ISSN: 1226-7244 (Print)
ISSN: 2288-243X (Online)
논문번호 15-03-20

j.inst.Korean.electr.electron.eng.Vol.19,No.3,424~430,September 2015
http://dx.doi.org/10.7471/ikeee.2015.19.3.424

CFB 모드에 기반한 2 차원 페이지 데이터의 광학적 암호화 응용

Application to 2-D Page-oriented Data Optical Cryptography Based on CFB Mode

길 상 근*★

Sang-Keun Gil*★

Abstract

This paper proposes an optical cryptography application to 2-D page-oriented data based on CFB(Cipher Feedback) mode algorithm. The proposed method uses a free-space optical interconnected dual-encoding technique which performs XOR logic operations in order to implement 2-D page-oriented data encryption. The proposed method provides more enhanced cryptosystem with greater security strength than the conventional CFB block mode with 1-D encryption key due to the huge encryption key with 2-D arrayed page type. To verify the proposed method, encryption and decryption of 2-D page data and error analysis are carried out by computer simulations. The results show that the proposed CFB optical encryption system makes it possible to implement stronger cryptosystem with massive data processing and long encryption key compared to 1-D block method.

요 약

본 논문은 CFB(Cipher Feedback) 모드에 기반한 2 차원 페이지 데이터의 광학적 암호화 응용 시스템을 제안한다. 광학적으로 구현된 CFB 암호화 시스템은 2 차원 페이지 데이터 암호화를 위해 자유공간 광 연결 이중 인코딩 기법을 이용한다. 또한, 제안된 방법은 기존의 1 차원 암호화키를 처리하는 CFB 방식보다 2 차원 페이지 단위로 배열된 매우 큰 암호화키를 제공하기 때문에 암호강도가 한층 더 강화된 암호화 시스템을 구현한다. 제안한 CFB 알고리즘의 성능을 검증하기 위해 컴퓨터 시뮬레이션을 통하여 2 차원 페이지 데이터의 암호화 및 복호화 과정을 보여주고 오차 분석을 수행하였다. 시뮬레이션 결과, 제안한 CFB 방식은 기존의 1 차원 블록 방식보다 데이터 처리용량과 긴 암호화키를 가지는 강력한 광학적 페이지 암호화 시스템을 가능하게 한다.

Key words : Optical encryption, CFB mode encryption, Optical XOR logic operation, Dual-rail encoding, Cryptography

* Dept. of Electro. Eng., The University of Suwon

★ Corresponding author : skgil@suwon.ac.kr (031-220-2598)

Manuscript received 26, Aug. 2015; revised 10, Sep. 2015 ; accepted 10, Sep. 2015

