심전도 신호의 특징 값을 이용한 암호화

김정환*, **김경섭***, 신승원*
건국대학교 의료생명대학 의학공학부*

Encryptions of ECG Signals by Using Its Fiducial Features

Jeong-Hwan Kim*, Kyeong-Seop Kim*, Seung-Won Shin*
School of Biomedical Engineering, Konkuk University*, Chungju, Korea

Abstract - 네트워크 기반 서비스를 이용하여 심전도 신호를 전송하는 과정에서 심전도의 특징 값을 조합한 one-time 템플릿 기반의 암호키를 생성하고 또한 이를 이용하여 심전도 신호를 암호화 하고자 하였다. 결과적으로 심전도 신호의 암호화/복호화 과정을 통하여 환자의 정보를 보호할 수 있는 생체 신호의 송수신 보안을 구현하고자 하였다.

1. 서 론

최근에 네트워크 기반의 서비스가 발달하면서, 네트워크로 의료정보를 전송하고 외부에서 정보를 획득이 가능한 원격 의료시스템 기술의 발전으로 인하여 의료분야의 서비스 질의 향상이 기대되고 있다. 그러나 의료정보에는 개인의 사적인 건강정보가 포함하기 때문에 해킹, 유출, 도용과 같은 불법적인 행위를 하여 개인의 신체적 상태에 관한 정보가 유출될 수 있다. 그러므로 의료 개인정보 보호는 상당히 중요한 사안이다. 또한 의료정보는 환자의 건강과 관련된 중요한 정보를 간직한 의무기록으로 해석된다. 즉, 의무기록은 환자를 진료하면서 경험한 것을 기록한 중요한 문서로 이를 통하여 환자의 치료방법 등을 결정할 수 있고, 다른 의사에게 처치를 넘기는 경우에도 필수적이며, 임상연구수행 및 치료적용에도 중요한 정보가 된다[1].

일반적으로 개인의 정보를 보호하기 위한 보안장치로 비밀키와 공개키 암호를 사용하는데, 두 방식 모두 장단점이 있다. 즉, 비밀키의 경우 암호화/복호화가 빠른 반면 키 관리가 어려운 단점이 있으며, 공개키의 경우 키 관리가 용이하고 안정성이 뛰어난 반면 처리 속도가 느리기 때문에 대용량의 데이터에 관한 암호화에는 부적합하다는 단점이 있다[2].

본 연구에서는 심전도 신호를 네트워크 기반서비스를 이용하여 송신하는 경우에서, 심전도 신호의 특징 값을 활용하여 one-time 템플릿 기반의[3] 암호키를 생성하고 암호화된 심전도 신호를 송신한 다음에, 이를 복호화하는 과정을 구현하였다.

2. 본 론

2.1 심전도 신호

심전도 신호는 심장이 수축과 이완에 따라서 발생하는 전기적 신호를 기록한 것이며, 심장상태와 질환을 진단할 수 있는 임상적 진단 파라미터를 제공한다. 즉, ***P***, ***Q***, ***R***, ***S***, ***T***라는 특징 값의 조합으로 해석되는 크기, 간격의 조합으로 이루어진 fiducial features 검출을 통하여 심장 기능의 이상여부를 판단할 수 있는 판단 근거로 사용된다[4].

P 파는 심방의 탈분극에 의해 발생되는 파형으로 심방의 흥분을 나타내며, 심방에서 심실로 전되는 과정에서 유도된다. 또한 ***Q*** 파는 심실 격벽 탈분극을 나타내며, ***R*** 파는 심실의 탈분극, ***S*** 파는 심실 기저부의 탈분극을 나타낸다. ***QRS*** complex는 약 0.1초 이내로 심장 전체의 탈분극 과정을 나타내며, 심실의 흥분과정에서 유도된다. 마지막으로 ***T*** 파는 심실의 재분극 과정에서 심실 흥분의 회복과정에서 발생된다.

2.2 심전도 신호의 암호화 및 복호화 과정

심전도 신호에 대한 암호화 알고리즘 적용은 암호화와 복호화 과정으로 구성되며, 각각 암호화 (복호화) 키를 심전도 신호에 반영하여 복호화 과정이 이루어진다.

