논문 2026-2-7 http://dx.doi.org/10.29056/jsf.2026.06.07

고속 푸리에 변환 기반 암호 시스템에서 하다마드 코드를 이용한 다중 이미지 암호화

송재훈*†

Multiple Image Encryption Using Hadamard Codes in Fast Fourier Transform-Based Encryption Scheme

Jae-Hun Song*†

요 약

IT 산업의 급속한 성장과 함께 디지털 기술에 대한 의존성이 점차 심화되고 있다. 기술이 정교해 지면서 개인정보 탈취 및 불법 복제와 같은 보안 위협이 지속적으로 증가함에 따라 데이터 보호의 중요성이 더욱 부각되고 있다. 따라서 정보의 무결성과 안전성을 보장하기 위한 효과적인 정보보안 기술이 강조된다.

본 연구에서는 고속 푸리에 변환(FFT)을 이용한 암호화 시스템에서 하다마드(Hadamard) 코드를 이용한 다중 이미지 암호화 방식을 제안한다. 빠른 데이터 송/수신이 가능한 FFT 암호화 시스템에 하다마드 코드를 이용해 다중 이미지를 암호화하는 방식을 적용하여 원하는 데이터만 복원 함으로써 데이터 관리의 효율성을 높인다. 또한 원본 및 암호화, 복원된 데이터의 상관계수를 통해 제안된 방식의 암호화 데이터의 성능을 확인해 본다.

Abstract

Rapid growth in the IT industry has increased reliance on digital technologies, leading to escalating security threats such as data leakage and unauthorized duplication. Consequently, effective information security technologies have become increasingly important for ensuring the integrity and confidentiality of transmitted data. This study proposes a multiple-image encryption scheme using Hadamard codes in a Fast Fourier Transform (FFT)-based optical encryption system. By incorporating Hadamard-code multiplexing into the high-speed FFT optical encryption framework, the proposed method enables selective decryption of target images, thereby improving data management efficiency. In addition, the cryptographic performance of the proposed scheme is validated through correlation coefficient analysis of the original, encrypted, and decrypted images.

한글키워드 : 고속 푸리에 변환, 정보 보안, 암호화, 하다마드 코드, 이미지 프로세싱

keywords : Fast Fourier Transform(FFT), Information Security, Encryption, Hadamard Code, Image Processing

* 경기과학기술대학교 컴퓨터모바일융합과
† 교신저자: 송재훈(email: sjhh81@gtec.ac.kr)
접수일자: 2026.06.01. 심사완료: 2026.06.10.
게재확정: 2026.06.20.

1. 서 론

IT 기술이 발전함에 따라 디지털 데이터는 개

인 및 기업 활동의 핵심 자산으로 자리 잡았다. 특히 인공지능(AI), 양자(Quantum), 광학 기술 등의 발전은 더욱 빠르고 정교한 정보 복제와 유출을 가능하게 하였고 최근 기업들은 해킹 및 비의도적 정보 유출 사고 또한 지속적으로 증가하고 있다. 디지털 데이터는 복제와 변조가 용이하여 저장 및 전송 과정에서의 기밀성과 무결성 확보가 중요한 보안 과제이며 차별화된 보안기술의 필요성이 특히 대두되고 있다[1-4].

일반적인 2D 영상 데이터에 비해 훨씬 방대한 정보를 포함하는 홀로그램 등 3D 영상 데이터의 등장으로, 대용량 데이터를 효율적으로 처리하면서 위상 정보를 함께 활용할 수 있는 다양한 연구가 제안 되어왔다. 대표적으로 원본 이미지의 각 픽셀값의 위상을 임의로 변조하는 랜덤 위상 마스크(Random Phase Mask, RPM) 기반 기법[5], 이산 푸리에 변환(Discrete Fourier Transform, DFT) 과정에서 계산 식의 파라미터를 암호키로 활용하는 암호화 기법[6] 등이 연구되었다. 이와 더불어 빠른 데이터 처리를 위해 고속 푸리에 변환(Fast Fourier Transform, FFT)을 이용하여 연산의 경로에 접근하여 데이터에 다양한 암호키를 적용하는 방법이 제안되었다[7, 8]. 다음으로 다중 이미지를 암호화 하는 기법으로 광신호의 Wavelength Multiplexing을 이용해 파장의 길이를 암호키로 사용하여 여러 이미지를 암호화 하는 방법이 제안되었으며[9], 하다마드 코드의 직교성(Orthogonality)을 이용하여 다중 이미지를 암호화하는 보안 시스템을 제안하였다[10, 11]. 이러한 연구를 기점으로 다중 영상 암호화 기술은 정보 전송 효율이 높다는 장점으로 인해 많은 관심을 받아왔으며, 키 공간 확장을 통한 보안성 확보와 딥 러닝 등을 결합하여 관련 연구가 지속적으로 수행되고 있다[12, 13].

