논 문
60-12-32

심전도 신호의 특징 값을 이용한 암호화

Encryptions of ECG Signals by Using Fiducial Features

김 정 환* · 김 경 섭† · 신 승 원** · 류 근 호***
(Jeong-Hwan Kim · Kyeong-Seop Kim · Seung-Won Shin · Keun Ho Ryu)

Abstract - With the advent of ubiquitous healthcare technology to provide a patient with the necessary medical services in anywhere and anytime scheme, the importance of securing safe communication without tampering the medical data by the unauthorized users is getting more emphasized. With this aim, a novel method for constructing encryption keys on the basis of biometrical measurement of electrocardiogram (ECG) is suggested in this study. The experiments on MIT/BIH database show that our proposed method can achieve safe communication by successfully ciphering and deciphering ECG data including premature ventricular contraction arrhythmia signal with compromising its fiducial features as biometric key to transmit the data via the internet network.

Key Words : ECG, Fiducial feature, Encryption, Decryption, Key

1. 서 론

의료정보는 의사가 환자에 대한 의료행위 수행을 통하여 수집된 환자의 신상정보, 병력, 진단명, 질환 상태, 치료 행위 및 경과 과정을 포함하는 포괄적인 사항들을 기록한 의무기록이며 기본적으로 환자가 아닌 타인에게 공개되지 않는 것이 원칙이다. 그러나 의료정보는 그 특성상 전문적인 의학지식의 해석을 필요로 하는바, 의사가 환자보다 정보의 내용을 더 정확히 이해하고 있고 또한 담당의사의 주관적인 판단아래 일부 내용이 외부에 공개될 수 있다는 특징을 갖는다. 이에 따라서 미국의 경우 개인의 의료정보 보호를 위한 HIPAA (Health Insurance Portability and Accountability Act)[1] 법률이 제정된 바가 있으며 국내에서도 개인 정보의 보호를 강화하는 추세에 따라서 의료정보의 보안에 대한 중요성이 강조되고 있지만, IT 기술이 활용된 네트워크를 기반으로 하여서 의료정보의 송수신이 자주 발생하고 또한 환자와 관련된 의료기관 사이에서 정보공유가 이루어지고 있는 실정이다. 또한 언제, 어디서나 환자의 건강관리 및 의료서비스를 제공하는 U-Health 서비스 도입으로 인하여 의료정보의 전송 및 교환이 자주 발생함으로써 의무기록의 전산화로 인한 이점에도 불구하고 불법적인 해킹, 정보의 고의적 유출 도용과 같은 행위를 통하여 환자의 프라이버시가 침해될 위험성이 점점 높아지고 있다.

일반적으로 정보를 전송하는 경우, 송신자가 암호화 키를 사용하여 의료정보 데이터를 암호화하여 전송하고 복호화 키를 가진 수신자가 암호화된 메시지를 해독하는 기법을 사용하는데 의료정보의 보안에도 동일한 방법이 적용될 수 있다. 암호화 키의 설정을 위해서 대칭 키 (비밀 키) 또는 비대칭 키 (공개 키)가 활용될 수 있는데, 비밀 키를 사용하면 암호화 및 복호화 과정이 빠른 반면에 키 관리가 어려운 단점이 있는 반면에 공개 키의 경우 키 관리가 용이하고 안정성이 뛰어나지만 암호화 및 복호화 수행 과정이 느리기 때문에 대용량의 데이터의 암호화에 부적합하다는 단점이 존재한다[2-3]. 기본적으로 암호화 전송기법은 송수신자 모두 동일하게 64비트 블록과 56비트의 키로 구성된 DES (Data Encryption Standard) 대칭 키를 사용하여 데이터를 암호화하는 대칭 키 암호방식 기법, 소인수분해 개념을 이용하여 설정된 2개의 비대칭 키를 사용하는 RSA (Rivest-Shamir-Adleman) 암호방식 기법 그리고 RSA 비대칭 키와 대칭 키를 혼합한 암호화 기법이[4] 사용되고 있다. 그러나 이런 유형의 암호화 송수신 기법에서 사용되는 키를 생성하는 과정에서 의료정보 특히 환자의 생체 정보 (예를 들면 심전도, 뇌전도, 의료영상)를 송수신하는 경우 환자 데이터 자체의 특성을 전혀 활용하지 못한다는 단점이 존재한다.