Ⅰ. 서론

최근에 인터넷 및 모바일 기기에서 정보의 해킹으로 인하여 개인 정보의 유출뿐만 아니라 막대한 금융 손실을 유발하고 있다. 따라서 최근에 와서는 공중망에 대한 정보의 보호가 중요해졌고 정보 보안을 강화시키는 방법이 등장하고 있다. 세계적으로 대표적인 전자적 암호화 방식으로는 DES(Data Encryption Standard), AES(Advanced Encryption Standard)와 같은 전자적 암호화 방식이 사용되고 있다[1]. 일반적으로 암호화란 암호화하고자 하는 평문(plain text)을 상호간이 서로 알고 있는 암호화키(encryption key)를 이용하여 암호문(cipher text)로 생성하는 과정을 일컫으며, 이렇게 전송된 암호문을 암호화시 사용한 같은 암호화키로 복호화하는 과정이다. 하지만 최근에 컴퓨터 장비들의 발달로 인해 기존의 전자적 암호화 기술은 외부의 암호해석 공격으로부터 암호문이 해석되기도 하는 측면이 발생하고 있다. 따라서 이러한 정보 해킹으로부터 암호 강도를 높이기 위해 암호화키의 길이를 증가시키는 방법이 도입됐으며 이는 정보의 용량뿐만 아니라 암호화 처리 속도 면에서도 그 한계를 나타나게 되었다[2]. 이와 같은 전자적 암호화 방식의 문제를 해결하기 위해 1990년대 초부터 여러 가지 방식의 광학적 기술을 적용한 암호화 기법이 지속적으로 연구되어 왔는데[3-7], 이는 전자적 보안 기법의 대안으로서 기존의 사용하였던 전자적인 알고리즘을 대신하여 암호화 시스템을 광학적으로 구현하는 것이다. 광학적 암호화 방식은 전자적 보안 기법에 비하여 정보의 크기, 처리 속도가 월등한 능력을 가지는 장점을 가지고 있기 때문에 좀 더 복잡하고 빠른 광학적 암호화 기법들을 수행할 수 있다.[8] 이러한 광학적 암호화 방식들은 홀로그래피 기술을 이용한 아날로그 처리 방식과 디지털 처리 방식인 XOR 연산을 이용한 광 암호화 기법이 제안되었으며, 대표적인 디지털 처리 방법으로는 광학적으로 빛의 편광 성분을 이용하여 XOR 연산을 하는 방법[9]과 이중 인코딩(dual-rail encoding) 기법을 사용하여 자유공간 광 연결 논리 XOR 연산을 기반으로 하는 암호화 방법[10-11]이 있다. 본 논문에서는 블록 암호화 기법의 대표적인 CFB(Cipher Feedback) 모드를 광학적인 XOR 연산을 이용하여 2 차원 페이지 데이터의 광 암호화 및 복호화를 수행하는 암호화 시스템을 제안한다. 제안한 시스템의 성능을 확인하기 위해서 암호화하고자 하는 이진(binary) 평문 데이터를 이중 인코딩 방식과 자유 공간 광 연결에 기반한 XOR 연산을 이용하여 암호화 및 복호화 시뮬레이션을 수행하였고 암호화키 오차에 따른 오차 분석을 수행하였다.

Ⅱ. CFB(Cipher Feedback) 모드 암호화 알고리즘

블록 암호화 방식중 CFB 암호화 알고리즘은 암호화키를 처음에 어떤 임의의 초기값(initial value)과 암호화한 다음 이를 첫 번째 평문과 XOR 연산을 하여 첫 번째 암호문을 만든다. 그 다음 궤환된 암호문은 암호화키와 다시 암호화하고 이를 두 번째 평문과 XOR 연산을 하여 두 번째 암호문을 만들어 궤환시켜 계속해서 연속적으로 암호문을 발생시키는 대칭형 블록 암호화 알고리즘이다. 이 방식은 이전 암호문과 다시 또 암호화함으로써 ECB(Electronic Codebook) 모드 방식보다 훨씬 더 해독하기 어렵다는 장점을 지닐 뿐만 아니라 암호화할 암호문의 패턴이 나타나지 않는 장점을 가지고 있다. 또한 암호화할 평문과 암호화된 암호문으로 암호화키를 알아낼 수가 없기 때문에 암호문과 평문의 쌍을 암호해독 공격자가 가지고 있다 하더라도 이전의 암호문이 없다면 해독이 불가능한 장점을 지닌다. 또한 CFB 방식의 장점은 블록 암호화 모드의 또 다른 방식인 CBC(Cipher Block Chaining) 모드와 비교하여 CBC 방식의 특징은 암호문이 어떤 블록 하나에 오류가 발생한다면 해당 평문 복호화에 오류가 발생하며 다음 연산에 의한 그 다음 평문 블록의 복원에도 영향을 미치는데 반하여 CFB 방식은 암호문과 암호화키를 연산하여 평문과 XOR 연산을 한 값을 넘겨줌으로써 평문 각각의 독립적인 암호화를 할 수 있게 되어 오류의 전파가 발생하지 않는다. 또한 OFB(Output Feedback) 모드와 달리 동기화를 시켜줄 필요도 없다.

