할 수 있게 되는 것을 볼 수가 있다. 따라서 오류의 전파가 발생하지 않는다. 다만 독립적인 암호화 방법을 사용하여 동기화를 시켜줄 필요가 있는 방법으로 비트 송신이나 삽입 등을 생각해야 한다. 본 논문에서는 이러한 OFB 방식을 이중 인코딩 XOR 연산을 통해서 간단하게 바꾼 광학적 OFB 암호화 시스템을 제안한다. 제안한 방식은 그림 2에서 표현된 암호화키에 의한 암호화 과정 E_k를 XOR 연산으로 치환하여 암호화를 수행하는 방식이다. 이를 수식적으로 바꾸면 다음과 같이 간단하게 표현할 수 있다.

$$C_i=P_i\oplus O_i,(O_i=E_k(I_{i-1})) \quad (3.5)$$
$$\rightarrow\ C_i=P_i\oplus O_i=P_i\oplus(I_{i-1}\oplus K)$$

$$R_i=C_i\oplus O_i,(O_i=E_k(I_{i-1})) \quad (3.6)$$
$$\rightarrow\ R_i=C_i\oplus O_i=C_i\oplus(I_{i-1}\oplus K)$$

여기서 K는 블록 암호화에 사용되는 암호화키를 나타낸다. 마찬가지로 $I_0=IV$는 초기값이다. 제안한 방식을 광학적인 시스템으로 구현하기 위해서 XOR 연산을 그림 2의 기존 OFB 암호화 알고리즘에 적용해 보면 수정된 XOR 연산 기반의 OFB 알고리즘의 블

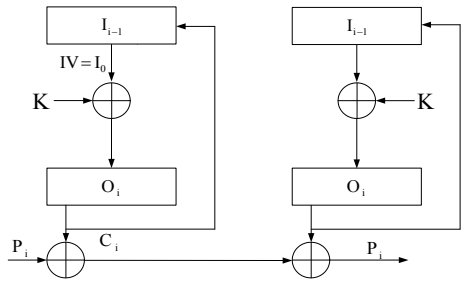


Fig. 3. Block Diagram of the proposed OFB encryption using XOR operation
그림 3. XOR 연산을 이용한 제안된 OFB 암호화 방식의 블록도

록 다이어그램은 그림 3과 같이 표현된다.

따라서, (3.5)식과 (3.6)식으로 표현된 제안한 OFB 알고리즘은 앞에서 설명한 이중 인코딩 기법을 이중의 XOR 연산이 수행된 수정 OFB 방식에 적용하여 광학적인 시스템으로도 구현이 가능하다. 그림 4는

본 논문에서 제안한 이중 인코딩 XOR 기법을 이용한 수정된 OFB 암호화 알고리즘의 암호화와 복호화 과정을 광학적으로 수행할 수 있는 개념적 구성도를 보여준다. 그림 4(a)의 암호화 시스템의 광학적 처리과

정은 다음과 같다. 먼저 SLM1s에 초기값을 정해 진수, 진수, 보수, 보수 순서로 입력하고 SLM2s에 암호화키를 진수, 보수, 보수, 진수 순서로 입력한다. SLM3s에 암호화할 영상을 진수와 보수로 순서적으로 입력한 뒤 광학적인 이중 인코딩 XOR 연산을 하면 암호화된 영상을 CCD2에서 얻는다. 이때 다음 암호화를 위해서 궤환될 암호 영상 정보는 CCD1에서 얻어진다. 한편, 암호문의 광학적 복호화 처리 과정은 그림 4(b)의 시스템과 같다. 복호화 과정은 암호화에 사용되었던 똑같은 광학 시스템을 이용하여 얻을 수 있다. SLM1과 SLM2에 암호화 과정에서 입력했던 초기값과 암호화키를 마찬가지로 진수와 보수 표현으로 입력하고 SLM3에 암호화된 영상을 진수와 보수로 입력하면 원래의 영상이 복호화 되어 CCD2에서 얻어진다. 이때 CCD1에 기록되는 궤환값은 다시 SLM1s에 진수와 보수로 입력되고, CCD2의 복호화된 영상은 다시SLM3s에 전달되어 계속해서 다음의 영상을 복원한다. 또한, 그림 4의 제안된 광학 시스템은 간략화 된 광학적 모듈 구조로 구현하여 제작할 수 있다.

