JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 31 No. 8, pp. 73-85, August 2026
https://doi.org/10.9708/jksci.2026.31.08.073

ROB Segmentation-Based Selective Encryption with Random Pattern Fragmentation for Spine X-ray Images

Cheolhun Hwang*, Geon-Yun Shin**

*Student, Dept. of Translational-Clinical Medicine, Gachon University, Incheon, Korea
**Professor, School of Computer Engineering & Applied Mathematics, Hankyong National University, Anseong, Korea

[Abstract]

This study proposes a region-of-background (ROB)-oriented selective encryption framework for protecting the PixelData of de-identified Digital Imaging and Communications in Medicine (DICOM) spine X-ray images. A convolutional neural network (CNN) detects the ROB, and its complementary region is defined as the region of interest (ROI). AES-256-GCM is applied to the ROI, AES-128-GCM to the ROB, and random pattern fragmentation (RPF) with 64×64 blocks is used to obscure regional boundaries. The framework was evaluated using 1,200 cervical, lumbar anteroposterior, and lumbar lateral images from the Cervical Spine X-ray Atlas and BUU-LSPINE datasets. The ROB segmentation model achieved a Dice similarity coefficient of 95.67(±0.43)% and an ROI-to-ROB error rate of 1.17(±0.25)%. The encrypted images showed an NPCR of approximately 99.61%, entropy values close to 8.0, and mean absolute adjacent-pixel correlations of 0.00245–0.00253. The mean processing time was 36.27 ms/MP, and all reconstructed images achieved a 100% SHA-256 hash match. The results suggest that the proposed framework may reduce computational burden while maintaining statistical security indicators comparable to previous methods. This study was limited to de-identified two-dimensional spine X-ray images and operational ROB reference masks; DICOM header de-identification and practical key-management implementation were beyond its scope.

▸ **Key words**: Medical image encryption, X-ray encryption, Selective encryption, Random Pattern Fragmentation, Deep learning segmentation

• First Author: Cheolhun Hwang, Corresponding Author: Geon-Yun Shin
*Cheolhun Hwang (qewqsa@gachon.ac.kr), Dept. of Translational-Clinical Medicine, Gachon University
**Geon-Yun Shin (gunyoon.shin@hknu.ac.kr), School of Computer Engineering & Applied Mathematics, Hankyong National University
• Received: 2026. 05. 26, Revised: 2026. 07. 16, Accepted: 2026. 07. 23.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

[요 약]

디지털 의료영상 및 통신(Digital Imaging and Communications in Medicine, DICOM) 기반 X-ray 영상의 안전한 저장과 전송을 위해, 본 연구에서는 배경영역(Region of Background, ROB) 기반 선택적 암호화 프레임워크를 제안하였다. 합성곱 신경망(Convolutional Neural Network, CNN)으로 ROB를 탐지하고, 그 보완 영역을 관심영역(Region of Interest, ROI)으로 정의하였다. 이후 ROI에는 AES-256-GCM, ROB에는 AES-128-GCM을 적용하고, 영역 경계를 은닉하기 위해 64 크기 블록 기반 무작위 패턴 분할(Random Pattern Fragmentation, RPF)을 적용하였다. Cervical Spine X-ray Atlas와 BUU-LSPINE 데이터셋의 경추, 요추 전후면, 측면 영상 총 1,200장을 평가한 결과, ROB 분할 모델은 주사위 유사도 계수(Dice Similarity Coefficient) 95.67(±0.43)%와 ROI-to-ROB 오류율 1.17(±0.25)%를 보였다. 암호화 영상은 약 99.61%의 픽셀 변화율(Number of Pixels Change Rate, NPCR), 8.0에 근접한 엔트로피, 0.00245–0.00253의 인접 픽셀 상관계수를 나타냈다. 평균 처리시간은 36.27 ms/MP였으며, 모든 영상에서 SHA-256 해시 일치율 100%를 확인하였다. 제안 방법은 선행 연구와 유사한 수준의 통계적 보안 지표를 유지하면서 계산 부담을 줄일 수 있는 가능성을 보였다. 다만 본 연구는 비식별화된 2차원 척추 X-ray 영상과 운영적 ROB 기준 마스크를 대상으로 하며, DICOM 헤더 비식별화 및 키 관리시스템 구현은 연구 범위에서 제외하였다.

▸ **주제어**: 의료 영상 암호화, X-ray 암호화, 선택적 암호화, 무작위 패턴 파편화, 딥러닝 세그멘테이션

I. Introduction

임상 현장에서는 영상 정보를 활용한 인공지능 연구가 빠르게 증가하고 있으며, 이러한 연구 성과를 실제 진료 환경에 도입하기 위한 웹 기반 AI 플랫폼, PACS 연동 시스템, 원격 판독 및 임상 보조 서비스가 활발히 개발되고 있다. 디지털 의료영상은 진단, 예측, 추적 관찰, 임상 연구의 핵심 자료로 활용되지만, 환자 식별 정보와 질병 관련 민감 정보를 동시에 포함하기 때문에 정보보호 관점에서 높은 보안 수준이 요구된다.

AI 기반 임상 플랫폼은 병원 내부망, PACS, 분석 서버, 데이터베이스, 외부 연동 모듈 등 여러 구성 요소와 연결되므로 데이터 전송 및 저장 과정에서 비인가 접근, 영상 탈취, 변조, 재식별 공격의 위험이 존재한다.

X-ray 영상은 접근성이 높고 검사 비용이 낮으며, 척추측만증, 압박골절, 퇴행성 질환 등 다양한 질환 평가에 널리 사용된다. X-ray 영상을 기반으로 자동 계측, 질환 분류, 임상 의사결정 보조 모델이 개발되고 있으며, 이러한 AI 모델을 임상 환경에 적용하기 위해 영상 전송 및 분석 결과 관리가 필수적으로 요구된다. 그러나 환자 영상이 분석 서버로 이동하거나 장기간 저장되는 구조에서는 사이버 공격에 의한 영상 탈취 가능성이 증가한다. 따라서 단순한 통신 구간 암호화뿐 아니라 영상 파일 자체에 대한 보안 기법이 필요하다[1][2].

의료영상 보안을 위해 혼돈 이론 기반 암호화 기법이 널리 연구되어 왔다[3][4]. 혼돈 기반 암호화는 초기 조건 민감성(high sensitivity), 큰 키 공간(large key spaces), 높은 무작위성(unpredictability)을 바탕으로 픽셀 위치와 값을 변화시켜 통계적 공격에 강한 특성을 보인다. 그러나 보안 강도를 높이기 위해 고차원 혼돈 시스템이나 반복 연산을 사용하는 경우 계산 복잡도가 증가하고, 실시간 임상 플랫폼에 적용하기 어려운 문제가 발생한다[5]. 이에 따라 진단적으로 중요한 영역에 강한 암호화를 적용하고 나머지 영역에는 상대적으로 경량화된 처리를 수행하는 선택적 암호화 기법이 제안되었다.

기존 선택적 암호화 연구는 주로 명시적인 관심영역(ROI) 추출을 기반으로 한다. 그러나 X-ray 영상에서 ROI는 촬영 프로토콜, 해부학적 부위, 임상 목적, 장비 특성에 따라 달라질 수 있다. 이로 인해 특정 데이터셋 또는 특정 진단 과제에 맞춘 ROI 추출 모델은 다른 X-ray 도메인으로 확장될 때 일반화 성능이 제한될 수 있다. 반면 X-ray 영상의 배경 영역은 일반적으로 어둡거나 정보가 거의 없는 영역으로 나타나며, 촬영 조건이 달라져도 비교적 일관된 특성을 보인다. 본 연구는 이러한 특성에 주목하여 ROI를 직접 정의하는 대신 진단 정보가 상대적으로 적은 배경 영역(Region of Background, ROB)을 먼저 탐지하고, 그

보완 영역을 진단 정보 영역으로 활용하는 ROB 지향 선택적 암호화 전략을 제안한다.

본 연구의 목적은 임상 플랫폼 환경에서 DICOM 기반 X-ray 영상 자체의 보안성을 향상시키는 것이다. 제안하는 프레임워크는 ROB 기반 선택적 AI 모델, 영역 적응형 암호화, 무작위 패턴 분할(random pattern fragmen-tation, RPF)을 결합한다. ROB에는 경량 암호화를 적용하여 처리 속도를 확보하고, 진단 정보가 포함된 영역(Region of Interest, ROI)에는 강한 암호화를 적용하여 환자의 의료 정보에 대한 기밀성을 보장한다. 또한 영역별 암호화에서 발생할 수 있는 경계 정보 노출과 구조 기반 공격을 억제하기 위해 RPF를 적용한다.