그림 1은 CFB 모드 암호화 알고리즘의 블록도를 나타내고, 평문 P_i와 암호문 C_i에 대한 암호화 수식은 다음과 같다.

$$I_0 = IV \tag{2.1}$$

$$I_i = C_{i-1}, \qquad 2 \le i \le m \tag{2.2}$$

$$C_i = P_i \oplus E_k(I_{i-1}), \qquad 1 \le i \le m \tag{2.3}$$

여기서 $I_0 = IV$는 초기값을 나타내고 $\oplus$는 XOR 연산을 의미하며 E_k는 암호화키에 의한 암호화 과정을 나타낸

다. 또한 m은 암호화하고자 하는 총 평문의 개수이다.

한편 i-번째 암호문 C_i에 대해서 CFB 방식의 복호화 수식은 다음과 같다.

$$R_i = C_i \oplus D_k(I_{i-1}) = P_i, \qquad 1 \le i \le m \tag{2.4}$$

여기서 D_k는 암호화키에 의한 복호화 과정을 나타낸다.

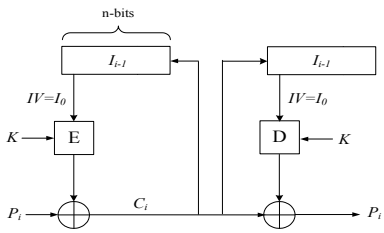


Fig. 1. Block diagram of CFB mode encryption algorithm
그림 1. CFB 모드 암호화 알고리즘의 블록도

III 제안한 CFB 모드의 광학적 암호화 시스템

일반적으로 디지털 암호화 기법에는 XOR 연산이 많이 이용된다. 이에 본 논문에서는 기존의 CFB 암호화 알고리즘을 XOR 논리 함수로만 표현되는 수정된 CFB 암호화 알고리즘을 제안한다. 특히 XOR 연산만의 암호화 방식은 만약 암호화에 사용되는 암호화키가 완전히 무작위적(random)이고 결코 재사용되지 않는다면 완전하게 보안성을 유지할 수 있다. 본 논문에서는 CFB 모드 방식에 기반한 이중 인코딩 XOR 연산을 통해서 간단하게 바꾼 CFB 암호화 시스템을 제안하고, 이를 광학적으로 2 차원 페이지 데이터로 확장된 암호화 응용을 제안한다. 기존의 전자적 블록 암호화 방식은 1 차원적인 n 비트 열(블록)의 암호화키와 평문, 암호문이 사용되는데 비하여 본 논문에서 제안한 방식은 2 차원의 페이지 단위의 n×n 비트 배열을 사용함으로써 매우 큰 암호화키를 구현할 수 있고 암호화하고자 하는 평문의 데이터량도 크게 할 수 있는 장점을 지닌다. 제안한 방식은 그림 1에서 표현된 암호화키에 의한 암호화 및 복호화 과정 E_k와 D_k를 XOR 연산으로 치환하여 암호화를 수행하는 방식이다. 그림 2는 제안한 2 차원 페이지 데이터 CFB 모드 암호화 방식의 블록도를 나타내고, Ⅱ절의 암호화 과정과 복호화 과정에 관한 수식 (2.3)식과 (2.4)식을 수식적으로 바꾸면 다음과 같이 간단하게 표현할 수 있다.

$$C_i = P_i \oplus (I_{i-1} \oplus K), \qquad 1 \le i \le m \tag{2.5}$$

$$R_i = C_i \oplus (I_{i-1} \oplus K) = P_i, \qquad 1 \le i \le m \tag{2.6}$$

여기서 (2.1)식과 (2.2)식은 여전히 유효하고, 초기값 $I_0 = IV$는 무작위하게 발생된 값이며, K는 암호화에 사용된 암호화키로 역시 무작위하게 발생된 값을 사용한다. 위 식에서 보는 것과 같이 XOR 연산을 이용한 CFB 방식도 해당 페이지의 암호문과 암호화키의 쌍이 해킹되었다 하더라도 이전 페이지의 암호문이 없다면 해당 페이지를 복호화할 수가 없다.

