PACS 시스템의 안전한 의료정보 저장 방법 연구

2024/05/01

BCG Lab 김아은

INDEX

PACS

❖ PACS란?

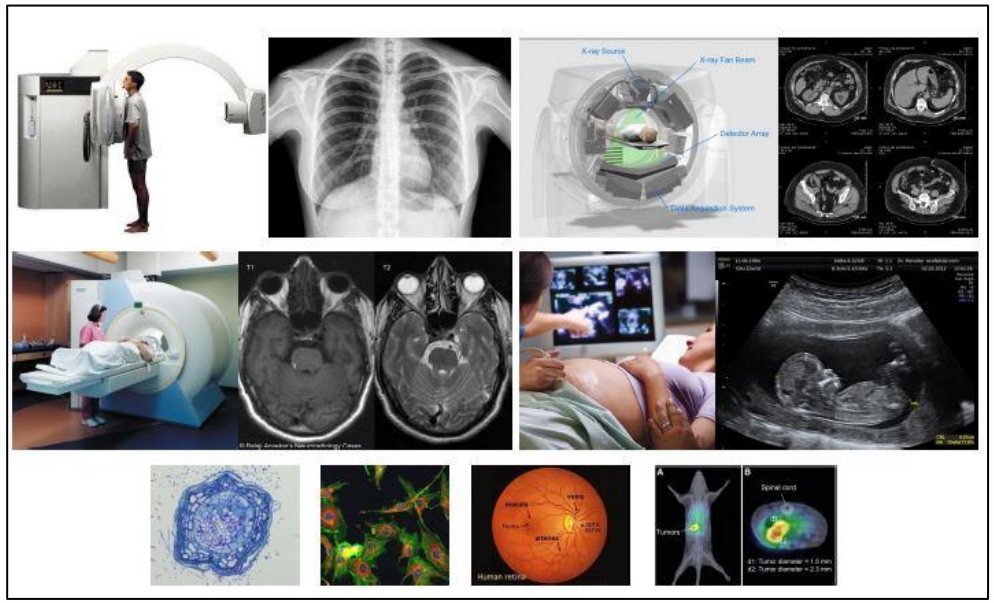
- Picture Archiving and Communication System, 의료영상저장 및 전송시스템
- X-ray, CT, MR, 초음파검사 등 첨단 진단 장치로부터 얻은 의료영상을 디지털화 하여 저장
- 병원 내 어디서나, 여러 부서에서 동시에 의료영상을 검색할 수 있는 시스템
- 초고속 인터넷 보급이 늘어나면서, 병원 외부로 의료영상을 전송하여 2차판독의 도움을 얻기도 함

그림1. PACS 도입 이전

출처: X Ray recycling

그림2. PACS 도입 이후

출처: Peekmed



의료영상

PACS로 전송되는 의료정보

❖ DICOM(Digital Imaging and Communications in Medicine)

- 서로 다른 영상장비들 간 발생한 의료영상이 원활하게 전송 및 교환될 수 있도록 의료영상의 저장형식과 통신방법을 규정한 약속
- `식약청 PACS DICOM 데이터 호환성 향상 및 보안적용 가이드라인`에 따라 방사선 영상 데이터를 DICOM으로 인코딩해야 함 (.dcm)
- 세계표준으로 DICOM, HL7, HIPAA 등이 있음

DICOM 도입 전

DICOM 도입 후

PACS로 전송되는 의료정보

❖ DICOM Tags

DICOM Tags

Search...