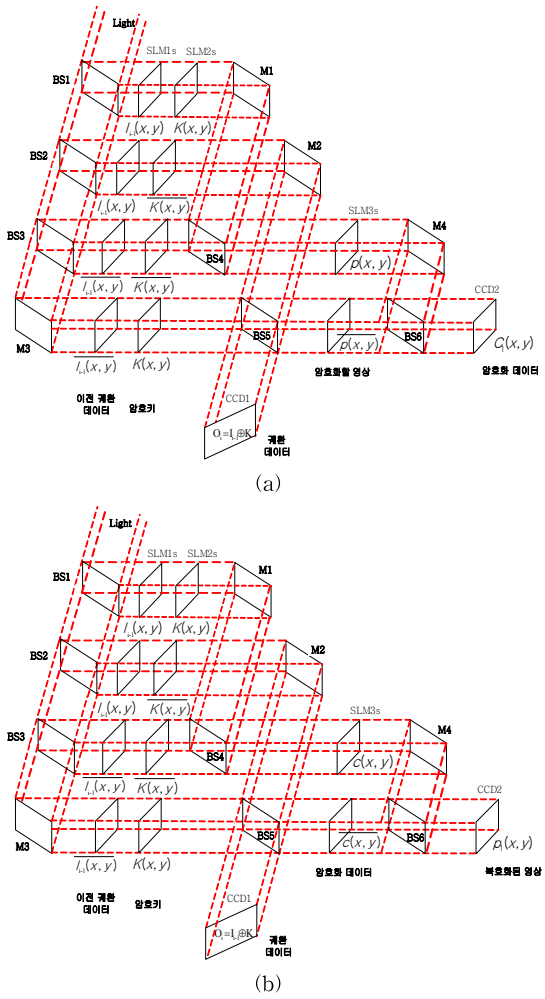


Fig. 4. Optical system of the proposed OFB encryption using dual-rail encoding XOR operations; (a) encryption system, (b) decryption system

그림. 4. 이중 인코딩 XOR 연산 방식을 이용한 제안된 OFB 알고리즘의 광학적 시스템; (a) 암호화 시스템, (b) 복호화 시스템

그림 5는 본 논문에서 제안한 그림 4의 OFB 암호화 시스템을 실제적으로 제작 가능한 암호화 모듈로설계된 광학 시스템을 보여준다. 그림 5에서 SLM은 그림 4에 비해 통합되어 3 개로 줄었고 BS도 간략화된 구조를 보여준다. 제안된 광 모듈에서 SLM의 직렬 배치는 각 SLM에 표현되는 입력 변수의 AND 연산을 수행하고 두 개의 BS는 OR 연산을 수행하게 된

다. 여기서 pixel matching aperture는 각 입력 변수의 진수와 보수를 표시하는 SLM에 표현되는 화소들의 정합과 회절 전파의 차단을 위해 사용된다. 또한 imaging lens는 SLM의 화소 크기와 CCD의 화소 크기의 다름을 정합시키기 위해 사용되었다. 이 광 모듈도 역시 그림 4(b)와 같이 SLM에 표시되는 입력 변수의 변환을 통해 복호화 과정을 수행하여 원래의 정보를 복원하는데 사용될 수 있다.