본 연구에서는 선행 연구[7, 8]에서 제안한 모델인 FFT 기반 암호화 방식을 확장하여 기존의 단일 이미지 암호화 방식이 아닌, 하다마드(Hadamard) 코드를 이용한 다중 이미지 암호화 기법을 제안한다. 제안한 방법은 하다마드 코드를 활용하여 기존 방식의 연산 복잡도를 줄이면서 여러 이미지를 동시에 암호화 및 저장할 수 있으며, 복원 과정에서는 원하는 하다마드 코드를 적용하여 특정 이미지만 선택적으로 복원할 수 있다. 또한 FFT 기반 암호화 알고리즘을 적용함으로써 빠른 데이터 처리 속도를 유지하면서도 효율적인 키 공간을 확보할 수 있도록 설계하였다. 이를 통해 다중 이미지의 암호화 및 복호화 성능과 제안 기법의 유효성을 검증하였다.

2. 데이터 암호화에 사용된 기술 기본 이론

2.1 FFT 버터플라이 알고리즘

고속 푸리에 변환의 수행 방식을 설명하기 위해 먼저 일반적인 이차원(2D) 이미지 데이터 $f(x, y)$의 주파수 분석을 위한 푸리에 변환은 다음 식 (1)과 같은 적분 형태로 정의된다.

$$F(u,v) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)e^{-i2\pi(ux+vy)}dxdy \quad (1)$$

푸리에 변환은 디지털 영역의 계산 과정에서 식 (2)와 같이 이산 푸리에 변환(DFT)으로 표현할 수 있다.

$$F(\alpha,\beta) = \sum_{a=0}^{M-1}\sum_{b=0}^{N-1} f(a,b)e^{-i2\pi(\frac{\alpha a}{M}+\frac{\beta b}{N})} \quad (2)$$

여기서 a와 b는 영상 공간 영역(Spatial Integer)에서의 이산 좌표(픽셀 인덱스)를 의미하고 α와 β는 공간 주파수(Spatial Frequency) 인덱스를 의미하며, M과 N은 각각 x축과 y축 방향의 샘플수를 나타낸다. 일차원(1D)의 경우

DFT는 다음 식 (3)과 같이 단순화된다.

$$F[a]=\sum_{a=0}^{M-1} f(a)w^{aa} \quad (3)$$

이때 복소 지수항은 트위들 팩터(Twiddle Factor)로 식 (4)와 같이 정의되며, 이는 연산 과정에서 반복적으로 사용되는 핵심 요소이다.

$$w=\exp(-i2\pi/M) \quad (4)$$

여기서 실수부가 $\cos(2\pi/M)$, 허수부가 $\sin(2\pi/M)$이며 $i=\sqrt{-1}$ 이고, M은 샘플 수를 의미한다. 이러한 DFT를 직접 계산할 경우 연산량은 $O(M^2)$이지만, FFT는 이를 $O(Mlog_2M)$으로 획기적으로 감소시킨다.

그림 1에서 보여지는 것처럼 FFT는 신호를 여러 단계로 분해하여 작은 DFT 연산으로 구성하는 방식이며, 이때 각 경로에서 수행되는 연산 구조를 버터플라이 연산이라 한다. 버터플라이 구조의 특징은 다음과 같다. 첫째, 입력 데이터는 먼저 비트 반전 순열(Bit-Reversal Permutation)을 거쳐 재배열 된다. 둘째, 이후 단계적으로 두 신호 성분을 결합하며 연산이 진행된다. 셋째, 각 경로마다 트위들 팩터가 곱해지며 주기성과 대칭성이 활용된다.

데이터 크기가 $M=2^m$일 경우 총 $\log_2 M$개의 단계가 형성되며, 각 단계에서 독립적인 연산 경로가 존재한다. 이러한 분해성을 통해 연산의 복잡성이 획기적으로 줄어들어 빠른 데이터 처리를 가능하게 한다[14-16].

본 연구에서는 이러한 FFT의 특정 연산의 경로의 번호가 암호키로 사용되며 추가적인 암호키를 적용함으로써 데이터 암호화의 복잡성을 더욱 높인다.

2.2 하다마드 개념

하다마드(H) 행렬은 모든 원소가 +1 또는 -1(0 또는 π)로 구성된 $N\times N$ 정방행렬이며, 행

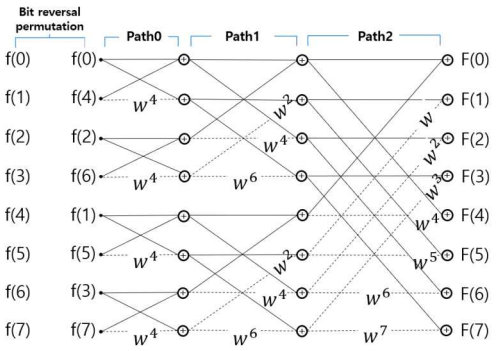

그림 1. M=8일 때 고속 푸리에 변환의 버터플라이 알고리즘(일차원)
Fig. 1. Butterfly algorithm of Fast Fourier Transform for M=8 (1D)

과 열 벡터가 서로 직교(Orthogonal) 한다는 특징을 가진다. n차 하다마드 행렬은 다음 식 (5)를 만족한다.

$$H_N^T H_N = NI_N \quad (5)$$

여기서 H_N^T는 전치행렬이고, I_N은 $N\times N$ 단위행렬이다. 이 조건은 서로 다른 두 행(또는 열)의 내적이 0이 됨을 의미한다.