(Group,E...	TAG Description	VR	V...	L...	Value
(0002,0000)	File Meta Information Group Length	UL	1	4	210
(0002,0001)	File Meta Information Version	OB	1	2	00\01
(0002,0002)	Media Storage SOP Class UID	UI	1	26	1.2.840.10008.5.1.4.1.1.2
(0002,0003)	Media Storage SOP Instance UID	UI	1	64	1.3.6.1.4.1.9590.100.1.2.203327578511590672108909764033949608752
(0002,0010)	Transfer Syntax UID	UI	1	20	1.2.840.10008.1.2.1 (Explicit VR Little Endian)
(0002,0012)	Implementation Class UID	UI	1	32	1.3.6.1.4.1.9590.100.1.3.100.9.4
(0002,0013)	Implementation Version Name	SH	1	14	MATLAB IPT 9.4
(0008,0005)	Specific Character Set	CS	1	10	ISO_IR 100
(0008,0008)	Image Type	CS	4	30	ORIGINAL\PRIMARY\AXIAL\HELICAL
(0008,0012)	Instance Creation Date	DA	1	8	20200311
(0008,0013)	Instance Creation Time	TM	1	10	114003.671
(0008,0016)	SOP Class UID	UI	1	26	1.2.840.10008.5.1.4.1.1.2
(0008,0018)	SOP Instance UID	UI	1	64	1.3.6.1.4.1.9590.100.1.2.203327578511590672108909764033949608752
(0008,0020)	Study Date	DA	0	0	
(0008,0022)	Acquisition Date	DA	0	0	
(0008,0023)	Content Date	DA	0	0	
(0008,0030)	Study Time	TM	0	0	
(0008,0032)	Acquisition Time	TM	0	0	
(0008,0033)	Content Time	TM	0	0	
(0008,0050)	Accession Number	SH	0	0	
(0008,0060)	Modality	CS	1	2	CT
(0008,0070)	Manufacturer	LO	0	0	
(0008,0080)	Institution Name	LO	0	0	
(0008,0081)	Institution Address	ST	0	0	
(0008,0090)	Referring Physician Name	PN	0	0	
(0008,1010)	Station Name	SH	0	0	
(0008,1030)	Study Description	LO	1	4	LUNG
(0008,103E)	Series Description	LO	1	16	Mediastinum 1.5
(0008,1070)	Operators Name	PN	0	0	

Export Edit Add Remove Apply Image Close

환자 인적사항	의사제공자 정보
환자 ID	의사 이름
환자 이름	등록번호
환자 주소	의료기관 이름
환자 연락처	의료기관 주소
환자 성별	의사 전화번호
환자 생년월일	진료과
	진료정보 전송 표준 규격
	진료기록 보고서 CDA

PACS 보안 기술

❖ PACS에 적용된 보안 기술

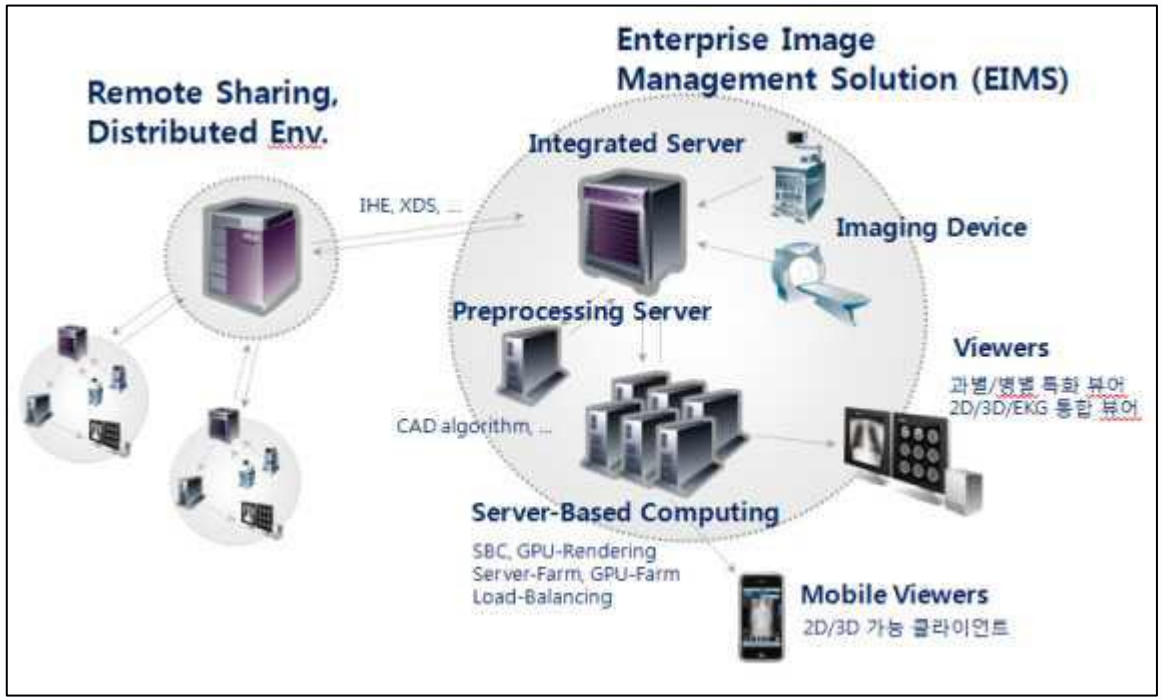
① 데이터 암호화 : 헤더 메타데이터의 선택적 암호화, 이미지 파일의 전체 암호화, 디지털 워터마킹