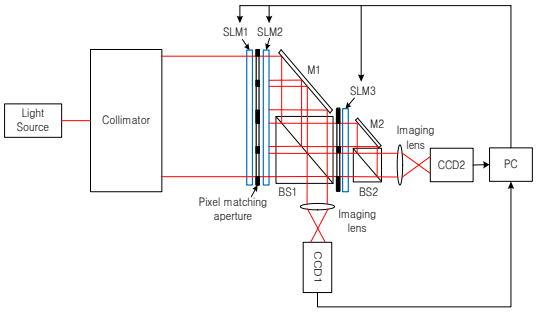


Fig. 5. Optical module implementation for the proposed OFB encryption system
그림. 5. 제안된 OFB 암호화 시스템의 광학적 모듈 구현

Ⅳ 시뮬레이션

본 논문에서 제안한 광학적 OFB 암호화 시스템의 성능을 검증하기 위해 전산 실험을 하였다. 제안한 시스템에 사용되는 입력은 이진 데이터이어야 하므로, 우선 암호화 하고자 하는 영상인 256 gray-level의 Lena(128×128) 영상을 그림 6과 같이 gray-level 값을 갖는 영상의 각 픽셀별로 ASCII 코딩을 통해 8-Bits 이진 값으로 변환하고, 이를 (4×2)의 블록 행렬로 표현하여 이진영상(512×256 화소)을 얻는다[11]. 그림 6은 이러한 ASCII 코딩과 블록 매핑 방법에 의한 이진 데이터 변환 과정을 보여준다.

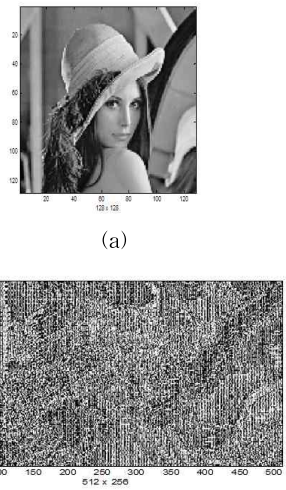


Fig. 7. Original image and the converted plain text data to be encrypted; (a) Lena image (b) converted binary plain text data
그림. 7. 암호화에 사용될 원 영상과 변환된 평문 데이터; (a) Lena 영상, (b) 변환된 이진 평문 데이타

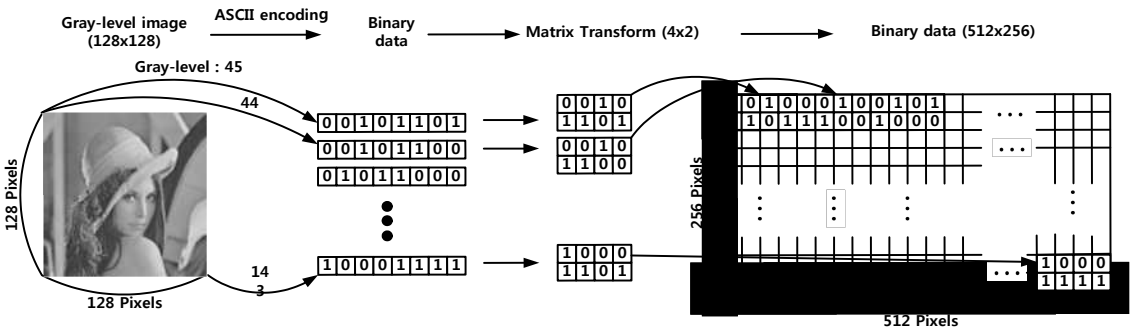
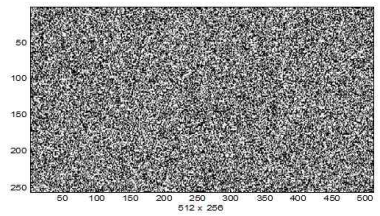


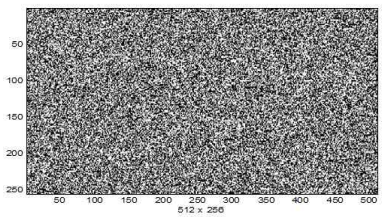
Fig. 6. A process for converting a 256 gray-level image into binary data
그림 6. gray-level 영상을 이진영상으로 변환하는 과정

본 논문에서는 그림 7(a)와 같이 암호화 목표 영상을 256 gray-level Lena 영상으로 하였고, (b)는 Lena 영상을 이진 데이타로 변환시킨 평문 데이터를 보여준다.