본 연구의 주요 기여는 다음과 같다. 첫째, X-ray 데이터셋 전반에서 일반화 가능한 ROB 지향 영역 분할 전략을 제안한다. 둘째, 영역 특성에 따라 암호화 강도를 달리하는 영역 적응형 암호화 구조를 제시한다. 셋째, RPF를 통해 ROI/ROB 경계를 은닉하고 구조 기반 공격에 대한 저항성을 높인다. 넷째, 공개 척추 X-ray 데이터셋을 이용하여 보안성, 복원성, 처리 효율성을 정량적으로 검증한다.

본 논문의 구성은 다음과 같다. 2장에서는 혼돈맵 기반 의료영상 암호화, 선택적 암호화 및 RPF와 관련된 선행 연구를 검토한다. 3장에서는 ROB 기준 마스크 생성과 CNN 기반 영역 분할, ROI와 ROB의 차등 암호화, RPF 기반 공간구조 은닉 및 복호화 절차로 구성된 제안 프레임워크를 설명한다. 4장에서는 공개 척추 X-ray 데이터셋을 이용하여 ROB 탐지 및 오분류 영향, RPF 적용 효과, 암호화 보안 성능과 처리 효율을 평가하고 기존 암호화 방법과 비교한다. 마지막으로 5장에서는 연구 결과를 요약하고, 제안 방법의 한계와 향후 연구 방향을 제시한다.

II. Preliminaries

1. Related works

1.1 Chaos-based medical image encryption

혼돈 이론 기반 암호화는 강한 무작위성, 초기 조건 민감성, 예측 불가능성으로 인해 의료영상 보안 분야에서 활발히 연구되어 왔다[3][4]. 혼돈 맵 기반 암호화는 픽셀 위치를 무작위로 섞는 혼돈화(confusion)와 픽셀 값을 변화시키는 확산(diffusion)을 통해 영상 데이터에 대한 통계 분석 공격을 어렵게 만든다. 이러한 접근은 혼돈 기반 순열과 확산 구조가 영상 암호화에 활용될 수 있음을 보여주지만, 전체 영상에 반복적인 변환을 적용하는 경우 영상 크기와 반복 횟수에 따라 계산 부담이 증가할 수 있다[5][6]. 로지스틱 맵(Logistic map), 헤논 맵(Henon map), 로렌츠 맵(Lorenz map), 베이커 맵(Baker map) 등을 활용한 다양한 방법이 제안되었으며, 여러 혼돈 시스템을 결합하거나 다단계 무작위화를 적용하여 보안성과 복호화 정확도를 동시에 향상시키고자 하였다[7].

최근에는 선형 함수 대신 거듭제곱 및 삼각함수 기반 항을 포함한 고차원 맵이 연구되었으며[8], DNA 시퀀싱, 웨이블릿 변환, 생체 인증과 결합한 의료영상 암호화 기술도 제안되었다[9][10][11]. 그러나 고차원 혼돈 시스템은 반복 횟수와 계산량을 증가시키며, 처리 속도 저하와 자원 소모 증가를 초래한다. 따라서 실제 임상 환경에서 대량의 DICOM 영상을 빠르게 처리하기 위해서는 충분한 보안성을 유지하면서도 계산 효율이 높은 경량 혼돈 모델과 선택적 암호화 구조가 필요하다.

1.2 Henon map-based chaos encryption

Zhao 등은 기존 혼돈 시스템의 복잡성과 계산 비용 증가 문제를 해결하기 위해 수정된 헤논 맵을 이용한 블록 기반 영상 암호화 방법을 제안하였다[12]. 이 방법은 입력 영상을 고정 크기 블록으로 나누고, 혼돈 시퀀스를 이용하여 블록 위치를 섞은 뒤 각 블록 내부 픽셀 값을 확산한다. 또한 가변 길이 비밀키를 도입하여 키 공간을 확장하고 전수조사 공격에 대한 저항성을 높였다.

수정된 헤논 맵은 비선형성과 키 민감도를 높이기 위해 반복적 매개변수 갱신 구조를 사용한다. 이는 로지스틱 맵 기반 단순 기법에서 나타나는 예측 가능성과 제한된 키 공간 문제를 보완한다[13]. 3D Cat Map 기반 방법[14]과 비교할 때 Henon 기반 모델은 블록 기반 처리 구조 덕분에 구조가 단순하고 처리 속도가 빠른 장점이 있다.

1.3 Random pattern partitioning

전통적인 암호화만으로는 패턴 복원이나 ROI 추론과 같은 구조 기반 공격을 완전히 방지하기 어렵다. 이를 보완하기 위해 무작위 패턴 분할(RPF)이 도입되었다. RPF는 영상을 임의의 블록 또는 조각으로 나누고 공간적으로 재배열함으로써 영상의 전역 및 국소 구조를 식별하기 어렵게 만든다. 블록 스크램블링 기법은 영상을 고정 크기 블록으로 분할한 뒤 혼돈 키 시퀀스에 따라 블록 순서를 무작위로 재배열하여 시각적 해석을 방해한다[15].

Liu 등은 혼돈 순열 행렬과 DNA 시퀀스를 결합하여 픽셀의 공간적 상관성을 감소시키고 통계적 공격에 대한 저항성을 높이는 영상 암호화 알고리즘을 제안하였다[16].

Fan과 Ding은 단일 암호화 기법에 의존하지 않고, 자기동기식 혼돈 스트림 암호, 2차원 이산 웨이블릿 변환 및 아널드 매핑을 결합한 복합 영상 암호화 방법을 제안하였다[17]. 이와 같은 다단계 순열 및 재배열 기법은 암호화된 영상의 공간적 구조를 추가로 은닉할 수 있다. 본 연구에서는 이러한 개념을 바탕으로 암호화된 ROI와 ROB 영역을 블록 단위로 재배열하는 RPF를 적용하여 영역 경계와 원래의 공간적 배치를 은닉하였다.

1.4 ROI and ROB-based selective medical image encryption

최근 의료영상 보안 분야에서는 전체 영상을 균일하게 암호화할 때 발생하는 계산 복잡도와 실시간 적용성 문제를 해결하기 위해 ROI 기반 선택적 암호화가 주요 연구 방향으로 제시되고 있다. Jamal 등은 의료영상에서 진단적으로 중요한 ROI를 자동 추출하고, 해당 영역에 혼돈 기반 S-박스(Chaotic S-boxes)와 스크램블링 기법을 선택적으로 적용하는 암호화 프레임워크를 제안하였다[18]. 이 방법은 배경 영역의 계산 부담을 줄이면서 진단 관련 영역의 보안 수준을 유지하여 대규모 의료영상 환경에서 효율적인 암호화와 복호화를 가능하게 한다.

III. The Proposed Scheme

본 장에서는 척추 X-ray 영상의 PixelData를 보호하기 위한 ROB 지향 영역 적응형 선택 암호화 프레임워크를 제시한다. 제안 프레임워크는 Fig. 1과 같이 (1) 연구 범위 (2) 보안 가정 설정, (3) DICOM 영상 전처리, (4) ROI와 ROB 영역 생성, (5) 영역별 차등 암호화, (6) RPF를 이용한 공간구조 은닉, (7) 복호화 및 원본 영상 복원의 순서로 수행된다.

본 연구는 X-ray 영상 전체에 동일한 암호화 알고리즘을 적용하는 대신, 촬영 정보가 존재하는 영역(ROI)과 촬영 정보가 거의 존재하지 않는 배경 영역(ROB)을 분리하고 서로 다른 암호화 강도를 적용하면 영상 보호 수준을 유지하면서도 연산 자원과 처리 시간을 크게 절감하는 것을 목표로 한다.

혼돈맵 기반 영상 암호화는 전체 픽셀에 동일한 confusion 및 diffusion 연산을 반복적으로 적용하는 방식이 일반적이다. 따라서 제안 방법의 차별점은 새로운 단일 암호화 알고리즘이 아닌 영상 영역의 특성에 따라 복수의 표준 암호화 구성을 선택적으로 적용하는 다계층 암호화 구조라는 데 있다.