개인의 생체 정보를 활용하여 암호화 키를 생성시키는 기법과 연관하여 Vladimir B. Balakirsky[5-7] 연구진은 한 개인의 유전자 정보의 일부인 28개의 요소들로 구성된 일종의 생체인증 데이터를 활용한 암호 키를 사용하였는데 본 연구에서는 환자의 생체신호를 송수신하는 과정에서, 신호의 특성 값을 도출하고 이를 이용한 비밀 키를 생성하여서 송수신 보안을 위한 암호화 및 복호화 기법을 제시하고자 하였으며 특히 환자의 심전도 신호의 송수신 보안을 위해서 심

* 준 회 원 : 건국대 의료생명대 의학공학부 석사과정
† 교신저자, 정회원 : 건국대 의료생명대 의학공학부 교수
건국대 의공학실용기술연구소 · 공박
E-mail : kyeong@kku.ac.kr
** 정 회 원 : 건국대 의료생명대 의학공학부 박사과정
*** 비 회 원 : 충북대 전자정보대학 소프트웨어전공 교수
접수일자 : 2011년 9월 22일
최종완료 : 2011년 11월 16일

전도 파형을 표현하는 특징 값들의 조합으로 이루어진 암호키를 생성하여 심전도 신호를 암호화 하여 전송한 다음에, 이를 수신하여 복호화 하는 기법을 제시하고자 하였다.

2. 본 론

2.1 심전도

심전도는 심장이 수축과 이완에 따라서 발생하는 전기적 신호를 기록한 것이며, 심장 질환을 진단할 수 있는 임상적 진단 파라미터를 제공한다. 예를 들면, 심전도 파형의 변화 지점을 표시하는 P, Q, R, S, T라는 특징 값의 조합으로 해석되는 신호의 크기, 거리, 모폴로지로 구성된 형태는 features 검출을 통하여 심전도 해석의 중요한 임상적 소견을 제공한다[8].

그림 1은 심전도 신호 파형의 특성을 표현하는 변곡점들과 이에 따른 신호 크기 및 간격으로 표현된 fiducial features의 예를 보여주고 있다.

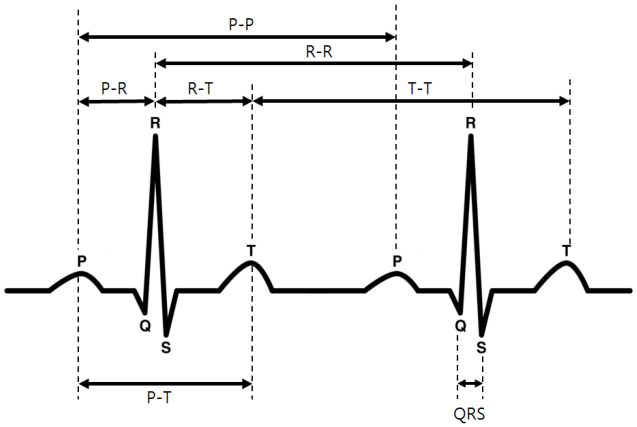


그림 1 심전도 신호의 특징 값
Fig. 1 Fiducial features of ECG signal

그림 1에서 표현된 정상적인 심전도 파형 이외에 비정상적인 리듬을 갖는 부정맥(arrhythmia) 심전도 신호가 발생할 수 있다. 부정맥 신호의 종류는 크게 정상 리듬의 심박수보다 심하게 느려지는 서맥성 부정맥과 심장의 수축·이완 리듬이 정상속도보다 빨라지는 빈맥성 부정맥으로 분류되는데, 이 중 심실조기수축(PVC: Premature Ventricular Contraction)은 동방결절에서 발생하는 정상적인 박동 이외에 심실근에서 시작되는 이상흥분으로 인하여 발생한다. PVC 부정맥 신호는 신경성 이상흥분 또는 피로, 흡연, 음주로 인하여 야기될 수 있다. PVC 부정맥은 일반적으로 특별한 문제가 되지 않지만 경우에 따라서 심실세동, 심실빈맥과 같은 위험한 상태로 진행되기도 한다[9]. 그림 2는 PVC부정맥 부분이 존재하는 심전도 신호를 보여주고 있다.