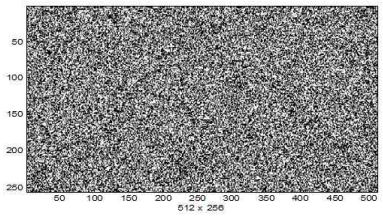
암호화 과정에서, 그림 8(a)는 제안한 OFB 암호화의 첫 번째 과정에서 사용된 초기값 영상(편의상 임의로 생성된 무작위 이진 코드를 사용함)을 보여주며, (b)는 암호화에 사용된 무작위로 생성된 암호화키를 보여주고, (c)는 그림 7(b)의 암호화 목표 영상이 이러한 초기값과 암호화키에 의해 암호화 된 첫 번째 영상을 보여준다.



(a)



(b)



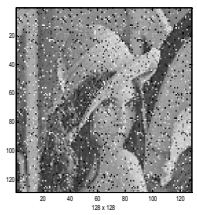
(c)

Fig. 8. Encryption process; (a) initial value image, (b) encryption key, (c) encrypted image

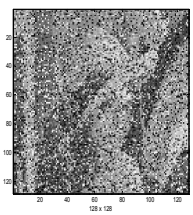
그림. 8. 암호화 과정; (a) 초기값 영상, (b) 암호화키, (c) 암호화된 영상

복호화 과정에서는, 그림 9(a)는 암호화 과정에서 사용된 똑같은 암호화키를 사용해 복호화 된 데이터를 ASCII 디코딩을 통하여 재생한 복원 영상이고, (b)~(d)는 암호화 과정에서 사용되지 않은 다른 키(암호화키와 틀린 키)에 의해 복호화 된 데이타를 ASCII 디코딩을 통하여 재생한 영상을 보여준다. 여기서 그림 9(b)부터 (d)는 복호화에 사용된 거짓 키가 원래의 올바른 키와 비교하여 각각 10%, 40%, 70%의 화소 오차가 있는 키를 사용하여 복원한 영상을 보여준다. 그림에서 알 수 있듯이 올바른 암호화키에 의해 복호화 된 영상은 원래의 Lena 영상이 완벽하게 복원됨을 알 수 있고, 틀린 키를 사용하였을 때는 키의 오차 정도에 따라 원래 영상이 잘 복원되지 않음을 보여준다.

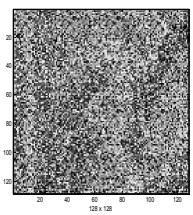
(a)



(b)



(c)



(d)

Fig. 9. Reconstructed image by decryption process; (a) original Lena image by the correct encryption key, (b)~(d) incorrectly decrypted image by the incorrect encryption key with 10%, 40%, and 70% error bits, respectively

그림. 9. 복호화 과정을 통한 재생된 영상; (a) 올바른 암호화키로 복호화 된 원 Lena 영상, (b)~(d) 올바른 키에 대하여 각각 10%, 40%, 70%의 화소 오차를 갖는 틀린 키로 복호화 된 영상

III 결론

본 논문에서는 기존의 블록 암호화의 대표적인 방법 중의 하나인 OFB 알고리즘을 광학적으로 구현 가능한 암호화 및 복호화 시스템을 제안하였다. 블록 암호화 방식 중에서도 OFB 방식은 기존의 CBC, CFB 방식이 가지고 있던 오류 전파 또는 오류의 영향을 받지 않는 장점을 가지고 있다. 또한 기존의 대