Sylvester 방식에 따라 재귀적으로 생성할 수 있으며, $N=2^m$ (m은 정수)일 때 다음식 (6)과 같이 확장된다.

$$H_{2N}=\begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix} \quad (6)$$

예를 들어 4-bit 하다마드 행렬은 다음식 (7)과 같은 형태를 갖는다.

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad (7)$$

하다마드 행렬은 다음과 같은 특성을 갖는다. 행 또는 열의 순서를 변경해도 직교성 유지, 행 또는 열의 부호 반전에도 직교성 유지, 그리고 Walsh-Hadamard 코드의 형태로 확장 가능하다.

이러한 직교 특성은 신호의 상호 간섭을 최소화 하는데 유리하며, 위상 변조 기반 암호화에 효과적으로 활용될 수 있다[17-19].

본 연구에서는 하다마드 행렬을 다중 이미지 암호화를 위한 암호키로 사용한다. 해당 코드를 다중 이미지의 각 픽셀에 +1 또는 -1(0 또는 π)을 복소수 곱셈을 수행하여 원본 이미지들에 구조적인 변형을 가한다. 이 방식은 이미지의 각 픽셀에 복잡한 랜덤 위상 암호키를 적용하지 않고도 연산의 부하를 줄이고 직교성 기반의 암호화 효과를 얻을 수 있게 된다.

3. 데이터 암호화 및 복호화

3.1 데이터 암호화 과정

하다마드 코드의 직교성은 다중 이미지 데이터를 상호 간섭 없이 암호화 및 복원할 수 있는 특성을 제공한다. 본 연구에서는 이러한 특성을 이용하여 식 (7)의 4-bit 하다마드 행렬의 각 행을 하나의 코드로 정의하고, 이를 원본 이미지에 적용하여 4개의 이미지를 동시에 암호화하는 방법을 제안한다.

먼저, 크기가 동일한 네 개의 입력 영상 $I_1(x, y)$, $I_2(x, y)$, $I_3(x, y)$, $I_4(x, y)$를 고려한다. 각 영상의 동일한 픽셀 위치 (x, y)에서의 값을 하나의 벡터로 정의하면 다음식 (8)과 같다.

$$\boldsymbol{I}(x,y) = \begin{bmatrix} I_1(x,y) \\ I_2(x,y) \\ I_3(x,y) \\ I_4(x,y) \end{bmatrix} \quad (8)$$

4-bit 하다마드 행렬 H를 이용하여 각 픽셀 벡터에 대해 선형 변환을 수행하면 식 (9)와 같이 암호화된 데이터 $S(x,y)$를 얻을 수 있다.

$$\boldsymbol{S}(x,y) = H_4^T \boldsymbol{I}(x,y) \quad (9)$$

즉, 각 픽셀 위치(x, y)에서 입력된 4개의 이미지에 하다마드 변환이 적용되며, 그 결과 다음 식(10)과 같은 네 개의 출력 성분이 생성된다.

$$\begin{bmatrix} S_1(x,y) \\ S_2(x,y) \\ S_3(x,y) \\ S_4(x,y) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} I_1(x,y) \\ I_2(x,y) \\ I_3(x,y) \\ I_4(x,y) \end{bmatrix} \quad (10)$$

예를 들어, 특정 픽셀 위치(x,y)에 다음과 같이 I_1=10, I_2=20, I_3=30, I_4=40의 값이 주어졌다고 가정했을 때, 식 (10)을 이용하여 하다마드 변환을 적용하면 S_1=100, S_2=-20, S_3=-40, S_4=0의 값이 나온다. 이 과정은 전체 영상에 대해 반복 수행되며, 결과적으로 입력 영상들은 서로 직교한 코드에 의해 결합 된 다중 데이터 형태로 변환된다. 여기서 이미지들에 사용된 하다마드 코드가 암호키처럼 사용된다.

다음으로 사용된 암호화 방식은 FFT 버터플라이 연산 구조 내부에서 선택적 데이터 변형을 수행하는 것을 핵심 개념으로 한다. 기존 방식이 입력 또는 출력 데이터에 직접 암호키를 적용하는 것과 달리, 본 방법은 FFT 버터플라이 연산 중 특정 경로에 접근하는 특징을 가지고 추가 암호키를 적용하여 데이터를 변환한다.

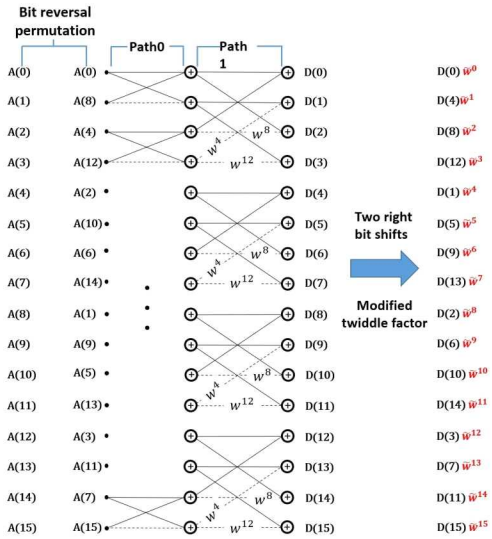

그림 2. M=16일 때 FFT의 버터플라이 알고리즘(일차원). 데이터에 비트 시프트 및 변형된 트위들 팩터 적용
Fig. 2. Butterfly algorithm of FFT for M=16 (1D). Application of bit shift and modified twiddle factor to the data