대칭형 암호화 시스템의 암호 강도는 암호화키 길이에 의존한다. 암호화키 길이가 길수록 암호문의 해독 공격은 더 어려워지고 암호 강도는 더 세어진다.

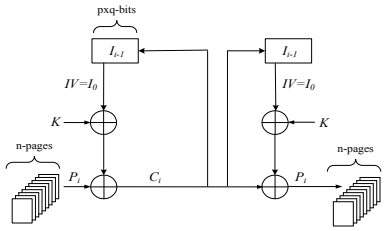


Fig. 2. Block Diagram of the proposed 2-D page-oriented data encryption based on CFB mode
그림 2. CFB 모드에 기반한 2차원 페이지 데이터의 암호화에 대한 제안 방식의 블록도

일반적으로 암호화키의 길이가 n-bits이면 올바른 암호화키를 찾기 위해서는 2^n 번의 암호해석 시도가 필요하다. 하지만 암호 강도를 높이기 위해 암호화키의 길이를 증가시키면 암호화 및 복호화 처리시간이 길어지고 암호문의 데이터 양도 늘어나 전송 시간이 길어지게 된다. 이렇게 암호화 키의 길이도 늘리고 많은 양의 데이터를 신속히 처리할 수 있는 요구를 만족하기 위해서 2 차원 페이지 데이터를 처리할 수 있는 광학적 암호화 방식은 그 대안이 될 수 있다. 따라서 암호화키의 길이를 2 차원 배열로 확대하여 증가시킬 수 있는 수정된 암호화 알고리즘을 광학적 장치로 구현하면 암호 강도뿐만 아니라 데이터 처리 속도도 동시에 향상시킬 수 있다. 만약 2 차원 암호화

키의 크기가 $p \times q$ 화소로 구성된다면 암호문을 해독하기 위한 암호화키를 찾는 시도는 $2^{p \times q}$ 으로 엄청나게 증가될 것이다. 본 논문에서는 이러한 광학적 특성과 XOR 연산 기반의 자유 공간 병렬 처리를 이용한 광학적 CFB 페이지 암호화 기법을 제안한다. 이 방식은 2 차원 페이지 형태의 암호화키와 평문을 구성하고 같은 2 차원의 암호문을 생성한다.

그림 3은 본 논문에서 제안한 이중 인코딩 방법과 자유 공간 광 연결 XOR 논리 연산에 기반한 2 차원 페이지 데이터의 CFB 모드의 암호화 및 복호화를 광학적 구현한 구성도를 보여준다.

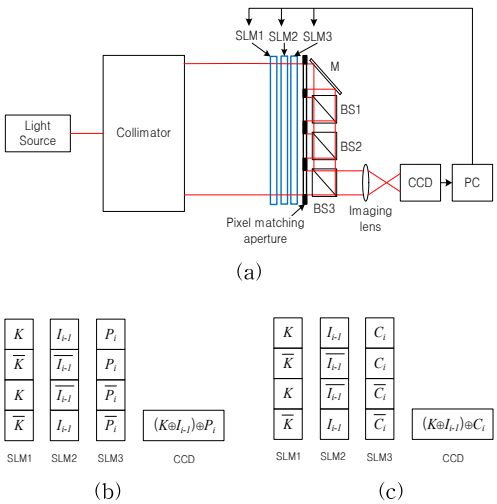


Fig. 3. Optical implementation for the proposed CFB mode encryption: (a) optical system using dual-rail encoding XOR operations, (b) representation of input SLM's data and output CCD data for encryption, (c) representation of input SLM's data and output CCD data for decryptionn