그림 2 PVC 부정맥 심전도 신호의 특징 구간
Fig. 2 PVC arrhythmia ECG signal

2.2 심전도 신호의 암호화 및 복호화

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

식 (1)에서 $e(n)$은 N개의 $X_1, X_2, \ldots, X_N$ 데이터로 이루어진 심전도 신호를 의미한다.

$$e(n) = [X_1, X_2, ..., X_N] \tag{1}$$

심전도 신호에 대한 암호화 과정 $E(n)$은 암호키 Ψ를 이용하여 식 (2)와 같이 변환된다.

$$E(n) = e(n) \otimes \Psi \tag{2}$$

여기서, 암호키는 심전도 신호를 전송할 때 심전도의 특징 값을 이용하여 생성된 one-time 템플릿 기반의 키[10]이며, 식 (3)과 같이 복원과정이 수행된다.

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

그림 3은 네트워크 기반의 송·수신 과정을 통하여 수행되는 심전도 신호의 암호화 및 복호화 과정을 보여주고 있다.

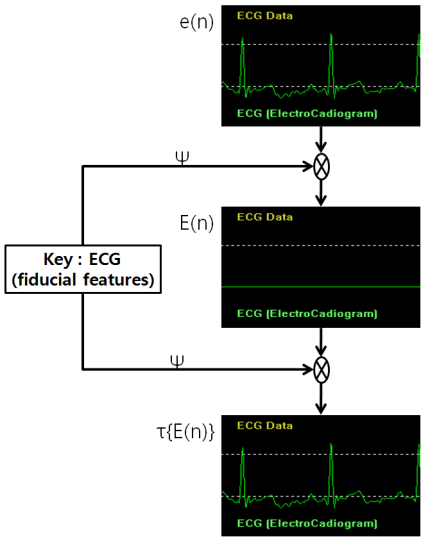


그림 3 심전도 신호의 암호화 및 복호화 과정
Fig. 3 Encryption and Decryption of ECG signal

그림 4는 Visual C++ 기반으로 심전도 신호의 암호화 및 복호화 과정을 구현한 GUI (Graphic User Interface) 설계 화면을 보여준다.

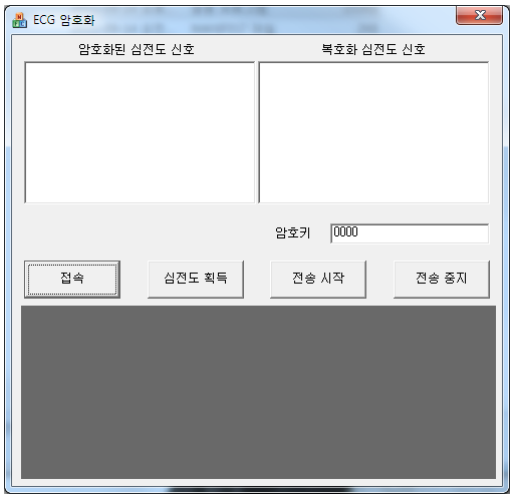


그림 4 심전도 암호화 및 복호화 GUI 화면
Fig. 4 GUI for transmission of encrypted ECG signal

그림 5는 심전도 신호를 Visual C++ 기반의 암호화 기능을 구현하는 crypto API 함수들을 설명하고 있다[11].

HCRYPTPROV: 해쉬 오브젝트 핸들 HCRYPTKEY: 암호화키 핸들 HCRYPTHASH: CSO 핸들
CryptAcquireContext(): CSP의 key-container 핸들 CryptCreateHash(): 빈 해쉬 오브젝트를 생성 CryptHashData(): 해쉬 오브젝트 추가 CryptDeriveKey(): 패스워드로부터 키 생성
CryptEncrypt(): 암호화키를 이용한 평문 암호화 CryptBinaryToString(): binary 데이터를 문자열의 형태로 인코딩
CryptDestroyHash(): 해쉬 오브젝트 소멸 CryptDestroyKey(): 키 파괴 CryptReleaseContext(): CryptAcqureContext 핸들 release

그림 5 Visual C++ "Crypto" 암호화 API
Fig. 5 Visual C++ "Crypto" encryption API

복호화 과정을 구현하기 위해서, 암호화 API 함수들을 동일하게 사용하지만 CryptEncrypt() 함수 대신에 CryptDecrypt() 함수(특정 암호화 키로 생성된 암호문을 복호화 함)를 사용하고 CryptBinaryToString() 함수 대신에 CryptStringToBinary() 함수(문자열에서 binary데이터 추출)를 사용한다.