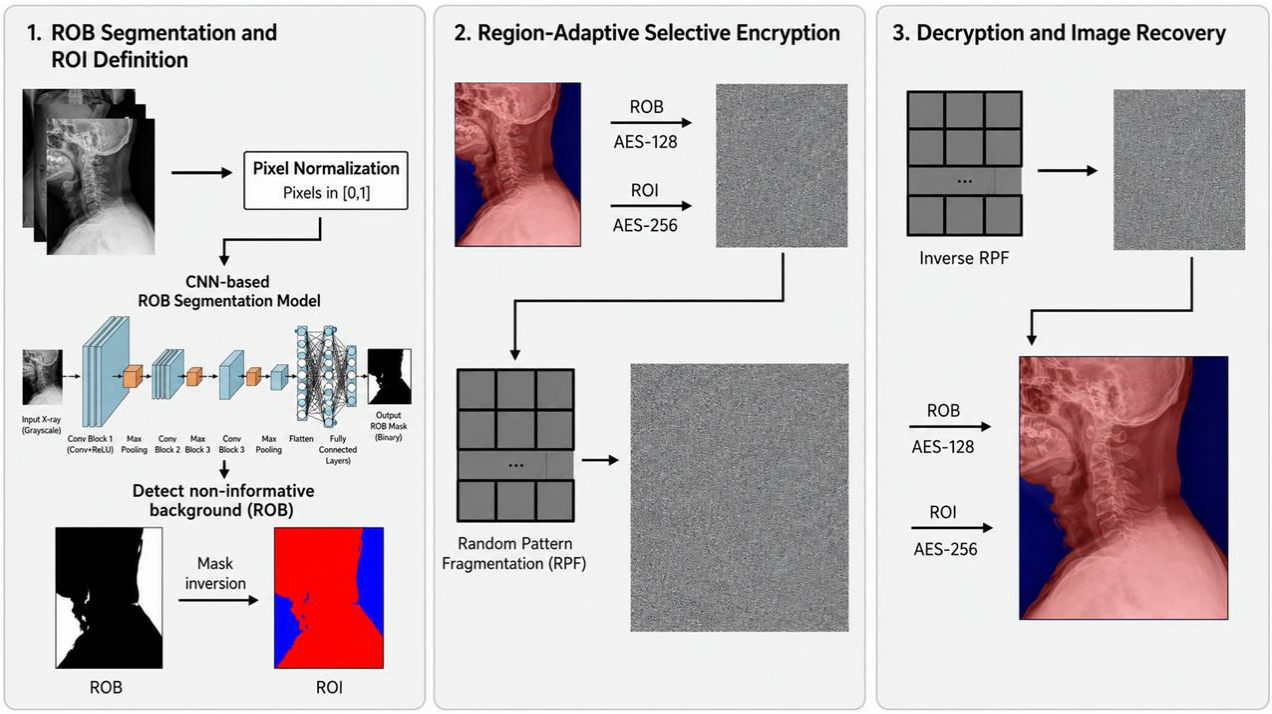

Fig. 1. Overview of the Proposed ROB Segmentation-Based Selective Encryption Framework

1. Research Scope and Design Rationale

DICOM 영상은 영상 픽셀뿐 아니라 환자 이름, 환자 식별번호, 검사일, 검사기관, 촬영 부위 및 검사 설명과 같은 다양한 정보를 포함한다. 본 연구는 DICOM 보안의 모든 요소를 하나의 알고리즘으로 해결하는 것을 목적으로 하지 않으며, 비식별화가 완료된 DICOM 객체의 PixelData를 보호하는 영상 암호화 알고리즘에 연구 범위를 한정한다. 의료영상의 연구용 추출 또는 기관 간 공유 과정에서는 기관별 데이터 관리 규칙에 따라 Patient Name, Patient ID 및 Accession Number 등의 직접 식별정보가 제거되거나 연구용 식별자로 변환된다. 또한 Study Description, Body Part, Study Date 등과 같은 정보는 연구 목적, 제공 범위 및 기관 정책에 따라 삭제, 일반화 또는 대체될 수 있다. 따라서 제안 프레임워크에 입력되는 DICOM 객체는 이러한 비식별화 절차가 선행된 것으로 가정한다.

제안 프레임워크는 다음 세 가지 설계 원칙을 따른다. 첫째, 환자 촬영 정보가 포함된 영역과 촬영 정보가 없는 배경 영역을 구분한다. 둘째, 두 영역 모두 암호화하되 영상 정보량과 보호 우선순위에 따라 암호화 강도를 차등 적용한다. 셋째, 영역별 암호화 이후에도 남을 수 있는 ROI와 ROB의 경계 및 공간적 배열을 RPF로 재배열한다.

2. Threat Model and Security Assumptions

제안 프레임워크의 보안성을 평가하기 위해 보호 대상, 공격자 능력 및 신뢰 대상을 다음과 같이 정의한다.

보호대상은 환자의 해부학적 구조가 포함된 X-ray PixelData, ROI와 ROB의 공간적 위치 및 경계, ROI와 ROB에 사용되는 암호화 키, RPF 블록 순열을 생성하기 위한 키 또는 초기값, ROI/ROB 마스크와 복호화에 필요한 보안 메타데이터이다. 비식별화된 DICOM 헤더에 남아 있는 촬영 부위, 영상 크기 및 영상 표현 정보는 본 연구의 직접적인 기밀성 보호 대상에 포함하지 않는다.

본 연구의 위협 모델은 공격자가 저장소, 연구 데이터베이스에서 X-ray 영상 정보를 탈취하려는 상황을 가정한다. 암호화 키를 생성하고 저장하는 키 관리시스템, 암호화 및 복호화가 수행되는 단말, 암호화 키를 인가된 사용자에게 전달하는 보안 채널은 신뢰 된 것으로 가정한다. 또한 암호화 또는 복호화 단말 자체가 완전히 침해된 경우, 메모리 덤프, 전력 분석 및 시간 분석 등의 물리적 사이드채널 공격, 키 관리 서버가 침해되어 원본 키가 유출된 경우, 인가된 사용자가 복호화된 영상을 악의적으로 유출하는 경우는 본 연구 범위에서 제외한다.

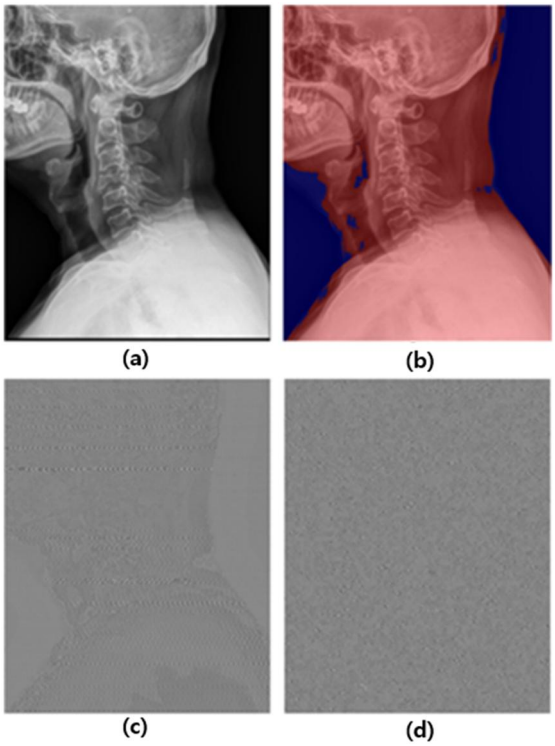

Fig. 2. Step-by-step encryption results

3. DICOM PixelData Preprocessing

본 연구는 DICOM 메타데이터 전체에 대한 비식별화 알고리즘을 제안하는 것이 아니라, 비식별화 이후에도 환자의 해부학적 구조를 포함하는 PixelData를 보호하는 데 목적이 있다.

X-ray 영상은 Photometric Interpretation에 따라 동일한 픽셀값이 서로 다른 밝기로 표시될 수 있다. MONOCHROME2에서는 일반적으로 낮은 픽셀값이 어둡게, 높은 픽셀값이 밝게 표시되며, MONOCHROME1에서는 그 반대로 표시된다. 따라서 ROB 분할에 앞서 Photometric Interpretation을 확인하고, MONOCHRO-ME2 영상을 기준으로 동일하게 변환한다.

영상 크기가 서로 다른 경우에는 원본 종횡비를 유지하면서 긴 변이 최대 512 픽셀이 되도록 축소한다. 짧은 변은 동일한 비율로 조정한다. 영상 정보는 intensity scaling을 통해 0과 1 사이로 정규화한다.