그림. 3. 제안한 CFB 모드 암호화의 광학적 구현: (a) 이중 인코딩 XOR 연산 방식을 이용한 제안된 광학적 시스템, (b) 암호화를 위한 입력 SLM과 출력 CCD의 데이터 표현, (c) 복호화를 위한 입력 SLM과 출력 CCD의 데이터 표현

그림 3(a)에서 세 개의 SLM(Spatial Light Modulator)의 직렬 배치는 각 SLM에 표현되는 입력 변수의 AND 연산을 수행하고 세 개의 BS(Beam Splitter)는 OR 연산을 수행하게 된다. 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 사용된다. 한편, 이 광학적 시스템은 SLM에 표시되는 입력 변수의 변환을 통해 복호화 과정을 수행하여 원래의 정보를 복원하는데 사용될 수 있다.

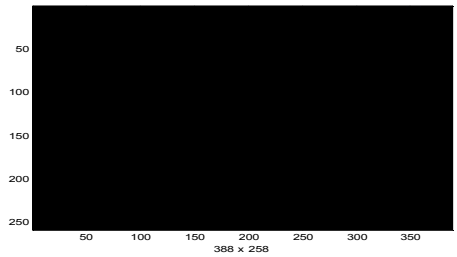
그림 3(b)와 (c)는 암호화 과정과 복호화 과정에서 각 SLM들에 표시되는 입력 변수들과 이때 CCD에 기록되는 암호화 데이터와 복호화 데이터를 나타낸다. 먼저 그림 3(b)와 같이 SLM1에 암호화키를 진수, 보수, 진수, 보수 순서로 입력하고 SLM2에 초기값을 진수, 보수, 보수, 진수 순서로 입력한다. SLM3에 암호화할 평문 데이터를 진수, 진수, 보수, 보수 순서로 입력한 뒤 광학적인 이중 인코딩 XOR 연산을 하면 암호화된 암호문 데이터를 CCD에서 얻어진다. 이때 획득된 암호문 정보는 다음 암호화를 위해서 SLM2에 궤환된다. 한편, 복호화 과정은 암호화에 사용되었던 똑같은 광학 시스템을 이용하여 얻을 수 있다. 그림 3(c)와 같이 SLM1과 SLM2에 암호화 과정에서 입력했던 암호화키와 초기값을 마찬가지로 진수와 보수 표현으로 입력하고 SLM3에 암호화된 암호문 데이터를 진수와 보수로 입력하면 원래의 평문 데이터가 복호화되어 CCD에서 얻어진다. 이때 이전 암호문은 SLM2에 궤환되어 다음 암호문을 복호화하는데 사용된다. 그림 3(a)의 광학적 구성도에 의해 (2.5)식과 (2.6)식과 같은 암호화와 복호화 연산 논리식을 얻을 수 있다.

$$\begin{aligned} C_i &= K \cdot I_{i-1} \cdot P_i + \overline{K} \cdot \overline{I_{i-1}} \cdot P_i \\ &\quad + K \cdot \overline{I_{i-1}} \cdot \overline{P_i} + \overline{K} \cdot I_{i-1} \cdot \overline{P_i} \\ &= P_i \oplus (I_{i-1} \oplus K) \end{aligned} \tag{2.7}$$

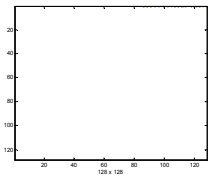
$$\begin{aligned} R_i &= K \cdot I_{i-1} \cdot C_i + \overline{K} \cdot \overline{I_{i-1}} \cdot C_i \\ &\quad + K \cdot \overline{I_{i-1}} \cdot \overline{C_i} + \overline{K} \cdot I_{i-1} \cdot \overline{C_i} \\ &= C_i \oplus (I_{i-1} \oplus K) \end{aligned} \tag{2.8}$$

