2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

PACS를 위한 블록 암호 알고리즘의 설계

정혜명*, 전문석**
*김포대학 멀티미디어전공
**숭실대학교 컴퓨터학부
e-mail:myoung@kimpo.ac.kr

A Design of Block Cipher Algorithm for PACS

Hye-Myoung Choung*, Moon-Seog Jun**
*Dept of Multimedia, Kimpo College
**Dept of Computer Engineering, Soongsil University

요약

정보통신의 발달로 인하여 의료분야에서도 컴퓨터 기반 환자기록이 보편화되었다. 이러한 의료정보에는 가족 병력 기록, 과거 병력 기록, 정신 질환 기록 등 개인의 텍스트 정보뿐만 아니라 X-ray 등과 같은 영상 정보들이 의료기관간의 내·외부로 이동되고 있다. 이러한 정보들은 네트워크 환경 하에서 자연히 노출될 수 있는 보안상의 문제가 대두되고 있다. 이를 위하여 기존의 의료 정보 시스템과 잘 호환되고, 안전하고, 효율적인 보안 장치가 필요한데 이러한 장치 중의 하나가 견고한 암호 알고리즘의 구축이다. 이 논문에서는 현재 PACS의 표준 프로토콜인 DICOM의 데이터 구조와 같은 크기의 블록으로 나누어 암호화는 알고리즘을 제안한다.

1. 서론

정보통신 기술의 발전과 의무기록 전산화 시스템(EMR : Electronic Medical Record), 처방전달 시스템(OCS : Order Communication System) 및 의료 영상정보 저장 및 전송 시스템(PACS : Picture Archiving Communication System) 등의 확대 보급으로 인하여 의료 정보들의 전송에 있어서도 편리한 시스템에 의존하려는 경향이 늘어나면서 이들 정보들의 보안 문제가 크게 대두되고 있다. 1989년 7월부터는 의료 전달 체계가 시행되고 있으며 2000년 7월 1일부터는 가정의학과를 제외한 모든 진료는 1차 병원을 거쳐서 차 상급 병원으로 가도록 제도가 강화되었다. 따라서 이러한 정보들을 보내고 받는 현재의 시점에서는 이들 정보에 대한 안전성 및 신뢰성 확보 측면에서 정보 보호가 중요한 역할을 담당하게 되는 것이다. 이러한 보안상의 문제를 해결하기 위한 대안으로 제시되고 있는 방법 중의 하나가 암호 알고리즘이다. 따라서 의료정보들을 정확하고 안전하게 전달하기 위한 요건으로는 안전성과 효율성도 중요하지만 그보다는 의료정보의 특성이 텍스트보다는 영상정보가 다 많다는 특성을 고려해 볼 때 암·복호화 속도가 빠르고 기존의 의료정보 시스템 특히 PACS와 잘 호환될 수 있는 암호 알고리즘의 구축이라고 할 수 있다.

이 논문에서 제안한 암호 알고리즘은 암호화 기법의 분류 중 메시지를 PACS의 표준 프로토콜로 사용되고 있는 DICOM(Digital Image Communications in Medicine) 표준과 같은 크기의 블록 단위로 분할하여 암·복호화하는 암호 알고리즘이다.

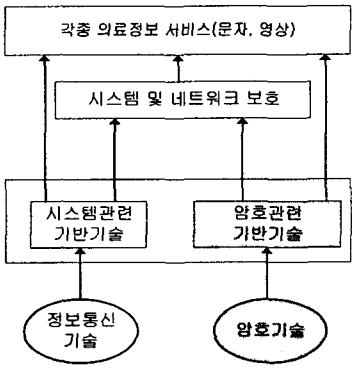
이 알고리즘은 기본적으로 비선형 변환과 선형 변환의 적절한 조합에 의해 설계되었으며, 알고리즘의 전체 구조는 데이터 블록의 좌우 측면에 교대로 비선형 변환을 적용시키는 Feistal 구조를 적용하여 설계하였다[6].

2. 의료정보와 정보보호

의료정보라 함은 환자와 의사를 중심으로 또는 그와

연관되어 발생되는 모든 자료 즉 환자기록, 진료기록, 환자와 관련된 검사자료, 영상자료, 처방전 등 임상자료뿐만 아니라 이와 관련되어 지불해야하는 진료비 및 의약품관련 자료 등을 말한다. 이러한 정보들이 병원 내에서뿐만 아니라 의약분업, 원격진료 등과 관련되어 원외약국, 1차 진료기관, 2차 진료기관들 사이에서 환자 관련 기록의 이동, 처방전의 전송 시 이들 정보의 정확성 및 안전성을 위하여 보안문제는 가장 중요한 문제 중의 하나이다.