2.3 C/S (Client/Server) 기반의 데이터 송수신

클라이언트가 서버에 접속해서 데이터를 주고 받으려면 데이터 소켓을 클라이언트와 서버에 각각 하나씩 가지고 있어야 하고, 서버에는 클라이언트의 접속요청을 받아들일 수 있는 서버 소켓을 추가적으로 가지고 있어야 한다. 서버 소켓에서 먼저 "Create" 함수를 호출해서 서버 소켓을 생성하고 "Listen" 함수를 호출해서 클라이언트의 접속요청을 감지한다. 이에 따라서 클라이언트가 서버에 접속하기 위해서는 "Create" 함수를 호출해서 소켓을 생성하고 서버의 TCP/IP 주소와 포트 번호를 지정하여 "Connect" 함수를 사용하여 서버에 접속을 요청한다. 클라이언트로부터 접속요청을 받은 서버 소켓은 별도의 데이터 소켓을 생성하고, "Accept" 함수를 수행하여 새로이 생성된 소켓과 클라이언트를 연결시켜 준다. 이때, 소켓이 클라이언트와 데이터를 송수신 역할을 담당하는데, 데이터를 송신할 때는 "Send" 함수를, 또한 수신할 때는 "Receive" 함수를 실행시킨다. (그림 6 참조)

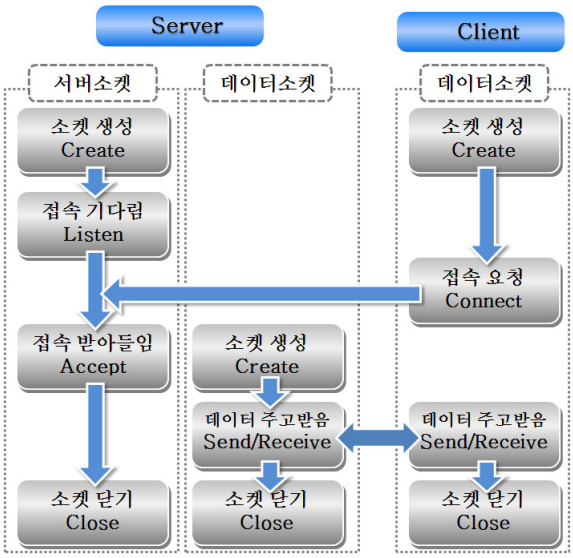


그림 6 클라이언트와 서버의 데이터 송·수신 프로토콜
Fig. 6 Data transmission protocol with C/S model

2.4 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.

$$d(n) = e(n) - e(n-1) \tag{4}$$

이 값을 제곱한 후에, 식 (5)와 같이 이동평균필터(moving average filtering) 기법을 사용하여 R-peak 값을 강조한다. 여기서 필터의 구간 길이는 5로 하였다.

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

결과적으로, 식 (5)의 값을 기준으로 해서 데이터의 최대값이 R-peak이고 또한 한 주기를 200개로 이루어 졌다고 가정하면, 반복적으로 R-peak를 검출할 수 있고, 아울러서 R-R 간격도 구할 수 있다. Q-peak를 검출하기 위해서 R-peak 값에서 좌측방향으로 일정한 범위내의 신호 차이를 구해보면 R-value와 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-peak점을 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 값과 범위 내 각각의 신호의 최대값을 갖는 지점을 T-peak라고 해석한다.

Case I: 표 1은 MIT/BIH data (ECG_100_1) 신호에 대해서 PQRST 변곡점들을 구한 다음에 이들의 거리 조합으로 이루어진 features를 보여주고 있다.

표 1 MIT/BIH(ECG_100_1) 심전도 신호의 fiducial features
Table 1 Fiducial features of MIT/BIH (ECG_100_1)

O_1 P-P	O_2 R-R	O_3 T-T	O_4 P-T	O_5 P-R	O_6 QRS	O_7 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

Case II: 표 2는 PVC를 포함한 MIT/BIH data (ECG_119_1)신호에 대해서 R 변곡점을 포함하는 심전도 신호 feature를 보여주고 있다.