Ⅳ 시뮬레이션

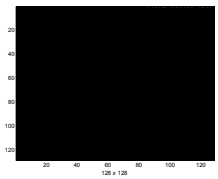
본 논문에서 제안한 XOR 연산의 이중 인코딩 자유 공간 병렬 처리를 이용한 광학적 CFB 모드 암호화 기법의 성능을 검증하기 위해 전산 실험을 하였다. 암호화할 평문 데이터는 Boolean XOR 연산을 하기



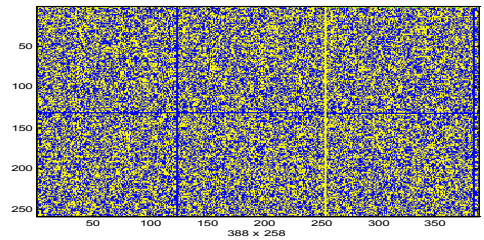
(a)



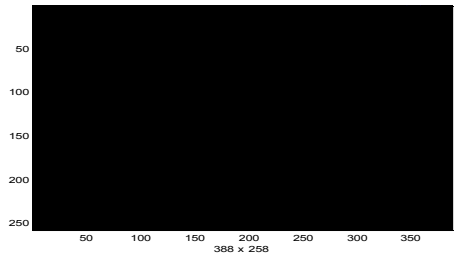
(b)



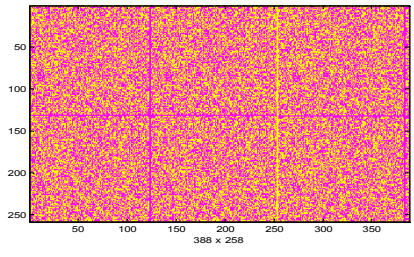
(c)



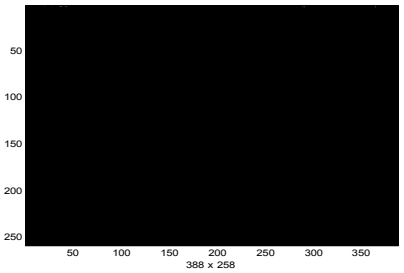
(d)



(e)



(f)



(g)

Fig. 4. Computer simulation results: (a) 6-pages of binary plain text data to be encrypted(P_i), (b) an encryption key(K), (c) initial value(I_0), (d) the encrypted 6-pages of cipher text(C_i), (e) the correctly decrypted plain text data by the correct encryption key, (f) the incorrectly decrypted plain text data by the incorrect encryption key, (g) the 1st and 5th incorrectly decrypted page data by the incorrect initial vale(I_0') and the incorrect cipher text(C_5')

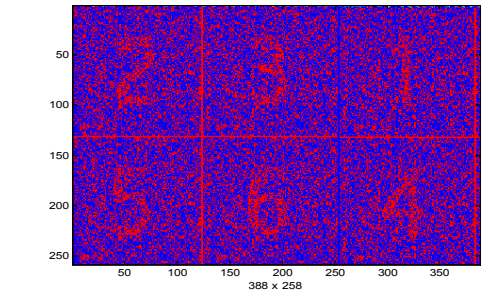
그림. 4. 암호화와 복호화의 전산 시늉 결과: (a) 암호화에 사용될 6-페이지의 이진 평문 데이터(P_i), (b) 암호화 키(K), (c) 초기화 값(I_0), (d) 6-페이지의 암호문 데이터(C_i), (e) 올바른 암호화키로 복호화된 원 평문 데이터, (f) 틀린 암호화키로 복호화된 데이터, (g) 복호화시 틀린 초기값(I_0')으로 복원된 첫 번째 틀린 페이지와 틀린 암호화 값(C_5')으로 복원된 다섯 번째 틀린 페이지를 보여주는 데이터

위해서 반드시 이진 데이터나 영상이어야 하므로 암호화할 목표 평문 데이터를 그림 4(a)와 같이 간단히 숫자 데이터를 사용하였다. 이때 평문 데이터는 2 차원 페이지로 표시되고 편의상 6 페이지를 선택하였고 한 페이지의 크기는 128×128 화소를 가지며 평문 P_1, P_2, …, P_6 를 나타낸다.