4. Operational Definitions of ROI and ROB

본 연구에서 사용하는 ROI는 병변, 척추체 또는 특정 해부학적 구조를 전문가가 지정한 임상적 관심영역을 의미하지 않는다. 본 연구의 ROI는 X-ray 조사에 의해 환자 신체, 연부조직, 골 구조, 촬영 마커 및 기타 촬영 정보가 영상에 표현된 촬영 유효영역을 의미한다. 반면 ROB는

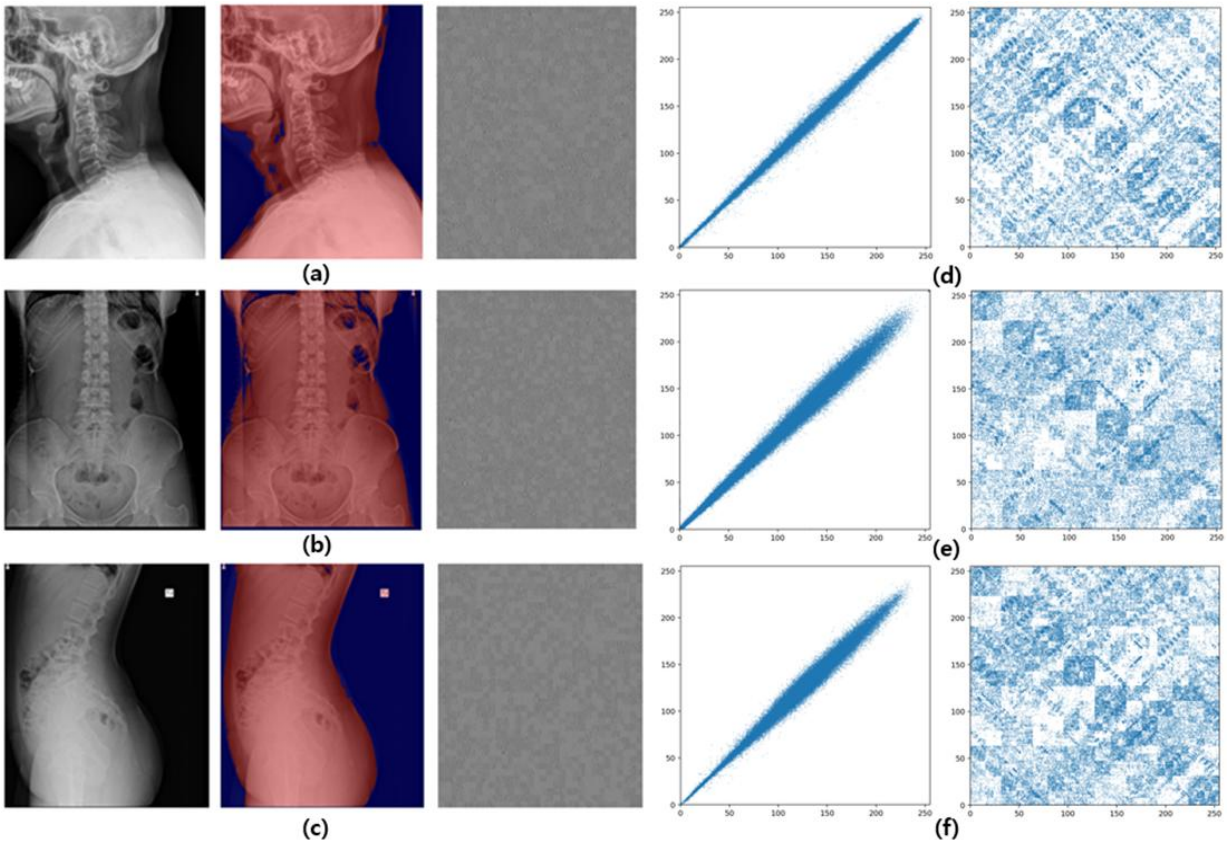

Fig. 3. ROB segmentation-based selective encryption results and adjacent-pixel correlation analysis for different spine X-ray views. (a) Cervical spine X-ray, (b) lumbar AP X-ray, and (c) lumbar LA X-ray images show the original image, segmentation, and encrypted image. (d)-(f) show the adjacent-pixel correlation distributions before and after encryption for each X-ray.

X-ray 촬영 정보가 거의 존재하지 않으며 영상 외곽에서 검은색 또는 낮은 신호강도로 나타나는 배경 영역으로 정의한다.

본 연구에 사용된 마스크는 영상의 신호강도와 외곽 배경 특성을 이용하여 생성한 operational reference mask이다. 따라서 본 연구에서 보고하는 ROB Dice similarity coefficient는 임상 병변 분할 정확도가 아니라, 제안한 배경 정의 규칙을 CNN 모델이 서로 다른 X-ray 영상에서 얼마나 안정적으로 재현하는지를 나타낸다. 보안 관점에서 환자 촬영 영역이 ROB로 잘못 분류되는 오류는 배경 일부가 ROI로 분류되는 오류보다 중요하다. 이에 따라 불확실한 픽셀을 ROI로 포함하는 보수적인 판정 방식을 적용한다. 이는 저선량, 과소노출, 촬영 마커, 주변 연부조직 또는 경계가 불분명한 영상에서 촬영 정보가 ROB로 잘못 분류되는 위험을 줄인다. 그 결과 ROB 분류가 불확실한 영역은 계산 효율보다 정보 보호를 우선하여 AES-256 적용 영역으로 처리된다.

픽셀 강도와 외곽 연결성만을 이용한 규칙 기반 처리로도 operational ROB를 구분할 수 있으나, 본 연구에서는 향후 다양한 영상분석 모델과의 통합 가능성을 고려하여 CNN 기반 픽셀 단위 분할 구조를 적용하였다. 임상 플랫폼에서는 척추체, 병변, 촬영 마커 또는 기타 보호 대상 영역을 탐지하는 여러 객체 탐지 및 분할 모델이 함께 사용될 수 있으며, 각 모델의 결과는 bounding box, polygon 또는 좌표 기반 JSON과 같이 서로 다른 형식으로 생성될 수 있다. 제안 프레임워크에서는 여러 영상분석 모델의 출력 결과를 공통된 픽셀 단위 보호 마스크로 변환하고, 이를 ROB 분할 결과와 결합하여 최종 ROI/ROB 암호화 정책 마스크를 생성할 수 있다. 이를 통해 객체 탐지 결과를 모델별 평문 JSON으로 별도 전송하기보다, 영상 암호화 과정에서 사용하는 하나의 공간 마스크 표현으로 통합할 수 있다는 점에 확장 가능성을 고려하였다.

5. Region-Adaptive Pixel Encryption

원본 X-ray PixelData를 ROI와 ROB의 각 영역에 속하는 원본 픽셀은 행 우선 순서로 추출하여 각각의 1차원 픽셀 스트림으로 변환한다. 16-bit DICOM 영상에서는 각 픽셀을 원본 Transfer Syntax의 바이트 순서에 따라

2byte 값으로 직렬화한다. ROI와 ROB의 픽셀 수가 AES 블록 크기의 배수가 아니더라도 AES-GCM은 임의 길이의 데이터 처리가 가능하므로 별도의 PKCS 패딩(padding)을 적용하지 않는다. ROB 암호화에는 128-bit 키를 사용하고 ROI 암호화에는 256-bit 키를 사용한다. 각 영역에는 영상마다 독립적으로 생성된 96-bit nonce를 사용하며, 제안 프레임워크에서는 재사용하지 않음을 가정하였다. 키 분배는 본 연구의 암호화 알고리즘 외부에 위치한 보안 키 관리시스템이 담당하는 것으로 가정한다.

ROI와 ROB에 서로 다른 AES 구성을 적용하더라도 암호문만으로 사용된 키 길이를 직접 구분할 수 없으며, 제안 방법의 안전성은 암호화 알고리즘을 숨기는 것에 의존하지 않는다. 영역별 구분의 주된 목적은 동일한 X-ray 영상 내부에서 보안 강도를 계층적으로 구분하는 것이다.

6. Random Pattern Fragmentation

영역별 암호화 이후의 영상에서는 ROI와 ROB 마스크의 형태에 따라 공간적 경계가 남는다. 이러한 경계는 원본 픽셀값을 직접 보여주지는 않지만 환자의 촬영 범위나 영상 외곽 형태에 관한 구조적 단서를 제공할 수 있다. 이를 완화하기 위해 영역별 암호화가 완료된 영상에 RPF를 추가로 적용한다.

영상의 가로 또는 세로 길이가 블록 크기의 배수가 아닌 경우 가장자리 영역은 별도의 잔여 조각(fragment)으로 관리한다. 픽셀값을 추가하거나 제거하지 않으며, 각 조각의 원래 위치와 크기는 역순열을 위해 보호된 보안 메타데이터로 관리한다.

RPF 순열은 로지스틱 맵을 사용하여 순차 배열을 생성한다. 본 연구에서 로지스틱 맵 기반 RPF는 이미 암호화된 블록의 위치를 재배열하여 경계를 추가로 은닉하는 역할만 수행한다. 이러한 구조는 전체 영상에 반복적인 고차원 혼돈 연산을 적용하는 기존 chaos-map 방식과 구별된다. 제안 방법은 표준 AES를 중심 암호 알고리즘으로 사용하고, 저차원 혼돈 순열은 암호문 블록의 후처리 단계로 제한하여 처리 복잡도를 낮춘다.

7. Decryption and Image Reconstruction

복호화는 암호화 과정의 역순으로 수행된다.