컴퓨터 기반 환자기록에는 단순한 텍스트형의 정보에서부터 방사선 사진에 이르기까지 광범위하고 다양한 정보가 있으며 이러한 정보들을 많은 사람들이 이용하고 있으며 이 정보들은 의미론적으로 상호 연결되어 있어서 복잡하며 이 정보로 지원해야 할 목적도 다양하며 광범위하다. 특히 이 분야에서는 진료 및 처방 정보가 신속하고 정확하게 전달되어야 하는데 그러기 위해서는 통신매체도 중요하지만 그보다도 더 중요한 것은 정보의 안전성, 즉 보안문제이다. 그러므로 이러한 보안 문제를 해결하기 위한 제반장치가 마련되지 않는다면 환자들의 중요한 정보들에 대한 안전을 기대할 수 없게된다. 따라서 정보의 안전을 보장하기 위해서는 상대방을 확인함과 동시에 정보의 복제에 의한 정보의 부당한 누출이나 손상을 방지하는 대책이 필요하다. 즉 사용자들에 대한 인증을 수행하고 데이터에 부정이 없다는 것을 증명하는 구조가 갖추어져 있어야 하며 이러한 데이터들이 다른 사람들에게 노출되어 손상을 입는 일이 없이 기밀성을 보장하는 암호화 및 복호화가 필요하다. 최근 네트워크의 발달에 따른 개방형 통신망을 통하여 개인의 생명과 관계된 중요한 정보들이 손쉽게 상대방에게 전달된다. 따라서 개인의 생명과 관계된 정보들에 관한 보안 문제는 더욱 더 중요하게 처리해야할 문제이다. 의료정보 서비스의 정보보호를 위한 기술은 그림 1과 같이 분류할 수 있다.



(그림 1) 의료정보 서비스와 정보보호

의료정보 관련 프로토콜로 PACS란 의료 영상 특히 방사선학적인 진단 영상들을 디지털 형태로 획득(Acruisition)한 후, 고속의 통신망을 통하여 전송하고 과거의 X-ray 필름 보관 대신에 디지털 정보 형태로 의료영상을 저장하며, 방사선과 의사들과 임상 의사들이 기존의 필름 뷰박스(Film Viewbox)대신에 영상조회 장치를 통하여 표시되는 영상을 이용하여 환자를 진료하는 포괄적인 디지털 영상 관리 및 전송 시스템을 말한다[1].

PACS를 구현하기 위해서 영상 표시 및 처리 (Image display and processing), 정보통신 및 네트워킹(Data communication and Networking), 데이터베이스(Database), 정보관리(Information management), 사용자 인터페이스(User interface)와 정보 저장 관리(Data storage/ archive management) 등의 기술들을 종합하여야 한다. 이러한 PACS시스템을 효과적으로 구축하기 위한 4대 원칙은 첫째, 임상적으로 수용 가능한 우수한 기술을 도입하고 유지하여야 하고 둘째, DICOM(Digital *Imaging Communications in Medicine*)표준 방식을 따라야 하며 셋째, 필름 없는 시스템을 경제적이고 효과적으로 만들고 유지하여야 하며 넷째, 병원 정보 시스템의 기대에 부응하는 성능을 제공하여야 한다. 그래야만 PACS가 기존의 필름 중심의 업무보다 효과적으로 영상관리 업무를 향상시키며 환자 진료의 질도 향상시킬 수 있다[2].

DICOM은 의료영상 장치들 사이에서 의료 영상과 정보를 전송하는 업계표준 프로토콜로 미국 진단방사선과 협회와 의료장비업체간에 합의로 제안되었으며 유럽과 일본 그리고 우리나라 PACS학회와 의료장비업체들도 채택하고 있는 표준 프로토콜이다. DICOM은 의료 영상을 교환하고 구성하는 방법과 그에 관련된 정보들을 기술한 자세한 명세(Specification)이다. DICOM은 산업 표준 네트워크 연결을 사용하여 CT(Computed Tomography)와 MRI(Magnetic resonance imaging)를 비롯하여 핵의학, 초음파 등의 각종 디지털 영상 장비와 다른 정보 시스템 간의 통신을 효과적으로 지원하며, 필름 프린터와 같은 영상 출력 장비와도 연결하여 사용할 수 있도록 한다. 최근에는 대부분의 의료기 업체들이 DICOM표준을 수용하고 있는데 이는 의료 관련 기관들이 환자에 대한 서비스의 질을 향상시키고 의료 영상과 관련된 정보들을 다루는데 있어 통일성을 기하고 있다. DICOM프로토콜에서의 자료표현이 32비트씩으로 구성되어 있다.