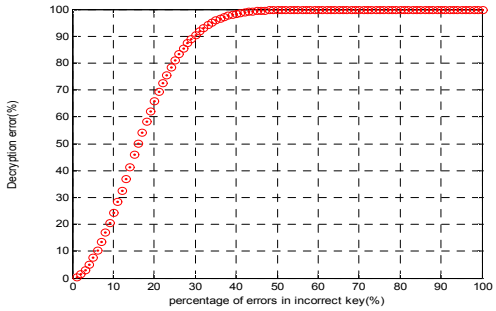
그림 4(b)는 암호화와 복호화에 사용되는 128×128 화소 크기를 갖는 하나의 2 차원 페이지로 구성된 암호화키를 보여준다. 여기서 암호화키는 편의상 무작위 값을 갖도록 발생시켰고, 수치적으로 하얀 화소는 1, 검은 화소는 0을 나타낸다. 암호화키의 크기가 128×128 화소라는 것은 암호화키의 길이가 16,384 bits라는 의미이며(통상 전자적 CFB 암호화에서의 암

호화키의 길이는 64-bits), 암호 강도는 올바른 암호화키를 찾기 위해 $2^{128\times128}$ 번의 시도가 필요하다는 것을 의미한다. 그림 4(c)는 CFB 암호화 기법에 필요한 초기값 I_0를 나타내며 이 또한 무작위 값을 갖도록 발생시켰다. 그림 4(d)는 초기값을 포함하여 궤환된 이전 암호문과 암호화키를 사용하여 광학적 CFB 방식으로 2 차원 페이지 암호화된 암호문을 보여준다. 본 논문에서 제안한 자유 공간 광 연결 XOR 논리 게이트의 특성으로 출력 암호문의 한 페이지의 크기는 입력 평문과 같은 128×128 화소의 크기를 가지며 암호문 C_1, C_2, …, C_6 를 나타낸다. 그림 4(e)는 암호문과 그림 4(b)에 보여진 암호화에 사용된 올바른 암호화키를 이용하여 복호화된 6 페이지의 복호화 데이터를 보여준다. 이때 암호화 초기값 I_0가 복호화 과정에서 사용된다. 마찬가지로 한 페이지의 크기는 입력 평문과 같은 128×128 화소의 크기를 가지며 복호화 데이타 R_1, R_2, …, R_6 를 나타낸다. 한편 그림 4(f)는 복호화할 때 암호화에 사용되지 않은 틀린 키로 복호화된 데이터로 원래의 평문 데이터인 그림4(a)의 숫자가 복원되지 않음을 보여준다. CFB 모드의 특징은 암호문이 어떤 블록(본 논문에서는 페이지) 하나에 오류가 발생한다면 해당 평문 복호화에 오류만 발생할 뿐 다음 과정에 의한 그 다음 평문 데이터의 복원에 영향을 미치지 않는다는 점이다. 그림 4(g)는 첫 번째 페이지 암호문이 초기값 I_0가 달랐을 때 첫 페이지가 틀리게 복원된 경우와 다섯 번째 암호문을 복호화할 때 이전 네 번째 암호문이 틀리게 전송되어 오류가 발생했을 경우 다섯 번째 페이지가 틀리게 복원된 경우를 보여준다. 그림에서 보듯이 해당 페이지에서만 복호화 오류가 나타나고 나머지 페이지에서는 올바르게 복호화 됨을 보여준다.