첫째, 인가된 복호화 모듈은 키 관리시스템으로부터 키 정보를 조회하고, ROI, ROB, RPF 및 마스크 복호화에 필요한 키를 획득한다. 둘째, 암호화된 마스크를 복호화하고 인증 태그를 검증한다. 마스크 인증에 실패하면 영상 복호화를 중단한다. 셋째, RPF 순열을 재생성하고 역순열을 적용하여 암호화된 조각을 원래 위치로 복원한다. 넷째, 복원된 영역별 암호문 배열에서 ROI와 ROB 영역의 픽셀 스트림 정보를 각각 추출한다. 다섯째, ROI, ROB 픽셀 정보를 각 암호화 정책에 따른 복호화를 적용한다. 여섯째, 복호화된 픽셀 스트림을 원래의 ROI와 ROB 위치에 재배치하여 복원 영상을 생성한다.

혼돈 맵 기반 영상 암호화는 전체 영상에 동일한 혼돈 시퀀스와 픽셀 확산 연산을 적용하거나, 고차원 혼돈계와 반복 연산을 결합하여 보안성을 높이는 경우가 많다. 이러한 방식은 영상 크기가 증가할수록 전체 픽셀에 대한 반복 계산이 증가한다. 제안 방법은 다음 측면에서 기존 접근과 차이가 있다.

첫째, 환자의 촬영 정보가 포함된 영역과 영상 정보가 거의 없는 배경 영역을 먼저 구분한다. 둘째, 두 영역을 모두 보호하지만 ROI에는 AES-256, ROB에는 AES-128을 적용하여 계산량을 적응적으로 배분한다. 셋째, ROI와 ROB의 구분이 영상의 공간적 경계로 나타나는 것을 줄이기 위해 암호화 이후 RPF를 적용한다.

본 연구에서 제안하는 프레임워크는 전체 영상에 높은 복잡도 연산 또는 단일 암호화 적용하는 방법보다 계산 자원과 처리시간을 절감하면서, 기밀성을 유지할 수 있음을 제안하는 목적을 가진다.

IV. Experiment and Results

1. Experimental setup and datasets

본 실험에서는 공개 척추 X-ray 데이터셋인 Cervical Spine X-ray Atlas (CSXA)와 BUU-LSPINE 데이터셋을 사용하였다. CSXA 데이터셋은 전문가 주석이 포함된 4,963장의 경추 X-ray 영상을 포함하며[19], BUU-LSPINE 데이터셋은 방사선 전문의가 주석을 부여한 전후방(AP) 및 측면(LA) 요추 X-ray 3,600건을 포함한다[20].

본 연구에서는 경추, 요추 AP, 요추 LA 각각 400장의 영상을 대상으로 하였다. 경추 영상의 해상도는 864 × 1012 pixels였으며, 요추 AP와 LA 영상의 해상도는 1392 × 2428 pixels였다.

학습, 검증 및 시험 세트로 8:1:1의 비율로 분할하였으며, 서로 다른 난수 시드를 이용한 20회 반복 hold-out 평가를 수행하였다. 각 반복에서는 서로 다른 난수 시드를 이용하여 학습, 검증 및 시험 세트를 다시 구성하였으며, CNN의 가중치도 새로 초기화하여 독립적으로 학습하였다. 본 연구에서 결과 값은 20회 반복에서 산출된 평균과

표준편차이다.

모든 실험은 동일한 하드웨어, 영상 해상도, 반복 횟수, 및 실행 조건에서 수행하였다. 64-bit Windows 운영체제가 설치된 워크스테이션에서 수행하였다. 하드웨어는 13th Gen Intel Core i9-13900K CPU, 32 GB system memory 및 8 GB 전용 그래픽 메모리를 갖는 NVIDIA GeForce RTX 3070 GPU로 구성하였다.

2. ROB Reference Mask Generation and CNN Configuration

본 연구에서 사용한 공개 데이터셋의 전문가 주석은 척추 구조, 영상 범주 또는 질환과 관련된 정보이며, ROB를 직접 표시한 전문가 주석은 아니다. 따라서 공개 데이터셋에 포함된 기존 주석 정보는 사용하지 않았다. ROB 기준 마스크를 생성하기 위해 모든 입력 영상에서 픽셀 강도를 0과 1 사이로 정규화하였다. 정규화 강도 0.2는 개발 단계에서 사전 설정한 경험적 임계값이며, 해당 값으로 생성된 마스크는 임상적 ground truth가 아닌 operational ROB reference mask로 사용하였다. 초기 영역에는 외곽 배경 외에도 영상 노이즈, 촬영 영역 내부의 국소적인 저강도 픽셀 및 촬영 마커 주변의 어두운 픽셀이 포함될 수 있다.

본 실험에서는 CNN이 operational ROB 기준을 원본 상태에서 재현하는 능력을 평가하기 위해 opening, closing 및 hole-filling과 같은 추가 형태학적 후처리를 CNN 예측 결과에 적용하지 않았다.

CNN 모델은 세 개의 인코딩 층, 하나의 중간층(bottleneck block), 세 개의 디코딩 층으로 구성하였다. 각 층은 두 개의 3×3 합성곱, 정규화 그룹, ReLU 활성화 함수로 구성하였으며, 특징 채널 수는 16, 32, 64, 128로 설정하였다. 인코더에서는 2×2 맥스 풀링(max pooling)을 사용하고, 디코더에서는 양선형 보간법을 이용하여 공간해상도를 복원하였다. 인코더와 디코더 간 skip connection은 사용하지 않았다. 최종 1×1 합성곱과 시그모이드 함수를 통해 픽셀별 ROB 확률 맵을 생성하였다. 손실함수는 이진 교차 엔트로피와 Dice 손실 함수를 동일한 가중치로 결합하여 사용하였다. 서로 다른 종횡비를 갖는 영상을 동적 크기로 처리하고 GPU 메모리 사용량을 일관되게 제한하기 위해 batch size를 1로 설정하였다. 입력 영상은 영상별 최소값과 최대값을 이용하여 0과 1 사이로 정규화하였다.

모델 최적화에는 AdamW optimizer를 사용하였으며, 초기 learning rate는 0.001, weight decay는 0.0001로 설정하였다. 최대 학습 epoch는 20으로 설정하였고, validation loss가 8회 연속 개선되지 않으면 학습을 조기 종료하였다. 학습 과정에서 validation loss가 가장 낮은 모델을 최종 모델로 선택하였다.

3. CNN-Based ROB Segmentation Performance

CNN 기반 ROB 분할 성능은 operational ROB reference mask와 예측 마스크 간의 Dice similarity coefficient(DSC), intersection over union(IoU), ROB-to-ROI 오류율 및 ROI-to-ROB 오류율을 이용하여 평가하였다(Table 1).

전체 영상에서 ROB Dice와 IoU는 각각 95.67(±0.43)과 91.69(±0.78)로 나타났다. 촬영 뷰별 Dice는 경추 97.56(±0.27), 요추 측면 96.90(±0.34), 요추 전후방 92.60(±1.13)으로 나타났다. 경추 영상에서 가장 높은 성능을 보였으며, 요추 전후방 영상은 외곽 배경의 형태와 저강도 영역의 다양성으로 인해 상대적으로 낮은 성능을 보였다.

Table 1. CNN-based ROB segmentation perfor-mance and pixel-level misclassification rates

Scope	Disc (%)	IoU (%)	ROBtoROI error (%)	ROItoROB error (%)
Overall	95.67 ±0.43	91.69 ±0.78	4.66 ±1.13	1.17 ±0.25
Cervical	97.56 ±0.27	95.23 ±0.51	2.72 ±0.66	0.44 ±0.13
Lumbar AP	92.60 ±1.13	86.24 ±1.93	8.10 ±2.52	1.07 ±0.25
Lumbar LA	96.90 ±0.34	93.99 ±0.65	3.25 ±0.88	1.36 ±0.39

전체 ROB-to-ROI 오류율은 4.66±1.13%였으며, ROI-to-ROB 오류율은 1.17±0.25%였다. ROB-to-ROI 오류는 배경 픽셀에 AES-256-GCM이 적용되어 처리량이 증가할 수 있으나 보호 수준은 감소하지 않는다. 반면 ROI-to-ROB 오류는 촬영정보가 포함된 픽셀에 AES-128-GCM이 적용되는 오류이므로 암호화 정책 측면에서 더 중요하다. 모든 촬영 뷰에서 ROI-to-ROB 오류율이 상대적으로 낮게 나타난 것은 불확실한 영역을 ROI로 분류하는 보수적인 정책이 반영된 결과로 해석할 수 있다.

따라서 기본 CNN 모델은 서로 다른 척추 X-ray 촬영 뷰에서 operational ROB 기준을 안정적으로 재현하였으며, 보안 정책상 중요한 ROI-to-ROB 오류를 낮은 수준으로 유지하였다. 다만 본 결과는 임상적 구조나 병변의 분할 정확도가 아니라 자동 생성된 operational ROB reference mask에 대한 재현 성능을 의미한다.