② 네트워크 보안 : 방화벽 및 네트워크 세분화, 네트워크 전송 암호화(TLS/SSL), 네트워크 모니터링

③ 물리적 보안 : 파일 서버 분리, 서버실에 보안 카메라 설치, USB 포트 등 물리적 포트 사용 안 함

④ 접근 제어 : 사용자 인증 및 접근제어, 모바일 장치에 대한 정책 정의(BYOD)

⑤ 감사 로깅 : 사용자 활동 감사 추적



LEA

❖ LEA(Lightweight Encryption Algorithm) 암호 알고리즘

- 개발연도 : 2013년
- 알고리즘 구분 : 128비트 블록암호
- 키 길이 : 128비트, 192비트 또는 256비트
- 구조 : ARX(Addition Rotation XOR) 기반 GFN(Generalized Feistel Network)

- 특징

  - 32비트 이상의 범용 프로세스에서의 빠른 소프트웨어 암호화
  - CPU 차원에서 비교적 빠른 처리가 가능한 ARX 연산으로 이루어짐
  - 비교적 적은 메모리와 리소스를 필요로 함

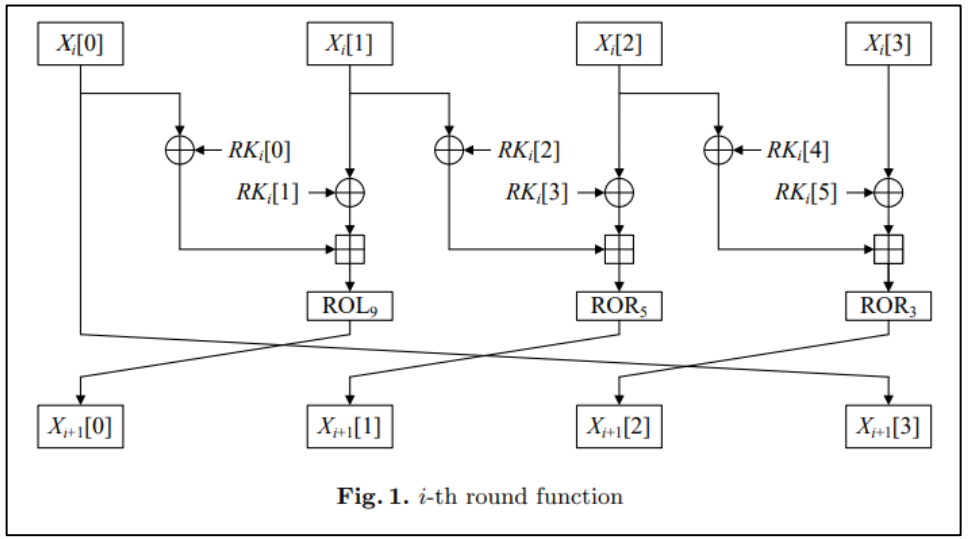


Fig. 1. *i*-th round function

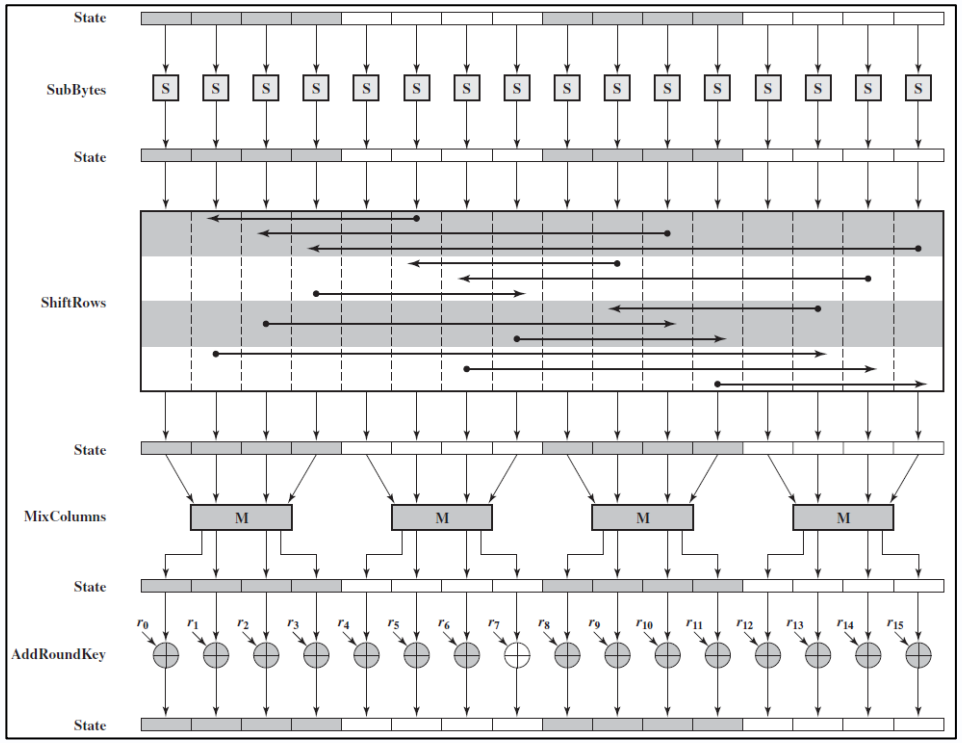
AES

❖ AES(Advanced Encryption Standard) 암호 알고리즘