한편 복호화 과정에서 암호화키 오차에 따른 복호화된 데이터의 오차 분석을 수행하였다. 그림 5(a)는 암호화 과정에서 사용된 올바른 암호화키에 대해서 복호화에 사용된 틀린 암호화키가 원래의 올바른 키와 비교하여 20%의 화소 오차가 있는 틀린 키를 사용하여 복호화한 데이터를 보여준다. 그림 5(b)는 틀린 암호화 키의 오차에 따른 복호화 된 데이터의 오차를 보여주는 그래프이다. 그림에서 알 수 있듯이 틀린 암호화키에 의해 복호화된 영상은 원래의 평문 데이타를 완벽하게 복원하지 못하고, 틀린 암호화키를 사용하였을 때는 복원에 사용된 키의 오차 정도에 따라 원래 평문 데이터에 오차가 발생함을 알 수 있다.



(a)



(b)

Fig. 5. Error analysis of decryption process: (a) incorrectly decrypted data by the incorrect encryption key with 20% error bits, (b) decryption error according to incorrect key error

그림. 5. 복호화 과정의 오차 분석: (a) 올바른 키에 대하여 20%의 화소 오차를 갖는 틀린 키로 복호화된 데이터, (b) 틀린 키 오차 정도에 따른 복원 데이터의 오차

V 결론

본 논문에서는 블록 암호화 방식중의 하나인 CFB 모드 암호화 알고리즘을 2 차원 페이지 데이터로 확장된 새로운 CFB 모드 암호화 기법으로 변형하고 이를 광학적으로 XOR 연산의 이중 인코딩 자유 공간 병렬 처리를 이용하여 암호화 및 복호화 시스템을 구현하는 방법을 제안하였고, 이를 전산 시뮬레이션을 통해 구현 가능성을 확인하였다. 제안한 방법의 광학적 구성도는 AND 연산이나 OR 연산 같은 광 논리를 자유 공간상에 연결하기 위한 거울과 BS와 암호

화할 평문과 암호화키를 2 차원 배열로 표시하는 SLM, 암호문을 기록하기 위한 CCD 등으로 매우 간단히 구현되고, 이 암호화 구성도는 같은 구조를 사용하여 복호화 과정도 수행할 수 있다. 전산 시뮬레이션에서 오직 올바른 암호화키로 사용할 경우에만 원래의 평문이 정확하게 복원되고 그 외 틀린 키를 사용하면 원 평문을 복원해 낼 수 없다는 것을 확인하였다. 그리고 암호화된 암호문으로 원래의 평문을 복원하기 위해서는 초기값 또는 그 이전 궤환된 암호문에 의해 암호화된 암호화키의 정보가 필요한데 본 논문에 사용한 이중 인코딩 XOR 연산 방식은 이러한 궤환을 자유로이 적용할 수 있다. 또한 제안된 방법은 기존의 CFB 방식을 광학적으로 구현했기 때문에 기존의 전자적인 CFB 방식의 장점과 광학적인 고속성과 병렬 처리의 특성으로 인해 많은 정보의 빠른 속도 암호화 및 복호화가 가능하다. 한편, 광 병렬 처리의 특성상 2 차원 평문 데이터와 암호화키를 사용함으로써 블록 데이터를 페이지 단위의 크기로 확장 증가하므로 기존의 1 차원 암호화 키를 사용한 방식보다도 한층 암호 강도가 강력해진 암호화 시스템이라고 할 수가 있다. 본 논문에서는 암호키의 크기를 128×128 화소로 하여 암호 강도는 올바른 암호화키를 찾기 위해 $2^{128\times128}$ 번의 시도가 필요한 암호화 시스템을 보여준다.

References

[1] B. Schneier, *Applied cryptography, 2nd ed.* John Wiley, New York, 1994.

[2] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "*On the security defects of an image encryption scheme*", Image and Vision Computing, Vol. 27, pp1371-1381, 2009.

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

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

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] S. K. Gil, "*Optical system implementation of OFB block encryption algorithm*", J.inst.Korean.electr.electron.eng., Vol. 18, No. 3, pp31-37, 2014.

BIOGRAPHY

Sang-Keun Gil (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.