표 2 MIT/BIH(ECG_119_1) 심전도 신호의 fiducial features
Table 2 Fiducial features of MIT/BIH (ECG_119_1)

O_1 P-P	O_2 R-R	O_3 T-T	O_4 P-T	O_5 P-R	O_6 QRS	O_7 R-T
1.59	1.49	1.12	0.98	0.26	0.17	0.72
1.03	1.05	1.06	0.51	0.16	0.06	0.35
1.04	1.05	1.04	0.54	0.18	0.06	0.36
1.02	1.00	0.98	0.54	0.19	0.06	0.35
1.52	1.62	2.02	0.50	0.17	0.06	0.33
1.56	1.46	1.09	1.00	0.27	0.19	0.73
1.06	1.07	1.04	0.53	0.17	0.06	0.36
0.98	0.99	0.99	0.51	0.18	0.06	0.33
0.96	0.97	0.98	0.52	0.19	0.06	0.33

PVC를 포함한 부정맥 심전도 신호는 R-peak를 제외한 나머지 특징점들이 정확하게 도출되지 않으므로 이런 경우 R-R 값의 조합으로 이루어진 암호화키를 선택하는 것이 좋다. 따라서 표 1, 2에서 표현된 심전도 신호의 fiducial features 조합을 이용하여 심전도 신호를 암호화시킬 수 있는 one-time 템플릿 기반의 "암호화 키"를 다음과 같이 생성할 수 있다.

즉, $O_1, O_2, ..., O_\ell$ 을 심전도 신호의 특징 점들의 조합으로 이루어진 시간상의 거리를 표현하는 값으로 설정하면, 암호화 키 Ψ는 식 (6)과 같이 생성될 수 있다.

$$\Psi = [f_1(O_1) f_2(O_2) ... f_\ell(O_\ell)] \quad (6)$$

따라서 심전도 신호의 암호화 과정은 식 (7)과 같은 과정을 거치고 또한 복호화 과정은 식 (8)의 과정으로 구현된다.

$$E(n) = e(n) \otimes [f_1(O_1)\ f_2(O_2)\ \ldots\ f_\ell(O_\ell)] \quad (7)$$

$$\tau\{E(n)\} = E(n) \otimes [f_1(O_1)\ f_2(O_2)\ \ldots\ f_\ell(O_\ell)] \quad (8)$$

만약에 심전도 신호가 비정상적인 리듬을 갖는 부정맥 신호의 특성을 갖게 되면 특징 값들의 일부만으로 (예를 들어 R-R 거리) 조합된 암호화 키를 생성한다.

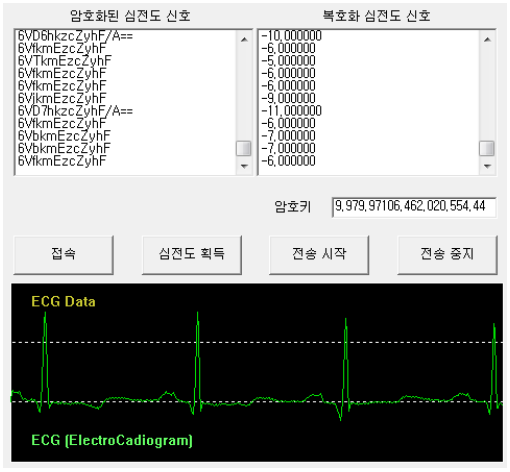
3. 결 과

그림 7은 네트워크 기반의 송·수신 과정을 통하여 심전도 신호가 암호화 및 복호화 되는 과정을 보여주고 있다. 여기서 사용한 암호키는 표 1, 2에서 나열된 특징 값들의 조합으로 도출된 키를 활용하였다. 또한 그림 7, 8, 9는 송신자가 입력한 암호키가 수신자와 동일한 경우 암호화된 심전도 신호가 성공적으로 복원되는 과정을 보여준다.

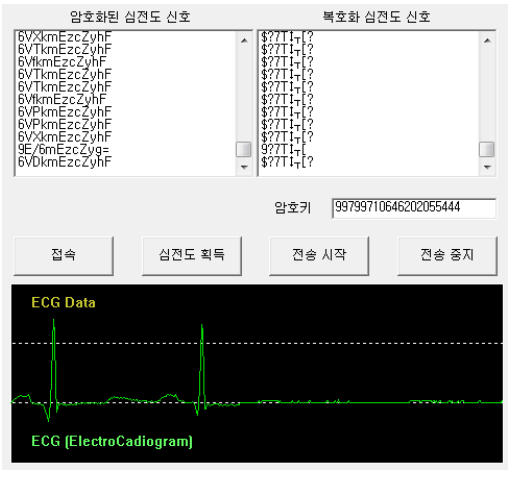
Case I: 암호화 키 $\Psi = [f_1(O_1)\ f_2(O_2)\ \ldots\ f_7(O_7)]$,

$$f(O_i) = (\frac{1}{N}) \cdot \sum_{\ell=1}^{N} O_i^{\ell}$$

여기서 O_i^{ℓ} : i_{th} 특징 값의 조합으로 이루어진 ℓ_{th} 거리



(a)