식 (1)에서 $e(n)$은 N개의 $x_1, x_2, x_3, \ldots, x_N$ 데이터로 이루어진 심전도 신호를 의미한다.

$$e(n) = [x_1, x_2, x_3, \ldots, x_N] \quad (1)$$

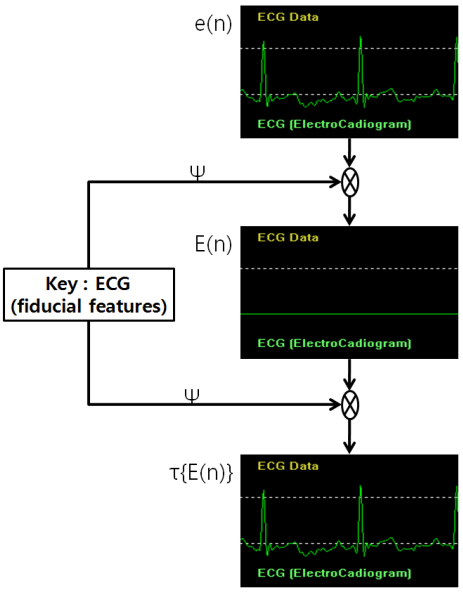
심전도 신호의 암호화 과정 $E(n)$은 암호키 Ψ를 이용하여 심전도 신호를 암호화하는 과정으로서 식 (2)와 같은 연산과정을 거친다.

$$E(n) = e(n) \otimes \Psi \quad (2)$$

여기서, 암호키는 심전도 신호를 전송할 때 심전도의 특징 값을 이용하여 생성된 one-time 템플릿 기반의 키이며, 식 (3)과 같은 복원과정이 수행된다.

$$\tau\{E(n)\} = E(n) \otimes \Psi \quad (3)$$

그림 1은 송·수신 과정을 통하여 심전도 신호가 암호화 및 복호화 되는 과정을 보여주고 있다.



<그림 1> 심전도 신호의 특징 값을 활용한 암호화 및 복호화 과정

2.3 심전도 신호의 특징점 검출

심전도 신호의 특징점을 검출하기 위하여 MIT/BIH 심전도 데이터를 활용하였다. 여기서 한 주기의 심전도 특징인 ***P***, ***Q***, ***R***, ***S***, ***T*** 점을 검출하기 위해 일정한 범위를 지정하여 특징점을 검출하는 방법을 선택하였다.

우선적으로 ***R***-peak를 검출하기 위해서 식 (4)와 같이 심전도 신호의 미분값인 $d(n)$을 구한다.

$$d(n) = e(n) - e(n-1) \quad (4)$$

제곱한 후에, 식 (5)와 같이 이동평균필터 기법을 사용하여 ***R***-peak 특성을 강조시킨다.

$$F(n) = \left(\frac{1}{5}\right) \cdot \sum_{N=-2}^{2} g(n+N)^2 \quad (5)$$

따라서 식 (5)에서 구한, 심전도 신호 데이터의 최대값이 R-peak이고 한 주기를 200 샘플로 가정하면, 반복적으로 R-peak를 검출할 수 있고, 또한 R-R 간격도 구할 수 있다.

Q-peak를 검출하기 위해서 R-peak 값에서 좌측방향으로 일정한 범위내의 신호 차이를 구해보면 R 값과 신호 사이의 최대로 차이가 생기는 지점이 발생하게 된다. 바로 이 지점이 Q-peak로 해석되며 S-peak 또한 Q-peak 검출법과 같은 방법으로 R-peak의 우측방향으로 일정한 범위를 지정하고 R 값과 최대 차이가 발생하는 지점을 S-peak로 해석한다.

또한 P-peak를 구하기 위해서는 위에서 구한 Q-peak 지점을 중심으로 좌측으로 R-R 간격의 (1/3) 크기만큼 범위를 지정하여 이 범위 안에서 최대값을 갖는 지점을 찾을 수 있는데, 이를 P-peak 지점으로 정의한다.

마지막으로 S-peak에서 우측으로 R-R 간격의 (1/2) 크기만큼 범위를 지정하여 S 값의 범위 내 각각의 신호의 최대값을 갖는 지점을 T-peak 값으로 해석된다.

위에서 제시한 방법으로 심전도 신호의 특징점들을 모두 검출하면 변곡점들이 발생한 시간을 구할 수 있다. 표 1은 MIT/BIH data(ECG_100_1) 신호에 대해서 $PQRST$ 변곡점들을 구한 다음에 이를 이용하여 심전도 신호의 fiducial features를 보여주고 있다.