- 개발연도 : 2001년 추정
- 알고리즘 구분 : 128비트 블록암호
- 키 길이 : 128비트, 192비트 또는 256비트
- 구조 : SPN(Substitution Permutation Network) 구조

- 특징

  - 8비트 이상의 범용 프로세스에서의 빠른 소프트웨어 암호화
  - SubBytes, ShiftRows, AddRoundKey 등 다양한 연산을 사용하여 복잡함
  - 안정성과 안전성 면에서 우수함



의료이미지 암·복호화 과정

❖ LEA 암호 알고리즘을 선정한 이유

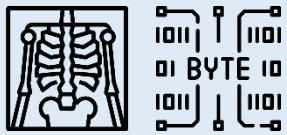
- 국제+국내 표준 암호 알고리즘 → 다른 시스템 및 장치와의 상호 운용성 및 호환성 보장
- 암호 분석 공격에 대해 강력한 보안을 제공 → 의료이미지와 같은 민감한 데이터에 높은 수준의 보안 제공

- 대다수의 PACS는 64비트 환경 → AES보다 LEA가 성능이 더 효율적일 것으로 예상함
- 경량화 및 효율화. 리소스가 제한된 환경과 계산 능력이 제한된 장치에 적합 ??

의료이미지 암·복호화 과정

❖ 암호화 과정

key, iv 생성



의료 이미지 데이터 로드
및 byte로 변환

암호화 모드 설정 및
암호화 수행 (.enc)