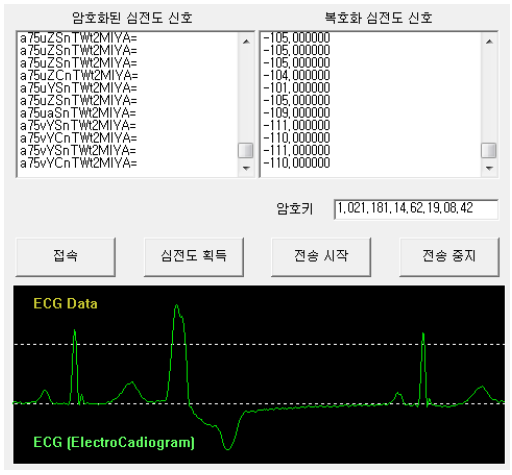
(b)

그림 7 심전도 신호의 암호화/복호화 송수신

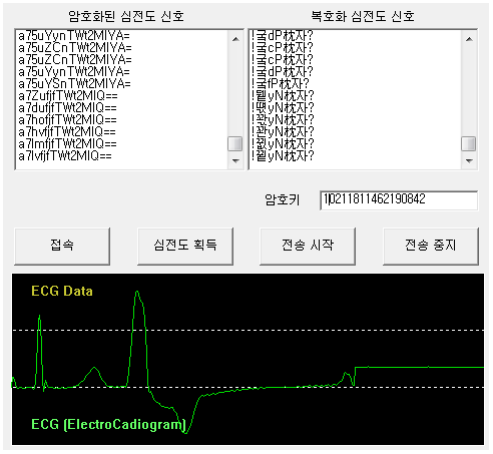
Fig. 7 Encryption and Decryption of ECG signals (a) 암호키가 인증된 경우 (b) 암호키가 인증되지 않은 경우

CaseII - a: 암호화 키 $\Psi = [f_1(O_1)\, f_2(O_2) \ldots f_7(O_7)]$

$$f(O_i) = (\frac{1}{M}) \cdot \sum_{\ell=1}^{M} O_i^{\ell}$$



(a)



(b)

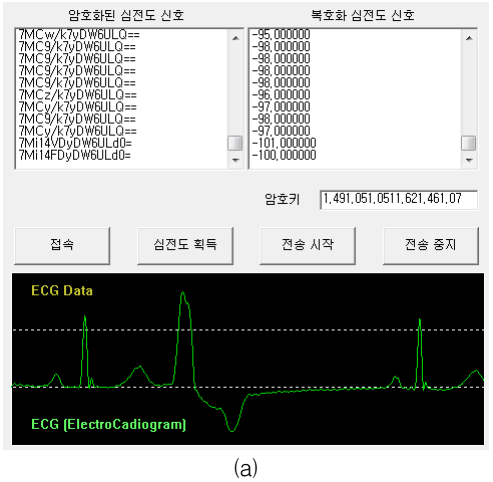
그림 8 PVC 신호의 암호화/복호화 송수신

Fig. 8 Encryption and Decryption of PVC arrhythmia (a) 암호키가 인증된 경우 (b) 암호키가 인증되지 않은 경우

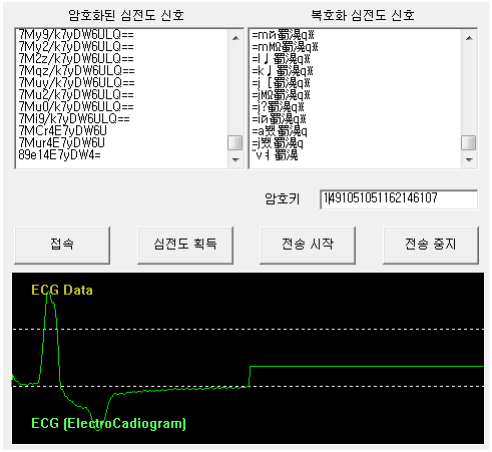
CaseII - b: 암호화 키 $\Psi = [f_1(O_R)]$,

$$f(O_R) = (\frac{1}{M}) \cdot \sum_{\ell=1}^{M} O_R^{\ell}$$

O_R^{ℓ} : R-R 간격으로 이루어진 ℓ_{th} 거리



(a)