4. Visual evaluation of the encryption process

ROB 지향 선택적 암호화의 통계적 영상 은닉 성능, 처

리효율 및 복원성을 평가하기 위해 경추, 요추 전후방 및 요추 측면 영상 총 1,200장에 대해 영역별 AES-GCM 암호화와 RPF를 적용하였다. 제안 프레임워크의 단계별 처리 결과는 Fig. 2에 제시하였다. Fig. 2는 원본 영상, ROB 분할 결과, 영역별 선택적 암호화 결과 및 RPF 적용 후 최종 암호화 영상을 순차적으로 보여준다. ROB에는 AES-128-GCM, ROI에는 AES-256-GCM을 적용하였으며, 암호화된 전체 영상에는 16 크기 블록 기반 RPF를 적용하였다. 각 영상의 암호화와 복호화 시간은 3회 반복 측정한 중앙값으로 산출하였고, 촬영 뷰별 결과는 영상 간 평균과 표준편차로 제시하였다(Table 2).

Table 2. CNN-based ROB segmentation perfor-mance and pixel-level misclassification rates (L: Lumbar, Bit-exact : Bit-exact match rate)

Scope	Cervical	L AP	L LA	Overall
NPCR (%)	99.61 ±0.97	99.61 ±0.26	99.61 ±0.28	99.61 ±0.60
UACI (%)	34.65 ±1.15	29.05 ±1.73	33.54 ±2.14	32.41 ±2.97
Enc. (ms)	6.42	168.98	177.57	117.66
Dec. (ms)	6.36	175.24	183.06	121.55
Total (ms)	12.78	344.22	360.63	239.21
Total (ms/MP)	29.88	55.33	50.99	45.40
Throughput (MP/s)	33.50	18.68	17.63	23.27
Bit-exact (%)	100	100	100	100
SHA-256 match (%)	100	100	100	100

Table 3. Comparison of Security and Processing Performance According to RPF Block Size (Mean |Corr.|: mean absolute adjacent-pixel correlation coefficient; Boundary Leakage AUC: area under the ROC curve for detecting ROI-ROB boundary leakage; Total Time: total processing time normalized by image resolution, expressed in milliseconds per megapixel [ms/MP])

Scope	ROB model only	ROB + RPF16	ROB + RPF32	ROB + RPF64	ROB + RPF128
NPCR (%)	99.6096 ±0.0057	99.6093 ±0.0062	99.6090 ±0.0058	99.6094 ±0.0056	99.6094 ±0.0058
UACI (%)	32.4138 ±2.9698	32.4149 ±2.9705	32.4139 ±2.9694	32.4138 ±2.9692	32.4140 ±2.9700
Entropy	7.9998 ±0.0001	7.9998 ±0.0001	7.9998 ±0.0001	7.9998 ±0.0001	7.9998 ±0.0001
Mean |Corr.|	0.0025 ±0.0011	0.0025 ±0.0010	0.0025 ±0.0011	0.0025 ±0.0011	0.0025 ±0.0010
Boundary AUC	0.5043 ±0.0060	0.5042 ±0.0057	0.5043 ±0.0061	0.5041 ±0.0060	0.5041 ±0.0058
Total time (ms/MP)	42.074 ±10.733	45.400 ±12.032	44.122 ±11.597	43.746 ±11.442	43.646 ±11.576

촬영 뷰별 시각적 암호화 결과와 인접 픽셀 상관분포는 Fig. 3에 제시하였다. Fig. 3(a)-(c)는 경추, 요추 AP 및 요추 LA 영상에서 원본 영상, ROB 기반 segmentation mask 및 암호화 결과를 보여준다. Fig. 3(d)-(f)는 각 촬영 뷰에서 암호화 전후의 인접 픽셀 분포를 비교한 결과이다. 원본 영상에서는 인접 픽셀이 대각선 방향으로 밀집된 분포를 보인 반면, 암호화 영상에서는 점들이 넓게 분산되어 공간적 상관성이 제거된 것을 확인할 수 있다.

전체 영상의 평균 NPCR은 99.61(±0.60)%로 나타났으며, 경추, 요추 전후방 및 요추 측면 영상에서도 모두 약 99.61%의 일관된 값을 보였다. 평균 UACI는 전체 영상에서 32.41(±2.97)%였으며, 경추 34.65±(1.15)%, 요추 전후방 29.05(±1.73)%, 요추 측면 33.54(±2.14)%로 나타났다. 요추 전후방 영상의 UACI가 다른 촬영 뷰보다 상대적으로 낮았으며, 이는 촬영 뷰별 원본 픽셀 강도 분포와 ROI/ROB 구성 비율의 차이에 영향을 받은 것으로 판단된다. NPCR과 UACI는 암호영상의 픽셀 변화 및 통계적 확산 정도를 나타내는 보조 지표[21][22]이며, 그 자체로 AES-GCM의 암호학적 안전성을 직접 입증하는 것은 아니다.

평균 암호화 및 복호화 시간은 경추 영상에서 각각 6.42 ms와 6.36 ms로 나타났다. 요추 전후방 영상에서는 각각 168.98 ms와 175.24 ms, 요추 측면 영상에서는 177.57 ms와 183.06 ms가 소요되었다. 요추 영상의 절대 처리시간은 경추 영상보다 크게 증가하였으나, 이는 원본 영상의 픽셀 수 차이에 기인한다. 해상도 차이를 정규화한 전체 처리시간은 경추 29.88 ms/MP, 요추 전후방 55.53 ms/MP, 요추 측면 57.58 ms/MP로 나타났으며, 처리량은 각각 33.50, 18.68 및 17.63 MPixel/s였다.

복호화 결과에서는 전체 1,200개 영상에서 원본과 복호화 영상 간 불일치 픽셀이 발생하지 않았다. 모든 영상에서 비트-정확 일치율과 SHA-256 해시 일치가 확인되어, 영역별 AES-GCM 암호화와 RPF 순열을 역순으로 적용한 후 원본 픽셀 배열이 손실 없이 복원됨을 확인하였다.

5. RPF Ablation Study

RPF의 효과와 처리 오버헤드를 평가하기 위해 선택적 AES-GCM만 적용한 조건과 4×4, 8×8, 16×16, 32×32 및 64×64 block 기반 RPF 조건을 비교하였다. 모든 조건은 동일한 ROI 및 ROB 암호문을 사용하였으며, 조건 간 차이는 RPF 적용 여부와 block 크기로 제한하였다(Table 3).

NPCR은 모든 조건에서 약 99.609%로 나타났으며, entropy는 7.9998로 8에 근접하였다. 평균 절대 인접 픽셀 상관계수(Mean |Corr.|)도 0.002491-0.002533 범위로 매

Table 4. Performance Comparison of Encryption Methods Across X-ray Image Types (C: cervical; L-AP: lumbar anteroposterior; L-LA: lumbar lateral; Mean |Corr.|: mean absolute adjacent-pixel correlation coefficient; Boundary Leakage AUC: area under the ROC curve for detecting ROI-ROB boundary leakage; Total Time: total processing time normalized by image resolution, expressed in milliseconds per megapixel [ms/MP])