칭키 암호화 방식에서의 암호화할 영상과 암호화된 영상을 만약에 동시에 도난당한다면 암호화키를 알아낼 수 있기 때문에 암호화 시스템 전체가 무력화되는 문제점을 가지지만 OFB 방식은 암호화할 영상과 암호화된 영상으로 암호화키를 알아 낼 수가 없다는 장점을 가진다. 마찬가지로 본 논문에서 제안한 광학적인 XOR 연산을 이중으로 이용한 OFB 방식의 시스템 역시 기존 OFB 방식의 장점을 가지고 있다. 암호화된 영상으로 암호화된 영상을 복원하기 위해서는 암호화키로만이 아닌 초기값 또는 그 이전 궤환된 영상이 필요하다. 본 논문에 사용한 이중 인코딩 XOR 연산 방식은 그 이상의 연산이 가능하고 내부의 궤환을 자유로이 적용할 수가 있다. 시뮬레이션에서 오직 올바른 암호화키로 사용할 경우에만 원래의 영상이 정확하게 복원되고 그 외 틀린 키를 사용하면 원 영상 을 알아낼 수 없다는 것을 확인하였다. 그리고 본 논문에서는 제안된 광학적 구성도를 실제 구현 가능한 광 모듈 형태로 제안하여 실질적인 광 암호화 시스템을 제안하였다. 기존의 블록 암호화인 OFB 방식을 광학적으로 구현하여 기존의 디지털적인 OFB 방식의 장점과 광학적인 고속성과 병렬성의 특성으로 인해 많은 정보를 빠른 속도로 암호화 및 복호화가 가능하기 때문에 기존의 OFB 방식보다도 한층 강력해진 암호화 시스템이라고 할 수가 있다. 앞으로 본 논문을 바탕으로 블록 암호화가 아닌 스트림 암호에도 적용하는 연구를 계획하고 있다.

References

[1] B. Javidi and J. L. Horner, "*Optical pattern recognition for validation and security verification*", Opt. Eng. Vol. 33, pp1752-1756, 1994.

[2] P. Refregier and B. Javidi, "*Optical image encryption based on input plane and Fourier plane random encoding*", Opt. Lett. Vol. 20, pp767-769, 1995.

[3] D. Weber and J. Trolinger, "*Novel implementation of nonlinear joint transform correlators in optical security and validation*", Opt. Eng. Vol. 38, pp62-68, 1999.

[4] T. Nomura and B. Javidi, "*Optical encryption using a joint transform correlator architecture*", Opt. Eng. Vol. 39, pp2031-2035, 1999.

[5] E. Cuche, F. Bevilacqua, and C. Depeursinge, "*Digital holography for quantitative phase-contrast imaging*", Opt. Lett. Vol. 24, pp291-293, 1999.

[6] G. Unnikrishnan and K. Singh, "*Double random fractional Fourier domain encoding for optical security*", Opt. Eng. Vol. 39, pp2853-2859, 2000.

[7] G-S Lin, H. T. Chang, W-N. Lie, and C-H Chuang, "*Public-key-based optical image cryptosystem based on data embedding techniques*", Opt. Eng. Vol. 42, pp2331-2339, 2003.

[8] S. H. Jeon, Y. G. Hwang, and S. K. Gil, "*Optical encryption of gray-level image using on-axis and 2-f digital holography with two-step phase-shifting method*", Opt. Rev. Vol. 15, pp181-186, 2008.

[9] T. Naughton, B. Hennelly, and T. Dowling, "*Introducing secure modes of operation for optical encryption*", J. Opt. Soc. Am. A Vol. 26, No. 10, pp2608-2617, 2008.

[10] J-W Han, C-S Park, D-H Ryu, and E-S Kim, "*Optical image encryption based on XOR operations*", Opt. Eng. **38**, 47-54, 1999.

[11] S. K. Gil, "*Optical CBC block encryption method using free space parallel processing of XOR operations*", Kor. J. of Opt. and Photo., Vol. 24, No. 5, pp262-270, 2013.

BIOGRAPHY

Gil Sang-Keun (Member)

1984 : BS degree in Electronic Engineering, Yonsei University.
1986 : MS degree in Electronic Engineering, Yonsei University.
1992 : PhD degree in Electronic Engineering, Yonsei University.
1993~1998 : Senior researcher in Advanced Technology Institute.
1998~present : Professor in Electronic Eng. The University of Suwon.