(b)

그림 9 PVC 신호의 암호화/복호화 송수신

Fig. 9 Encryption and Decryption of PVC arrhythmia (a) 암호키가 인증된 경우 (b) 암호키가 인증되지 않은 경우

4. 결 론

네트워크 기반의 클라이언트/서버 환경에서 심전도 신호의 송수신 보안성을 확보하기 위해서 심전도 신호의 특징값을 기반으로 하여서 one-time 템플릿 기반의 암호키를 생성시키는 방법을 구현하였다. 따라서 각 개인마다 고유하게 특성 값의 조합으로 표현되는 심전도 신호의 features를 이용하여 암호화 키를 설정할 수 있는 가능성을 제시하였다. 추후로 생체 암호키를 심전도 신호와 함께 전송될 때 수신단에서 이 생체 암호키를 획득할 수 있는 방법에 대한 연구가 이루어져야 할 것으로 사료된다.

감사의 글

이 논문은 2011년 교육과학기술부로부터 지원받아 수행된 연구임(지역거점연구단 육성사업 / 충북 BIT 연구중심 대학육성사업단)

참 고 문 헌

[1] Steve Bass, Lisa Miller, Bryan Nylin, “HIPAA (히파) 호환 솔루션 구현을 위한 전략,” 정보문화사, 2002.

[2] 김상겸, “독일의 의료정보와 개인정보보호에 관한 연구,” 한·독사회과학논총, 제 15권 제 2호, pp. 9-12, 2005.

[3] 임채균, 이기영, 임명재, 정용규, “의료정보보안의 현황과 전망,” 전자공학회지 제 37권 6호, pp. 587-589, 2010.

[4] 허진경, “분산 암호화를 이용한 웹 어플리케이션 보안,” 한국 콘텐츠 학회 논문집, 제 8권 4호, pp. 10-16, 2008.

[5] Vladimir B. Balakirsky, Anahit R. Ghazaryan, A. J. HanVinck, “Constructing Passwords from Biometrical Data,” ICB200, pp. 889-898, 2009.

[6] V. B. Balakirsky, A. R. Ghazaryan, A. J. HanVinck, "Additive block coding schemes for biometric authentication with the DNA data," BIOID, 2008, LNCS, Vol. 5372, pp.160-169, Springer, Heidelberg, 2008.

[7] V. B. Balakirsky, A. R. Ghazaryan, A. J. HanVinck, "Mathematical model for constructing passwords from biometrical data," Security and Communication Networks, Vol. 2(1), pp. 1-9, Wiley, 2009.

[8] John G. Webster, Medical instrumentation, 1998.

[9] 오용성 역, “쉽게 이해하는 심전도,” 4판, 대한의학서적, 2001.

[10] 정윤수, “One-time 템플릿 기반의 바이오인증 프레임워크 표준,” 정보처리학회지, 제 18권, 제 4호, pp. 61-65, 2008.

[11] 강선명, “Visual C++ 암호화 프로그래밍,” (주)프리렉, 2003.

저 자 소 개

김 정 환 (金 柾 桓)

2011년 건국대학교 의학공학부 졸업. 2011년~현재 동대학원 석사과정 재학 중.

김 경 섭 (金 敬 燮)

1979년 연세대학교 전기공학과 졸업. 동대학원 석사 (1981). The University of Alabama in Huntsville, Ph.D. (1994). 2001년~현재 건국대학교 의학공학부 교수.

신 승 원 (辛 承 元)

2005년 건국대학교 의학공학부 졸업. 동대학원 석사 (2007). 2007년~현재 동대학원 박사과정 재학 중.

류 근 호 (柳 根 鎬)

1976년 숭실대학교 전산학과 졸업. 연세대학교 전산전공 석사 (2007). 동대학원 박사 (1988). 1986년~현재 충북대학교 전자정보대학 소프트웨어전공 교수.