블록 암호 시스템은 고정된 크기의 입력 블록을 고정된 크기의 출력 블록으로 변형하는 암호 알고리즘

에 의해 암호화 및 복호화 과정을 수행하며 출력 블록의 각 비트는 입력 블록과 키의 영향을 받아 결정된다. 정해진 블록 단위로 메시지를 처리하는 블록 암호 알고리즘이다. 대부분 현대의 블록 암호 알고리즘은 "confusion과 diffusion의 반복에 의하여 강력한 암호 알고리즘을 설계할 수 있다"고 하는 Shanon의 이론을 기반으로 설계되었다[3]. 즉, 혼돈(confusion)이론은 암호문 비트들의 통계적 분포가 평문 비트들의 통계적 분포에 어떻게 의존되는가를 판단하기 어렵게 만드는 것이고 확산(diffusion)이론은 평문의 각 비트들의 영향이 암호문 비트들에 어떻게 영향을 주는가를 판단하기 어렵게 만든다는 것이다. 따라서 이들 이론에 기초해서 만든 알고리즘들의 비도는 높아지는 장점이 있는 반면 단점으로는 블록 단위로 암호화가 이루어지므로 평문 비트들이 완전한 하나의 블록을 구성한 다음에 암호화의 과정이 이루어지므로 블록의 크기에 따라 지연 될 수 있으며 암호화 과정에서의 오류는 여러 변환에 영향을 미치므로 그 영향이 크다는 것이다. 블록 암호 시스템의 암호변환을 함수로 표현하면 다음과 같다.

$$C = f(P, K)$$

C는 암호문, P는 평문, K는 키, f는 합성 함수를 의미한다.

보통 n 비트 블록 암호 알고리즘이란 고정된 n 비트 평문이 동일한 길이를 갖는 n비트 암호문으로 바뀌는 것을 말하며 여기에서 말하는 n 비트는 블록의 크기를 나타낸다. 이러한 변형 과정에서는 암호화 및 복호화 시 동일한 키가 사용된다[4].

블록 암호 시스템은 크게 둘로 나눌 수 있는데 한 부분은 암호 알고리즘 부분 또 한 부분은 키 생성 부분으로 구성되며 실제로 암호 알고리즘은 공개되므로 비도는 키 생성부분에 의존해서 정해진다. 즉, 평문 블록의 길이를 n, 키 블록의 길이를 m 이라 하면 2^n개의 가능한 평문 블록과 2^m 에 대한 암호화 함수라고 하면 이 함수는 치환이 되거나 길이가 n인 평문 블록과 암호문 블록 사이는 일대일 대응이 된다[5].

3. 블록 암호 알고리즘의 설계

이 논문에서 제안하는 암호 알고리즘은 대칭 키 암호 알고리즘에 바탕을 두고 고정된 크기의 입력 블록을 고정된 크기의 출력 블록으로 변형하는 즉 블록 단위로 메시지를 처리하는 블록 암호 알고리즘이다. 현대의 암호학에 있어서, 대칭키 암호 알고리즘은 메시지의 비밀성을 제공하는 암호 시스템의 중요한 요소이다. 보통 n 비트 블록 암호 알고리즘이란 고정된 n 비트 평문이 동일한 길이를 갖는 n 비트 암호문으로 바뀌는 것을 의미하는데, 여기서 n 비트는 블록의 크기를 나타낸다. 결국 이러한 변형 과정에서 동일한 키인 암호키와 복호키가 작용하여 암·복호화를 수행하게 되는 것이다.

일반적인 Feistel의 구조를 바탕으로 한 이 암호 알고리즘은 입·출력문의 크기와 암호화에 사용되는 입력키의 크기가 각각 128비트이다.

제 1 단계에서는 평문을 4개의 32비트 단어로 나누어서 첫 번째 단계에서는 각각의 단어를 4개의 키워드와 배타 논리합을 한다. 제 2 단계에서는 16라운드의 순환이 일어나는데 16라운드의 첫 번째 단계는 이전의 라운드에서 나온 왼쪽 두 개의 단어는 다음 단계의 입력으로 사용된다. 그 다음엔 4개의 독립된 비 선형 함수 S-Boxes(Substitution Box]를 적용하여 치환하고 MDS 행렬을 이용하여 선형 혼합 단계를 거친다. S-Boxes와 MDS(Maximum distance separable) 행렬을 거친 결과를 두 개 모아서 조합시킨다. 그리고 두 개의 키워드가 더해진다. 이 두 개의 결과는 오른쪽 단어와 배타 논리합 된다. 다음 처리 단계를 위하여 왼쪽 반쪽과 오른쪽 반쪽이 바꾸어진다. 이 과정이 16번이 반복 적용되는 것이다. 그리고 제 2 단계 이후에 마지막 처리 단계는 바꿈이 반대로 이루어진다. 제 3 단계에서는 4개의 단어는 암호문을 생성하기 위해서 4개의 키 단어와 배타적 논리합을 수행한다.