❖ 복호화 과정

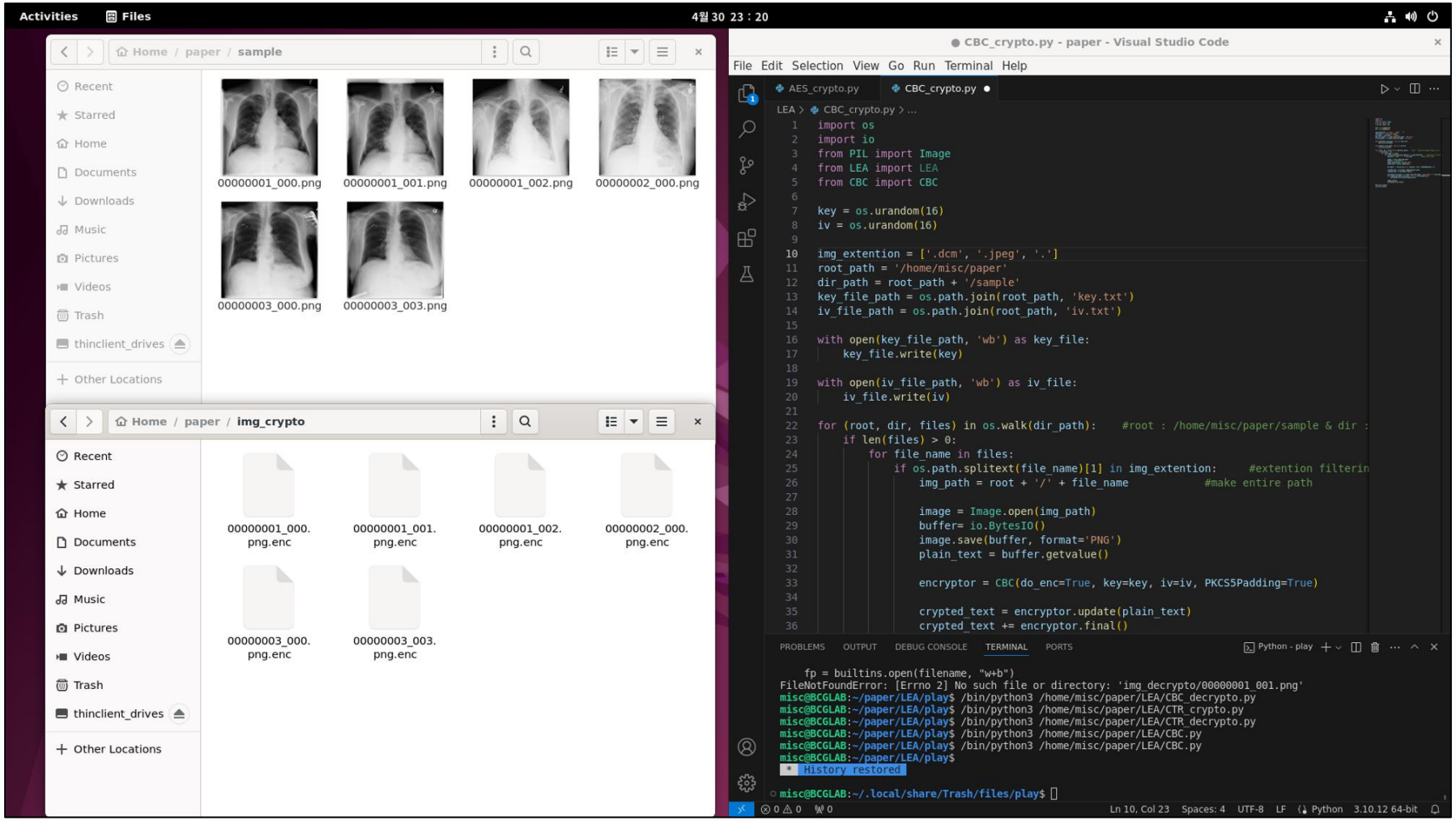
key, iv 불러오기

암호화된 이미지 로드
및 복호화 모드 설정

복호화 수행 (.png)

의료이미지 암·복호화 과정

❖ 시범영상



기대효과

❖ PACS의 의료데이터에 LEA를 적용하면 얻는 이점

- 전력 소비가 낮음
- 빠른 처리 속도 : AES와 비교했을 때, 약 1.5~2배 빠른 속도로 처리
- 상대적으로 적은 메모리와 연산 리소스를 사용함

논문 작성 과정

❖ 주제 선정

- 관심사에 대한 최신 논문을 먼저 읽어보기 (최신부터 역순으로)
- 기존 논문을 단순히 읽고 정리하는 것 X

  → 기존 연구에서 어떤 개선할 점이 있는지, 다른 적용 방법이 있는지 등에 대해 생각해보기
- 첫 논문은 깊게 이해 → 이후 논문은 확실한 이해보다는, 서론·결론만 읽고 문제점/개선점 파악하기
- 선배, 교수님과 적극적으로 소통하면서 피드백 받기
- 보고서(회의록 등)는 꾸준히 작성하기 (안 적으면 정리가 되지 않고, 진행이 더딤)

❖ 동향 파악

- 한 장의 표로 요약한다고 생각하고 정리하면 어떤 관점에서 보았는지 알 수 있어 일목요연하게 정리됨

  ex) refer/사용 알고리즘/데이터셋/정확도 결과로 작성 후 표로 정리하기

감사합니다

Q&A