그림 2에서 보이는 것처럼 일차원 입력 데이터 크기가 $N=2^m$일 경우, FFT는 총 m개의 경로로 구성된다. 각 경로는 서로 다른 위치의 데이터 결합 구조를 가지며, 본 연구에서는 이 경로 중 하나를 선택하여 암호 연산이 이루어지도록 설정한다. 즉, 선택된 경로 번호는 첫 번째 암호키로 사용된다. 데이터 크기가 증가함에 따라 FFT 연산 단계에서 형성되는 경로의 수 또한 증가하고 특히, 이차원 데이터의 경우 행과 열 방향에 대해 각각 FFT가 수행되므로, 적용 가능한 경로의 조합 범위가 더욱 확장된다. 두 번째 암호키로 변형된 트위들 팩터 값을 넣게 된다.

$$\tilde{w}=\exp(-i2\pi/M') \tag{11}$$

기본 트위들 팩터는 원본 데이터의 크기에 따라 M 값이 결정되지만 식 (11)의 M'에 임의의 값을 넣어 변형된 트위들 팩터 값을 만들고 버터플라이 연산이 완료된 결과 값 $D(j)$에 변형된 트위들 팩터 값을 곱셈 형태로 적용하였다. 이 과정에서 원본 데이터의 진폭 및 위상 정보가 아주 랜덤한 값을 가지게 변형되며, 이는 픽셀 배열에 랜덤 위상 마스크를 부여하는 것과 유사한 동작을 수행한다. 여기서 M'에 들어가는 값이 두 번째 암호키로 사용된다. 마지막으로 데이터 암호화 복잡성을 높이기 위해 세 번째 암호키로 Bit-Shift(BS)를 적용하였다. 그림 2에 보여지는 바와 같이 데이터 $D(j)$에 Bit-Shift를 이용하여 데이터 배열의 위치를 바꾸게 된다. 다시 말해 데이터 인덱스를 이진수로 표현한 후, 좌우 방향 비트 시프트 연산을 통해 새로운 인덱스를 생성한다. 예를 들어 N=256에서 j=3은 이진수로 0000 0011이며, 우측으로 한번 시프트 시 1000 0001이 되어 십진수 129로 변환된다. 이에 따라 3번 위치의 데이터는 129번 위치로 이동한다. 본 연구에서는 오른쪽 Bit-Shift의 횟수를 세 번째 암호화 키로 이용하여 데이터 순서를 랜덤하게 재구성한다.

3.2 데이터 복호화 과정

하다마드 코드를 이용해 결합된 다중 이미지의 복호화 과정은 다음 식 (12)과 같이 표현된다.

$$\boldsymbol{I}(x,y)=\frac{1}{4}H_4\boldsymbol{S}(x,y) \tag{12}$$

즉, 각 이미지는 해당 하다마드 코드와의 내적 연산을 통해 복원된다. 위에서 설명한 3. 1 데이터 암호화 과정의 예시 값을 이용하여 복원하면 S=[100, -20, -40, 0]에서 첫 번째 이미지 I_1(x,y)의 복원은 식 (12)에 의하여 코드 1을 적용하면 I_1(x,y)={(100+(-20)+(-40)+0)}/4=10 이 나온다.

동일한 방식으로 나머지 이미지도 복원을 하면 원본 픽셀 데이터 값으로 복원된다. 이를 통해 암호화 과정에서 결합된 데이터가 직교성에 의해 상호 간섭 없이 정확히 분리됨을 확인할 수 있다.

FFT에서 버터플라이 알고리즘을 이용해 암호화된 데이터를 복원하기 위해 암호화된 데이터에 역 고속 푸리에 변환(Inverse Fast Fourier Transform, IFFT)을 적용한다. 이 과정에서는 암호화 단계에서 사용된 경로 번호, 변형된 트위들 팩터, 그리고 비트 시프트를 복원키로 활용하여 원본 데이터를 재구성한다.

먼저 경로 번호로 데이터에 접근했을 때, FFT 과정에서의 버터플라이 연산 결과와 IFFT 과정에서의 버터플라이 연산 결과는 데이터의 위치와 값에서 차이가 존재한다. 따라서 단순히 동일 경로의 값을 대응시키는 방식으로는 정확한 복원이 이루어지지 않으며, 이 차이를 고려한 추가적인 정렬 과정이 필요하다.

일반적으로 IFFT 수행 시 각 경로의 결과 값이 FFT에서의 해당 경로 값과 동일할 것으로 예상할 수 있으나, 실제로는 그렇지 않다. 예를 들어, 그림 3에서와 같이 복원 과정에서 암호키 경로 1을 예를 들어 적용하면, 연산 결과로 얻어지는 데이터의 위치 $D(j)$가 그림 2의 결과와 상이함을 확인할 수 있다.