Model	Spine	NPCR (%)	UACI (%)	Entropy	Mean |Corr.|	Boundary AUC	Total time (ms/MP)	SHA-256 match (%)
Proposed	C	99.6095 ±0.0091	34.6513 ±1.1524	7.99956 ±0.00004	0.00249 ±0.00103	0.50211 ±0.00164	29.374 ±0.854	100
	L ap	99.6094 ±0.0026	29.0537 ±1.7326	7.99996 ±0.00001	0.00253 ±0.00107	0.50322 ±0.00159	41.592 ±13.258	100
	L la	99.6095 ±0.0026	33.5354 ±2.1385	7.99996 ±0.00001	0.00245 ±0.00106	0.50184 ±0.00163	37.856 ±5.839	100
Henon Map [12]	C	99.6096 ±0.0092	34.6529 ±1.1521	7.99956 ±0.00004	0.00251 ±0.00108	0.50210 ±0.00164	76.664 ±0.812	100
	L ap	99.6093 ±0.0027	29.0532 ±1.7324	7.99996 ±0.00001	0.00249 ±0.00107	0.50321 ±0.00159	93.923 ±1.024	100
	L la	99.6097 ±0.0026	33.5351 ±2.1382	7.99996 ±0.00001	0.00246 ±0.00105	0.50181 ±0.00163	89.856 ±0.936	100
RPF [15]	C	99.6095 ±0.0091	34.6512 ±1.1523	7.99956 ±0.00004	0.00253 ±0.00108	0.50208 ±0.00164	27.188 ±0.742	100
	L ap	99.6094 ±0.0026	29.0536 ±1.7325	7.99996 ±0.00001	0.00252 ±0.00107	0.50319 ±0.00159	43.764 ±0.864	100
	L la	99.6095 ±0.0026	33.5356 ±2.1384	7.99996 ±0.00001	0.00248 ±0.00106	0.50179 ±0.00163	47.747 ±0.801	100
Chaotic Map [7]	C	99.6094 ±0.0093	34.6515 ±1.1526	7.99956 ±0.00004	0.00260 ±0.00109	0.50206 ±0.00164	33.912 ±2.184	100
	L ap	99.6092 ±0.0028	29.0539 ±1.7327	7.99996 ±0.00001	0.00259 ±0.00107	0.50317 ±0.00159	42.742 ±2.516	100
	L la	99.6094 ±0.0027	33.5356 ±2.1387	7.99996 ±0.00001	0.00255 ±0.00106	0.50177 ±0.00162	38.912 ±2.301	100
Chaotic S-boxes [18]	C	78.7421 ±0.8421	23.3012 ±1.2145	7.60481 ±0.0124	0.00254 ±0.00108	0.60391 ±0.0126	91.214 ±6.842	100
	L ap	78.7634 ±0.8512	23.2415 ±1.1984	7.60611 ±0.0118	0.00253 ±0.00107	0.60521 ±0.0131	89.214 ±6.214	100
	L la	78.7489 ±0.8465	23.3058 ±1.2261	7.60594 ±0.0121	0.00245 ±0.00106	0.60501 ±0.0129	82.684 ±5.973	100

우 낮았다. 경계 누설(Boundary leakage) AUC는 ROB Model Only에서 0.504385, RPF 조건에서 0.504159–0.504370으로 나타나 모두 무작위 분류 기준인 0.5에 근접하였다. 이러한 결과는 영역별 선택적 AES-GCM만으로도 높은 암호문 무작위성과 낮은 인접 픽셀 상관성이 확보되며, RPF 적용이나 블록 크기 변화가 NPCR, UACI, entropy 및 경계 누설 AUC를 추가로 크게 개선하지는 않음을 보여준다.

반면 전체 처리시간은 RPF 블록 크기에 따라 차이를 보였다. ROB Model Only의 전체 처리시간은 42.074 (± 10.733) ms/MP였으며, RPF 16, RPF 32, RPF 64 및 RPF 128은 각각 45.400 (± 12.032), 44.122 (± 11.597), 43.746 (± 11.442), 43.646 (± 11.576) ms/MP로 나타났다. ROB Model Only 대비 평균 처리시간 증가율은 RPF 16이 약 7.9%, RPF 32가 약 4.9%, RPF 64가 약 4.0%, RPF 128이 약 3.7%였다. 블록 크기가 증가할수록 블록 수와 순열 연산 횟수가 감소하여 RPF 처리 오버헤드가 낮아지는 경향을 보였다.

RPF 128은 비교한 RPF 조건 중 가장 낮은 평균 처리시간을 보였으나, RPF 64와의 차이는 0.100 ms/MP로 약 0.23%에 불과하였다. 반면 RPF 64는 RPF 128보다 작은 블록을 사용하여 암호문 블록의 공간적 위치를 보다 세분화하여 재배열할 수 있다. 이에 따라 본 연구에서는 RPF-64를 최종 블록 크기로 선정하였다.

RPF는 AES-GCM의 통계적 무작위성을 직접 향상하는 독립 암호화 알고리즘이라기보다, ROI와 ROB 암호문 블록의 원래 공간적 배치를 추가로 은닉하는 보조적인 난독화 계층의 역할을 수행한다. 모든 조건에서 비트 정확(bit-exact) 복원율과 SHA-256 일치율은 100%였으며, RPF 적용과 블록 크기 변화로 인한 영상 정보 손실은 발생하지 않았다.

6. Comparison of encryption model performance

제안 모델의 성능을 검증하기 위해 헤논 맵[12], RPF[15], 혼돈맵[7], 혼돈 기반 S-박스[18] 모델과 비교하

였다. 모든 모델은 동일한 경추(C), 요추 전후면(L-AP), 요추 측면(L-LA) 영상에 적용하였으며, 처리시간은 영상 크기로 정규화한 ms/MP 단위로 평가하였다.

제안 모델의 성능을 검증하기 위해 헤논 맵, RPF, 혼돈 맵, 혼돈 기반 S-박스 모델과 비교하였다. 모든 모델은 동일한 경추(C), 요추 전후면(L-AP), 요추 측면(L-LA) 영상에 적용하였으며, 처리시간은 영상 크기로 정규화한 ms/MP 단위로 평가하였다.

제안 모델은 CNN으로 ROB를 탐지한 후 ROI에는 AES-256-GCM, ROB에는 AES-128-GCM을 적용하는 영역별 차등 암호화 방식이다. 이후 로지스틱 맵 기반 RPF를 적용하여 ROI-ROB 경계를 은닉하였다. RPF 블록 크기는 5절의 ablation study 결과를 반영하여 64 크기로 설정하였다.

헤논 맵 모델은 (a=1.4), (b=0.3)의 혼돈맵을 이용하여 블록 순열과 픽셀 확산을 수행하였다. RPF 모델은 영상을 64 크기 블록으로 분할한 후 블록 순열, 회전 및 반전을 적용하였다. Chaotic Map 모델은 8 크기의 블록과 로지스틱 맵 매개변수 4.0을 사용하여 영상 전체를 혼합하였다. 혼돈 기반 S-박스 모델은 Logistic-Tent 혼돈맵으로 동적 S-box를 생성하고 ROI에 선택적으로 치환 및 확산을 적용하였다.

Table 4에서 제안 모델은 모든 영상 유형에서 약 99.61%의 NPCR과 8.0에 근접한 엔트로피를 기록하였다. 평균 절대 인접 픽셀 상관계수는 0.00245-0.00253으로 매우 낮았으며, 경계 누설 AUC도 0.50184-0.50322로 0.5에 근접하여 ROI-ROB 경계가 효과적으로 은닉되었음을 확인하였다.

제안 모델의 평균 처리시간은 36.27 ms/MP로, 헤논 맵의 86.81 ms/MP와 혼돈 기반 S-박스의 약 87.70 ms/MP보다 크게 짧았다. 또한 RPF와 Chaotic Map에 비해서도 유사하거나 더 낮은 처리시간을 유지하였다. 반면 혼돈 기반 S-박스 모델은 ROB가 암호화되지 않아 NPCR, UACI 및 엔트로피가 감소하고 경계 누설 AUC가 약 0.60으로 증가하였다.

모든 모델은 복호화 후 SHA-256 일치율 100%를 기록하였다. 제안 모델은 높은 확산성과 낮은 픽셀 상관성을 유지하면서도 전체 영상 보호, 경계 은닉, AES-GCM 기반 무결성 검증 및 빠른 처리 속도를 제공하였다. 따라서 제안 방법은 선행 연구와 유사한 수준의 통계적 보안 지표를 유지하면서도 연산 부담을 효과적으로 감소시킴을 입증하였다.

V. Conclusions

본 연구에서는 비식별화된 DICOM 척추 X-ray 영상의 PixelData를 보호하기 위해 ROB 지향 영역 적응형 선택 암호화 프레임워크를 제안하였다. 제안 방법은 CNN을 이용하여 촬영 정보가 거의 없는 ROB를 먼저 탐지하고, 그 보완 영역을 ROI로 정의한다. 이후 ROI에는 AES-256-GCM, ROB에는 AES-128-GCM을 적용하며, 영역별 암호화 이후 로지스틱 맵 기반 RPF를 추가하여 ROI와 ROB의 공간적 경계를 은닉하였다.

CNN 기반 ROB 분할 모델은 전체 영상에서 95.67±0.43%의 Dice와 91.69±0.78%의 IoU를 기록하였다. 특히 보안 정책상 중요하게 고려되는 ROI-to-ROB 오류율은 1.17±0.25%로 나타나, 촬영 정보가 포함된 픽셀이 상대적으로 낮은 암호화 강도의 영역으로 분류되는 오류를 최소화하였다. 이러한 결과는 임상 병변 또는 해부학적 구조의 분할 정확도가 아니라, 영상 강도와 외곽 연결성을 기반으로 생성한 operational ROB reference mask의 재현 성능을 검증한 것이다.

RPF ablation study에서는 블록 크기에 따른 NPCR, UACI, 엔트로피, 인접 픽셀 상관계수 및 경계 누설 AUC의 차이가 크지 않았다. RPF-128이 가장 짧은 처리시간을 보였으나 RPF-64와의 차이는 약 0.23%에 불과하였다. 이에 따라 공간적 재배열의 세분성과 처리 효율을 함께 고려하여 64 크기 블록을 최종 설정으로 선정하였다. RPF는 AES-GCM의 암호학적 안전성을 직접 높이는 독립 암호화 알고리즘이라기보다, 암호화된 ROI와 ROB의 원래 공간적 배치를 추가로 은닉하는 보조 계층으로 해석할 수 있다.