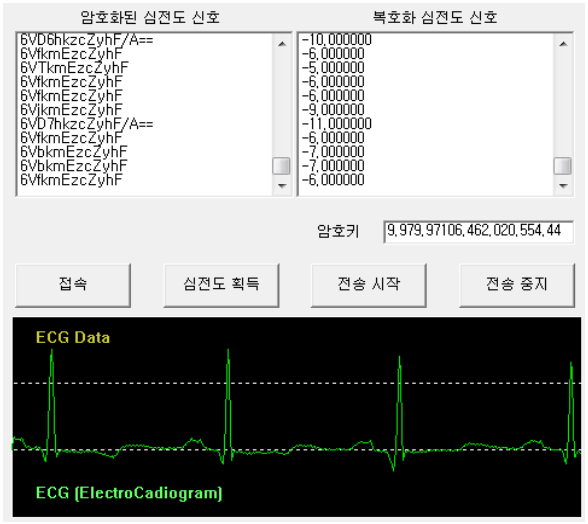
<표 1> MIT/BIH(ECG_100_1) 심전도 신호의 fiducial features

P-P	R-R	T-T	P-T	P-R	QRS	R-T
0.92	0.92	0.9	0.58	0.2	0.06	0.38
0.93	0.88	0.88	0.56	0.2	0.04	0.36
0.83	0.89	0.96	0.51	0.15	0.05	0.36
0.94	0.89	0.88	0.64	0.21	0.05	0.43
0.88	0.92	1.05	0.58	0.16	0.05	0.42
0.75	0.73	0.57	0.75	0.2	0.05	0.55
1.09	1.12	1.15	0.57	0.18	0.05	0.39
0.96	0.95	0.92	0.63	0.21	0.06	0.42
0.96	0.92	0.90	0.59	0.2	0.05	0.39
0.89	0.88	0.88	0.53	0.16	0.05	0.37
0.82	0.87	0.91	0.52	0.15	0.04	0.37

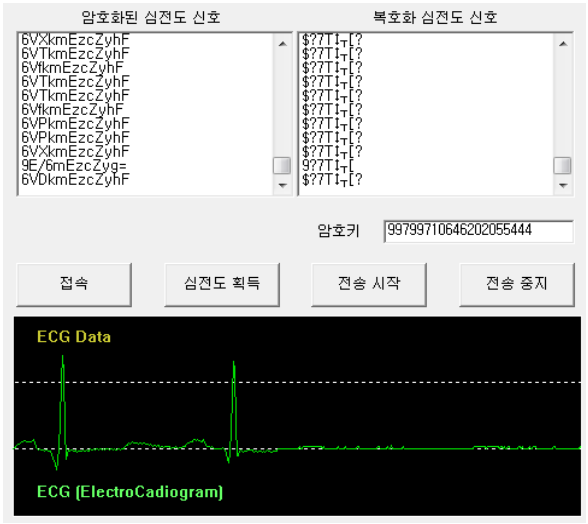
결과적으로 표 1에서 표현된 fiducial features의 조합을 이용하여, 심전도 신호를 암호화 시킬 수 있는 one-time 템플릿 기반의 "암호화 키"를 생성할 수 있다.

2.4 심전도 신호의 복호화

그림 2는 네트워크 기반의 송·수신 과정을 통하여 심전도 신호가 암호화 및 복호화 되는 과정을 보여주고 있다. 여기서 사용한 암호키는 표 1에 나열된 특징값들의 조합으로 도출된 키를 활용하였다. 또한 그림 2는 송신자가 심전도 신호를 전송할 때 입력한 암호키가 수신자와 동일한 경우 송신 데이터 값이 성공적으로 복호화 되어서 심전도 신호를 복원하는 과정을 보여준다.



(a)



(b)

<그림 2> 심전도 신호의 암호화/복호화 송수신 과정
(a) 암호키가 인증된 경우
(b) 암호키가 인증되지 않은 경우

3. 결 론

네트워크 기반의 클라이언트/서버 환경에서 심전도 신호의 송수신 보안성을 확보하기 위해서, 심전도 신호의 특징값을 이용하여 one-time 템플릿 기반의 암호키를 생성시키는 알고리즘을 구현하였다. 추후로 생체 암호키를 심전도 신호와 함께 전송될 때 수신단에서 생체 암호키를 복원할 수 있는 방법에 대한 연구가 이루어져야 할 것으로 사료된다.

[Acknowledgement]

"이 논문은 2011년 교육과학기술로부터 지원받아 수행된 연구임"(지역거점 연구단원성 사업 / 충북 BIT 연구중심대학 육성사업단)

[참 고 문 헌]

[1] 김상겸, "독일의 의료정보와 개인정보보호에 관한 연구," 한·독사회과학논총, 제 15권 제 2호, pp. 9-12, 2005.
[2] 강선명, "Visual C++ 암호화 프로그래밍," 2003.
[3] 정윤수, "One-time 템플릿 기반의 바이오인증 프레임워크 표준," 정보처리학회지, 제 18권, 제 4호, pp. 61-65, 2008.
[4] John G. Webster, Medical instrumentation, 1998.