이를 보정하기 위해 먼저 데이터 순서를 재정렬하는 Bit Reversal Permutation(BRP)을 수행하고, 연산 과정에서 포함된 트위들 팩터 w를 제거한다. 이 과정을 거치면 그림 2의 암호화 데이터와 동일한 배열 구조를 갖는 값을 얻을 수 있으며, 해당 데이터를 이용하여 추가로 적용했던 변형된 트위들 팩터 $\tilde{w}$ 를 제거한다. 또한 비트 시프트 연산에 대해서는 암호화 시 적용된 횟수만큼 역연산을 수행해야 한다. 본 연구에서는 두

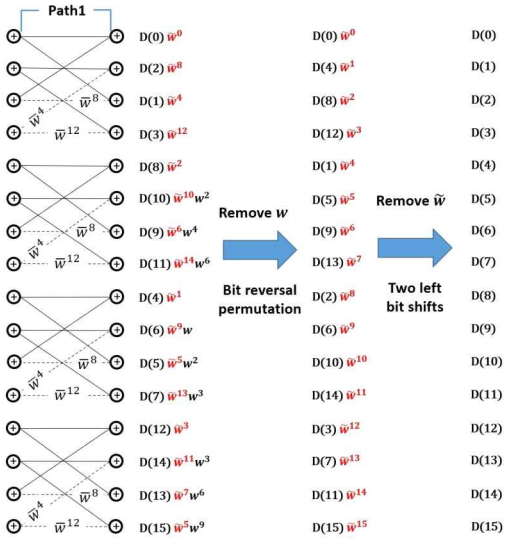

그림 3. 데이터 복원을 위해 경로 1에서 IFFT. 변형된 트위들 팩터 제거와 왼쪽 비트 시프트.

Fig. 3. IFFT along path 1 for data reconstruction. Application of Modified Twiddle Factor and Left Bit Shift

번의 좌측 비트 시프트가 적용되었으므로, 동일한 횟수로 역과정인 우측 비트 시프트를 수행해 데이터의 원래 순서를 회복한다. 이후 남은 IFFT 버터플라이 연산을 수행하기 위해 트위들 팩터 w를 다시 적용하고, BRP를 통해 데이터 배열을 정렬한 뒤 IFFT를 완료한다. 이러한 과정을 통해 최종적으로 복원된 이미지를 획득할 수 있다.

4. 시뮬레이션

4.1 다중 이미지 암호화/복호화 시뮬레이션

본 논문에서는 256×256픽셀 해상도를 가지는 서로 다른 원본 이미지 4개를 이용하여 다중 이미지를 합성하였다. 그림 4에서 사용된 원본 이미지를 보여주고 있으며, 이때 4-bit 하다마드 코

드를 이용하여 하나의 이미지로 합성하고 그 데이터에 FFT 버터플라이 알고리즘의 암호키를 적용하여 시뮬레이션하였다.

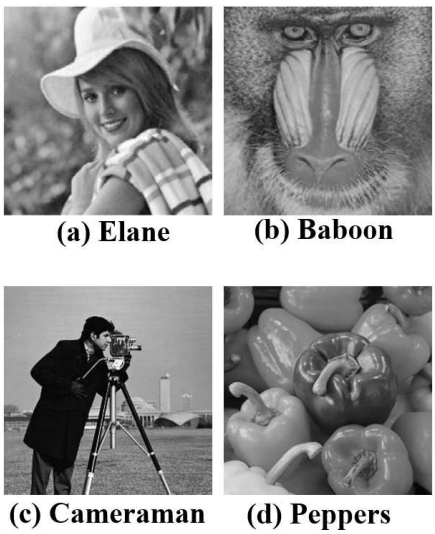

그림 4. 원본 이미지
Fig. 4. Original Images.

FFT에서 사용된 암호화 키는 경로 번호, 변형된 트위들 팩터, 비트 시프트를 이용하였으며 데이터 분석의 일관성을 위해 4개의 원본 이미지에 동일한 암호키를 적용하였고 사용된 암호키를 표 1에 정리하였다.

다음의 그림 5는 하다마드 4-bit의 각 코드를 적용하여 하나로 합성된 이미지를 보여주고 있으며, 그림 6은 합성된 데이터에 FFT 버터플라이 암호화 키를 적용해 최종 암호화된 데이터 결과를 보여주고 있다. 다음으로 정확한 하다마드 코드와 암호키를 이용하여 복원했을 때 데이터를 그림 7에서 보여주고 있다. 그리고 데이터 복원 시 잘못된 키 정보를 이용하여 복원을 시도 했으며 그림 8에서 그 결과를 확인할 수 있다. 이때 복원을 시도하기 위해 사용된 키를 표1에 작성하였다.

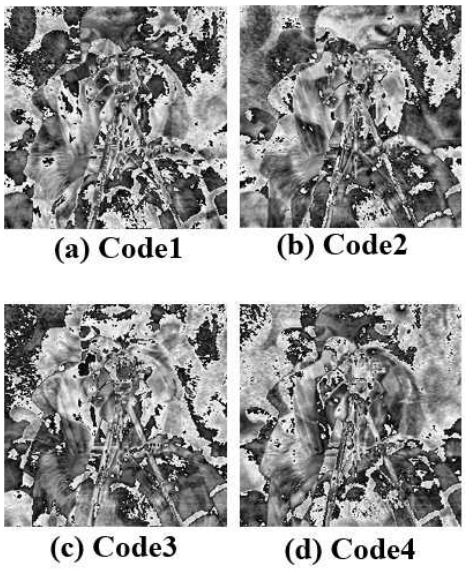

그림 5. 하다마드 코드를 적용해 4개의 다중 이미지를 하나의 이미지로 합성
Fig. 5. Multiplexing of four images into a single image using Hadamard codes