제안 모델은 모든 촬영 뷰에서 약 99.61%의 NPCR과 8.0에 근접한 엔트로피를 기록하였으며, 평균 절대 인접 픽셀 상관계수는 0.00245-0.00253으로 나타났다. 경계 누설 AUC도 0.50184-0.50322로 무작위 분류 수준인 0.5에 근접하여, 암호화 영상에서 ROI와 ROB의 경계를 구분하기 어려운 것으로 확인되었다. 또한 모든 영상에서 비트 단위 일치와 SHA-256 해시 일치율 100%를 달성하여 복호화 후 원본 정보가 손실 없이 복원됨을 확인하였다.

비교 실험에서 제안 모델은 헤논 맵, RPF 및 혼돈맵과 유사한 수준의 NPCR, 엔트로피 및 인접 픽셀 상관 성능을 유지하였다. 평균 처리시간은 36.27 ms/MP로 헤논 맵과 혼돈 기반 S-박스보다 짧았으며, RPF 및 혼돈맵과 비교해서도 유사하거나 낮은 처리시간을 보였다. 따라서 제안 모델은 선행 연구와 유사한 수준의 보안 지표를 유지하면서 계산 부담을 줄여, 보안성과 처리 효율성을 함께 확보할

수 있는 가능성을 보였다.

본 연구는 비식별화 이후의 2차원 척추 X-ray Pixel Data 보호에 범위를 한정하였으며, DICOM 헤더 비식별화, 키 분배 및 키 관리시스템의 구현, 침해된 단말과 사이드채널 공격은 다루지 않았다. 또한 ROB 기준 마스크는 전문가 주석이 아닌 operational reference mask를 이용하여 생성하였으므로, 임상적 구조 분할 성능으로 해석해서는 안 된다. 향후 연구에서는 다양한 촬영 장비와 기관에서 획득한 X-ray 영상에 대한 외부 검증, 다른 해부학적 부위 및 3차원 의료영상으로의 확장, 보안 키와 마스크 메타데이터의 안전한 관리, 임상 AI 플랫폼과 연계한 실제 운영 환경 평가가 필요하다.

ACKNOWLEDGEMENT

This work was supported by a research grant from Hankyong National University in the year of 2024.

REFERENCES

[1] K. N. Singh and A. K. Singh, "Towards integrating image encryption with compression: A survey," ACM Transactions on Multimedia Computing, Communications, and Applications, Vol. 18, pp. 1-21, 2022. DOI: 10.1145/ 3498342

[2] Q. Natsheh, A. Sălăgean, D. Zhou, and E. Edirisinghe, "Automatic selective encryption of DICOM images," Applied Sciences, Vol. 13, No. 8, p. 4779, April 2023. DOI: 10.3390/app13084779

[3] K. Jain, A. Aji, and P. Krishnan, "Medical image encryption scheme using multiple chaotic maps," Pattern Recognition Letters, Vol. 152, pp. 356-364, 2021. DOI: 10.1016/j.patrec. 2021.10.033

[4] A. Z. Hussain and M. A. A. Khodher, “Medical Image Encryption Using Multi Chaotic Maps,” TELKOMNIKA (Telecommunication Computing Electronics and Control), Vol. 21, No. 3, pp. 556-565, June 2023. DOI: 10.12928/telkomnika.v21i3.24324

[5] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," Signal Processing: Image Communication, Vol. 41, pp. 144-157, 2016. DOI: 10.1016/j.image.2015.10.004

[6] A. A. Steffi and D. Sharma, "Modified algorithm of encryption and decryption of image using chaotic mapping," International Journal of Science and Research, Vol. 2, No. 2, pp. 77-80, February 2013.

[7] P. R. Sankpal and P. A. Vijaya, "Image encryption using chaotic maps: A survey," Proceedings of the 5th International Conference on Signal and Image Processing, pp. 102-107, Bangalore, India, January 2014. DOI: 10.1109/ICSIP.2014.80

[8] Y. Wang, K. W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," Applied Soft Computing, Vol. 11, No. 1, pp. 514-522, January 2011. DOI: 10.1016/j.asoc.2009. 12.011

[9] S. Mortajez, M. J. Dehghan, and A. Azizi, “Securing DICOM Images with a Novel Chaotic Encryption Scheme Utilizing Wavelet Transform and Biometric Fingerprint,” Research Square, June 2024. DOI: 10.21203/rs.3.rs -4462062/v1

[10] A. H. Allaf and M. A. Kbir, "A review of digital watermarking applications for medical image exchange security," Proceedings of the 3rd International Conference on Smart City Applications, pp. 472-480, Tetouan, Morocco, October 2018. DOI: 10.1007/ 978-3-030-12040- 6_42

[11] A. F. Qasim, F. Meziane, and R. Aspin, "Digital watermarking application for developing trust in medical imaging workflow: State-of-the-art review," Computer Science Review, Vol. 37, p. 100282, August 2020. DOI: 10.1016/j.cosrev.2020.100282

[12] H. Zhao, S. Xie, J. Zhang, and T. Wu, “A Dynamic Block Image Encryption Using Variable-Length Secret Key and Modified Henon Map,” Optik, Vol. 230, Art. no. 166307, March 2021. DOI: 10.1016/j.ijleo.2021.166307

[13] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, Vol. 24, No. 9, pp. 926-934, September 2006. DOI: 10.1016/j.imavis.2006. 02.021

[14] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons & Fractals, Vol. 21, pp. 749-761, 2004. DOI: 10.1016/j.chaos.2003. 12.022

[15] N. L. Santos, B. V. Ghita, and G. L. Masala, “Enhancing Data Security in Cloud Using Random Pattern Fragmentation and a Distributed NoSQL Database,” Proceedings of the 2019 IEEE International Conference on Systems, Man and Cybernetics, pp. 3735-3740, Bari, Italy, October 2019. DOI: 10.1109/SMC.2019. 8914454

[16] R. Liu, X. Liu, and C. Hu, "Image encryption algorithm based on chaotic permutation matrix and DNA sequence," Multimedia Tools and Applications, Vol. 76, pp. 18127-18147, 2017. DOI: 10.1155/2014/917147

[17] C. Fan and Q. Ding, “A Novel Image Encryption Scheme Based on Self-Synchronous Chaotic Stream Cipher and Wavelet Transform,” Entropy, Vol. 20, No. 6, Art. no. 445, June 2018. DOI: 10.3390/e20060445

[18] S. S. Jamal, M. M. Hazzazi, M. F. Khan, Z. Bassfar, A. Aljaedi, and Z. ul Islam, "Region of interest-based medical image encryption technique based on chaotic S-boxes," Expert Systems with Applications, Vol. 238, Art. no. 122030, 2024. DOI:

10.1016/j.eswa.2023.122030

[19] Y. Ran et al., "A high-quality dataset featuring classified and annotated cervical spine X-ray atlas," Scientific Data, Vol. 11, Art. no. 625, 2024. DOI: 10.1038/s41597-024 -03383-0

[20] P. Limprasert, S. Narkbuakaew, N. Phaisanwong, et al., "BUU-LSPINE: A Thai open lumbar spine dataset for spondylolisthesis detection," Applied Sciences, Vol. 13, No. 15, p. 8646, July 2023. DOI: 10.3390/app13158646

[21] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," Journal of Selected Areas in Telecommunications, Vol. 1, pp. 31-38, 2011.

[22] E. H. Rachmawanto, C. A. Sari, A. Susanto, and M. Doheir, "A comparative study of image cryptographic method," Proceedings of the International Conference on Information Technology, Computer, and Electrical Engineering, pp. 336-341, Semarang, Indonesia, September 2018. DOI: 10.1109/ICITACEE.2018. 8576916

Authors

Cheolhun Hwang received the B.E. degree in computer engineering from Gachon University, Seongnam, South Korea, in 2019, and the M.E. degree in software engineering from Gachon University, in 2020.

He is currently pursuing the Ph.D. degree in Translational -Clinical Medicine at Gachon University, Seongnam, Korea. His research interests include translational research, biomedical engineering, medical data security, machine learning, artificial intelligence, medical imaging security, and AI-based clinical decision support systems.

Geon-Yun Shin received MS and PhD degrees in computer engineering from Gachon University, Republic of Korea, in 2018 and 2023, respectively. He is a professor in the major of information security, Hankyong National University, Korea. His research interests include AI security, LLM Security, unknown attack detection, dark web, open set recognition, and reinforcement learning.