원문 $p_0, \ldots, p_{15}$의 16 바이트(128비트)는 4개의 32 비트 단어, $p_0, \ldots, p_3$로 나누어진다.

그리고 첫 번째 단계에서 4개의 키워드와 배타적 논리합 된다.

$$R_{0,i} = P_i \oplus K_i \qquad i = 0,\ldots,3$$

두 번째 16라운드의 순환에서는 처음 두 개의 워드는 한 라운드의 입력으로 사용되고 세 번째 워드는 S-Boxes와 선형혼합단계를 거쳐서 나온 출력과 배타적 논리합 되고 한 비트가 오른쪽으로 시프트 된다. 네 번째 워드는 오른쪽으로 한 비트 순환된 후 이전 라운드에서 나온 두 번째 출력과 배타적 논리합 된다. 마지막으로 두 개의 반쪽 부분이 바꾸어진다. 아래의 표현에서 r은 1, ..., 15이고 ROR과 ROL은 처음 32비트 입력변수를 회전시키는 함수로 두 번째 입력변수는 회전되는 비트의 수를 나타낸다

$(F_{r,o}, F_{r,1}) = F(R_{r,0}, R_{r,1}, r)$

$R_{r+1,0} = ROR(R_{r,2} \oplus F_{r,0}, 1)$

$R_{r+1,1} = ROL(R_{r,3}, 1) \oplus F_{r,1}$

$R_{r+1,2} = R_{r,0}$

$R_{r+1,3} = R_{r,1}$

그리고 16라운드 후 마지막 처리단계에서는 마지막 처리단계의 자리바꿈을 하지 않고 확장키의 4개 단어와 배타적 논리합이 수행된다. 따라서 암호문 4개의 단어는 16바이트로 쓰여진다. 이러한 변형과정을 통해서 암호화 및 복호화를 수행하는 것이다.

$$Ci = R_{16,(i+2) \bmod 4} \oplus K_{i+4} \qquad i = 0,...,3$$

이 논문에서 제안하는 암호 알고리즘은 다음 기준에 의해서 설계되었다.

- 128비트 대칭형 블록 암호기이다.
- 128비트의 키길이를 갖는다.
- 알고리즘의 기본 구조는 Feistel구조를 이용한다.
- 라운드 수는 16라운드이다.
- 사용된 내부함수는 안전성이 입증된 치환테이블을 이용한다.
- 설계가 단순하고 분석과 구현이 쉽다.
- DICOM표준의 데이터 구조와 데이터 변환에 맞도록 내부처리의 단위를 4바이트씩(32비트)으로 하였다.

4. 블록 암호 알고리즘의 적용

제안한 블록 암호 알고리즘을 구현해본 환경은 다음과 같다.

- 시스템 : Pentium Pro 200MHz 이상
- 메모리 : 64MB 이상
- OS : Windows 98
- 컴파일러 : MS Visual C/C++ 6.0

이 알고리즘에서 암호화 하고자하는 file명을 받아들여서 암호화하여 중간 파일을 생성하고 다시 복호화하여 최종 파일을 만들었다.

이 알고리즘에서의 암호화 과정은 평문과 암호문의 크기가 각각 128비트이고 암호키는 내부적으로 128비트를 취하여 키 생성 알고리즘에 의해 생성된다.

이 논문에서는 AES2 후보 암호 알고리즘과 SEED 암호 알고리즘을 대상으로 성능을 비교 분석한 결과 타 알고리즘에 비해 암·복호화의 수행속도가 타 알고리즘에 비해 빠른 것으로 나타났다.

테스트를 위한 환경은 다음과 같다.

- 시스템 : Pentium Pro 200MHz
- 시스템 소프트웨어 : Windows 98
- 컴파일러 : MS Visual C/C++ 6.0
- 메모리 : 64MB

참고문헌

[1] 대한의료정보학회, "보건의료정보학", 현문사, pp 201-227, 1999.

[2] 한국보건정보교육학회, "보건정보학개론", 현문사, pp 211-238, 2000.

[3] C.E. Shannon. Communication Theory of Secrecy System. Bell System Technical Journal, vol.28, pp.656-715. October 1949.

[4] 이민섭, "현대 암호학", 교우사. 1999.

[5] 전자통신연구원, "암호학의 기초", 경문사, 1999.

[6] H. Feistel. W. A. Notz and J. L. Smith, "Some Cryptographic Techniques for Machine-to-Machine Data Communications," Proceedings on the IEEE, v. 63, n. 11, pp. 1545-1554, 1975.