4.2 암호화 데이터 성능 분석

본 연구에서는 제안한 암호화 알고리즘 및 마스크의 성능을 검증하기 위해 식 (13) 정의된 원본 이미지와 복호화 이미지 간의 상관계수(Correlation Coefficient, CC)를 지표로 활용하여 원본과 복호화 이미지 간의 통계적 유사성을 분석하였다.

$$CC = \frac{cov(d, o)}{\sigma(d)\sigma(o)} \tag{13}$$

여기서 cov(d, o)는 두 이미지 간의 교차 공분산을, σ(d)와 σ(o)는 각각 복호화된 이미지와 원본 이미지의 표준편차를 나타낸다. 일반적인기준에 따르면 CC 값이 0.25 미만일 경우 암호화 성능의 유효성이 인정되고 CC가 1에 가까울수록 복호화된 이미지와 원본 이미지 간의 유사성이 높음을 의미한다[20, 21].

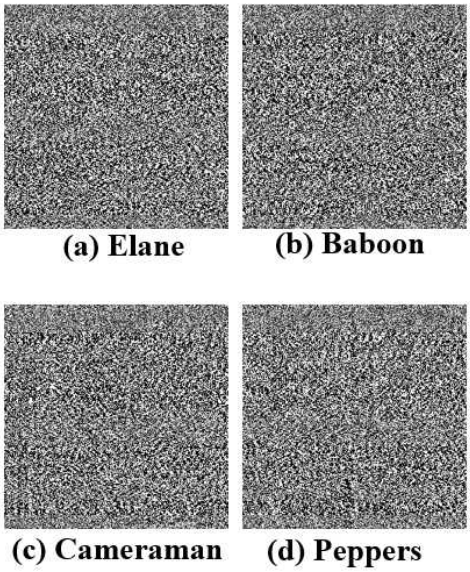

그림 6. 암호화된 이미지
Fig. 6. Encryption Images.

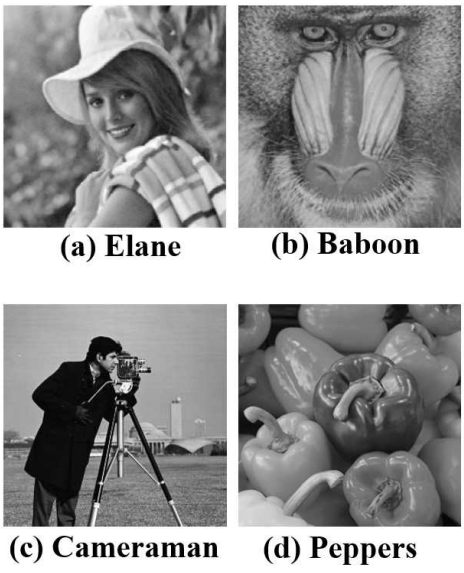

그림 7. 복호화된 이미지
Fig. 7. Decryption Images.

본 연구에서 분석 결과를 표 1에 작성하였으며 반복적인 시뮬레이션을 통하여 평균을 낸 결과 암호화된 데이터의 평균 CC값은 0.0063을 보여주었으며, 잘못된 키를 가지고 복원을 시도했을 경우 평균 CC 값은 0.0038의 값을 확인할 수 있었다. 암호화 성능의 판단 기준인 0.25보다 현저히 낮은 것으로 나타났다. 이는 복호화 이미지와 원본 이미지 간의 상관관계가 거의 존재하지 않음을 의미하며, 다중 이미지 암호화에서도 본 기법의 우수한 암호화 성능을 뒷받침한다.

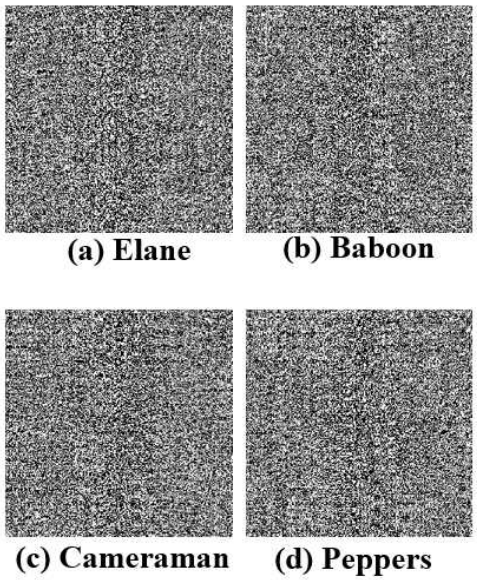

그림 8. 잘못된 암호키로 데이터 복원
Fig. 8. Decryption with an Incorrect Key.

또한 암호 키 공간(Key Space) 분석을 통해 암호키의 강도를 분석해 보았다. 본 연구에서 사용된 이차원 이미지 256×256 기준 하다마드 행렬의 4개 코드 중 하나를 선택하고, x, y축에 대해 FFT 경로 선택, 트위들 팩터 및 비트 시프트를 각각 독립적으로 적용한다, 따라서 전체 키 공간은 $K=4\times(8\times8)\times(256\times256)\times(8\times8)\approx2^{30}$ 수준으로 현재 구현에서는 약 10.7억 개의 서로 다른 키 조합을 생성할 수 있다. 하지만 현재 구현에서는 계산 복잡도를 고려하여 이미지 전체에 동일한 암호키를 적용했지만, 제안된 구조는 이차원 이

미지 배열에서 각 행 및 열에 서로 다른 FFT 경로, 트위들 팩터 및 비트 시프트를 독립적으로 적용할 수 있도록 설계되었다. 따라서 데이터의 크기가 증가할수록 선택 가능한 키 조합의 수가 함께 증가하며, 이에 따라 전체 키 공간 역시 지수적으로 확장될 수 있다. 즉, 제안 기법은 데이터 크기와 키 적용 방식에 따라 더 큰 키 공간을 확보할 수 있는 구조적 특성을 가진다.

5. 결 론

본 논문에서는 선행 연구에서 제안된 FFT 암호화 알고리즘을 기반으로, 하다마드 코드를 적용하여 다중 이미지를 효과적으로 암호화 및 복호화하는 기법을 제안하였다. 또한, 실험 결과를 바탕으로 제안된 방식이 암호화 데이터의 보안성능 및 안전성을 분석하였다. FFT 버터플라이 알고리즘의 경로 번호와 비트 시프트, 변형된 트위들 팩터를 기본 암호키로 사용하였고, 여기에 하다마드 코드를 각 이미지에 적용함으로써 코드 값이 추가적인 암호키처럼 사용되는 것과 동시에 다중 이미지를 암호화할 수 있는 방법을 제안하고 검증하였다. 이는 하다마드 코드를 이용한 다중 이미지 합성에서 원본 데이터에 더미 데이터 또는 워터마킹 데이터를 같이 합성하여 원본 데이터의 무결성을 확인 및 암호화 복잡성을 더욱 높일 수 있을 거라 판단된다. 또한 본 논문에서 사용되는 FFT 버터플라이 암호화 알고리즘은 빠른 속도뿐만 아니라 데이터가 커질수록 여러 경로에 암호키 세트를 적용할 수 있는 특징을 가지며 간단한 정수값으로 구성되는 특징을 가진다. 하다마드 코드 또한 Bit 수를 증가시켜 더욱 많은 코드를 구성하여 다중 이미지를 중첩할 수 있으므로 견고하고 효율적인 암호화 알고리즘을 수행할 수 있다. 제안된 방식을 이용해 암호화된 데이터가 충분한 성능을 가지는지 CC를 이용해 분석해 보았으며 기준 0.25 대비 0.0063으로 우수한 성능을 보여주고 있다고 판단된다.

본 연구를 통해 다중 이미지를 효율적으로 암호화 하기 위해 FFT 버터플라이 암호화 알고리즘에 하다마드 코드의 직교성을 이용하였다. 성능 분석을 통해 암호화된 데이터의 가능성을 충

표 1. 이미지 데이터에 사용된 암호키 및 CC 분석
Table 1. Encryption Keys and CC Analysis for Image Data

	FFT / 그림	Elane		Baboon		Cameraman		Peppers	
		행	열	행	열	행	열	행	열
암호화	그림 6 (a) - (d)	경로 2	경로 3	경로 2	경로 3	경로 2	경로 3	경로 2	경로 3
		하다마드 코드 1		하다마드 코드 2		하다마드 코드 3		하다마드 코드 4	
		2 BS	5 BS	2 BS	5 BS	2 BS	5 BS	2 BS	5 BS
		M'=90	M'=150	M'=90	M'=150	M'=90	M'=150	M'=90	M'=150
		CC = 0.0054		CC = 0.0117		CC = 0.0025		CC = 0.0055	
잘못된키	그림 8 (a) - (d)	경로 3	경로 5	경로 3	경로 5	경로 3	경로 5	경로 3	경로 5
		하다마드 코드 4		하다마드 코드 3		하다마드 코드 2		하다마드 코드 1	
		3 BS	2 BS	3 BS	2 BS	3 BS	2 BS	3 BS	2 BS
		M'=45	M'=220	M'=45	M'=220	M'=45	M'=220	M'=45	M'=220
		CC = 0.0013		CC = 0.0041		CC = 0.0060		CC = 0.0036	

분히 확인하였으며, 본 논문에서 제안한 알고리즘은 차세대 데이터 보안 기술로서의 높은 잠재력을 지니고 있으며, 보안성이 요구되는 공공 및 민간 기관의 데이터 암호화 인프라에 폭넓게 적용 가능할 것으로 기대된다.

참 고 문 헌

[1] P. Refregier, B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding”, Optics Letter, 20, pp.767-769, Jan. 1, 1995. DOI: https://doi.org/10.1364/OL.20.000767

[2] D. Kong, L. Cao, G. Jin, B. Javidi, “Three-dimensional scene encryption and display based on computer-generated holograms”, Applied Optics, 55(29), pp.8296-8300, Oct. 7, 2016.
DOI: https://doi.org/10.1364/AO.55.008296

[3] B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, MS. Millán, et al. “Roadmap on optical security”, Journal of Optics, 18(8):083001, Jul. 22, 2016.
DOI:/10.1088/2040-8978/18/8/083001

[4] Y. Zhang, B. Wang, “Optical image encryption based on interference”, Optics Letter, 33(21), pp.2443-2445, Oct. 21, 2008.
DOI: https://doi.org/10.1364/OL.33.002443

[5] G. Unnikrishnan, J. Joseph, K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domain”, Optics Letter, 25(12), pp.887-889, Jun. 15, 2000.
DOI: https://doi.org/10.1364/OL.25.000887

[6] Y. Zhou, K. Panetta, S. Agaian, “Image encryption using discrete parametric cosine transform”, 2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers, IEEE, pp.395 - 399, Nov, 2009.
DOI: /10.1109/ACSSC.2009.5469838

[7] J. Song, Y. H. Lee, “Optical image encryption using different twiddle factors in the butterfly algorithm of fast Fourier transform”, Optics Communications, 485, 126707, Apr. 15, 2021.
DOI: /10.1016/j.optcom.2020.126707

[8] J. Song, Y. H. Lee, “Study on Application of Encryption Mask in Butterfly Algorithm of fast Fourier Transform”, Journal of Appraisal Software Assessment and Valuation, 20(4), pp.103-116, Dec. 20, 2024.
DOI: /10.29056/jsav.2024.12 .11

[9] X. He, H. Tao, Z. Jiang, Y. Kong, S. Wang, and C. Liu, “Single-shot Optical Multiple-image Encryption by Jointly Using Wavelength Multiplexing and Position Multiplexing”, Applied Optics, 59(1), pp.9-15, Jan. 1, 2020.
https://doi.org/10.1364/AO.59.000009

[10] I. H. Lee, M. Cho, “Double Random Phase Encryption using Orthogonal Encoding for Multiple-image Transmission”, Current Optics and Photonics, 18(3), pp.201-206, June. 3, 2014.
DOI: /10.3807/JOSK.2014.18.3.201

[11] Y. H. Kim, J. H. Song, I. Moon, Y. H. Lee, “Interference-based multiple-image encryption using binary phase masks“, Optics and Lasers in Engineering. 107, pp.281 - 287, Apr. 13, 2018.
DOI: /10.1016/j.optlaseng.2018.01.012

[12] H. Tian, X. Zhuang, A. Yan, H. Zhang, “A novel multiple-image encryption with multi-petals structured light”, Scientific Reports, 14, 19559, Aug. 22, 2024.
DOI: /10.1038/s41598-024-70425-3

[13] Y. Wang, X. Liu, Z. Li, et al, “Multiple images simultaneous encryption and decryption via deep-learning assisted interferenceless coded aperture correlation holography”, Optics Communications, 573, 131018, Dec. 15, 2024.
DOI: /10.1016/j.optcom.2024.131018

[14] J. Cooley, J. Tukey, “An algorithm for machine computation of complex Fourier series”, Mathematics of Computation. 19, pp.297-301, May. 1, 1965.
DOI: https://doi.or g/10.2307/2003354
[15] R. N. Bracewell, “The Fourier Transform and Its Applications”, third ed., McGraw Hill, ISBN:9780073039381, 1999.
[16] Y. Zhou, W. Cao, L. Liu, S. Agaian, C.L.P. Chen, “Fast Fourier transform using matrix decomposition”, Information Science, 291, pp.172 - 183, Jan. 10, 2015.
DOI: /10.1016/j.ins.2014.08.022
[17] J. J. Sylvester, “Thoughts on Inverse Orthogonal Matrices, Simultaneous Sign Successions, and Tessellated Pavements in Two or More Colours”, Philosophical Magazine, 34(232), pp.461-475, May. 13 2009.
DOI: /10.1080/147864467 08639914
[18] D. Sundararajan, M. O. Ahmad, “Fast Computation of the Discrete Walsh and Hadamard Transforms”, IEEE Transactions on Image Processing, 7(6), pp.898-904, Jun. 1998.
DOI: https://doi.org/10.1109/83.679439
[19] M. N. Islam, M. S. Alam, “Optical encryption and multiplexing of personal identification information using orthogonal code”, Optical Engineering, 45(9), 098201, Sep. 1, 2006.
DOI: https://doi.org/10.1117/1.2 354449
[20] M. Udovičić, K. Baždarić, L. Bilić-Zulle, M. Petrovečki, “What we need to know when calculating the coefficient of correlation?”, Biochemia Medica, pp.10-15, Jun. 15, 2007.
DOI: http://doi.org/10.11613/BM.2007.002.
[21] A.G. Asuero, A. Sayago, A.G. Gonzalez, “The correlation coefficient: An overview”, Critical Reviews in Analytical Chemistry, 36 41-59, Jan. 12, 2007.
DOI: /10.1080/10408340500526766

저 자 소 개

송재훈(Jae-Hun Song)

2011.8 홍익대학교 전자전기공학과 졸업
2011.9-2017.8 성균관대학교 전자전기컴퓨터공학과 석사, 박사
2019.3-2025.2 : 성균관대학교 IT융합연구원 선임연구원
2025.3-현재 : 경기과학기술대학교 컴퓨터모바일융합과 조교수
<주관심분야> 정보보안, 이미지 프로세싱, 홀로그램 광암호화