Journal of the Korea Convergence Society
Vol. 8. No. 3, pp. 115-121, 2017
https://doi.org/10.15207/JKCS.2017.8.3.115

헬스케어 환경을 위한 칼라 모델 기반의 사용자 인증 키 설립 기법

정윤수
목원대학교 정보통신융합공학부

User Authentication Key Establishment Scheme based on Color Model for Healthcare Environment

Yoon-Su Jeong
Dept. of information Communication Convergence Engineering, Mokwon University

요 약 병원의료 서비스는 사용자의 헬스케어 정보를 융합하여 신속한 의료서비스를 사용자에게 제공하거나 의료서비스의 질 개선을 위해서 많은 노력을 하고 있다. 그러나, 최근 연구에서는 사용자의 헬스케어 정보를 유·무선을 통해 병원 서버에 전달하려고 할 때, 사용자의 헬스케어 정보가 노출되는 문제점이 있다. 본 논문에서는 사용자의 헬스케어 정보를 안전하게 전달하기 위한 칼라 모델 기반의 사용자 인증 키 설립 프로토콜 기법을 제안한다. 제안 기법은 칼라 모델에서 사용되는 칼라 정보를 랜덤하게 3개 추출하여 추출된 임의의 정보를 벡터화하여 사용자 인증에 필요한 키 정보를 직교 벡터의 합으로 구함으로써 효율성을 높이는 것을 목적으로 한다. 또한, 제안 기법은 추가적인 암호 알고리즘을 사용하지 않으면서 사용자 인증에 필요한 키 정보를 안전하게 생성할 수 있다. 성능 평가 결과, 제안 기법은 사용자의 헬스케어 정보의 수가 증가할수록 생성된 정보를 처리하는 서버의 시간이 기존 기법보다 평균 8.1% 낮게 나타났으며, 오버헤드는 기존 기법보다 7.7% 낮은 결과를 얻었다.

• **주제어** : 칼라 모델, 인증, 프로토콜, 헬스케어, 융합

Abstract Hospital medical services are making great efforts to provide prompt medical services to patients or improve the quality of medical services by convergence patient's healthcare information. However, recent research suggests problems about safety and efficiency when trying to transmit patient's healthcare information to hospital server via radio and wireless. In this paper, we propose a color model - based patient authentication key establishment protocol method to securely transmit patient healthcare information. The proposed method extracts randomly three color information used in the color model and vectorizes the extracted arbitrary information to obtain the key information required for user authentication as the sum of orthogonal vectors to improve the efficiency. In addition, the proposed method can securely generate key information used for user authentication without using an additional encryption algorithm. In performance evaluation result, proposed method shows that the server processing time of the sensed information is 8.1% higher than the existing method and 7.7% lower than the existing method.

• **Key Words** : Color Model; Authentication; Protocol; Convergence; Healthcare

*Corresponding Author : 정윤수(bukmunro@mokwon.ac.kr)
Received January 31, 2017 Revised February 20, 2017
Accepted March 20, 2017 Published March 28, 2017

1. 서론

헬스케어 서비스는 사용자 위치에 상관없이 사용자의 정보를 병원 서버에 전달하여 건강 상태를 관리하는 서비스를 의미한다[1]. 헬스케어 서비스는 기존 의료 서비스를 제공받기 위해서 통신 및 의료 장비를 이용하여 진료 및 예약관리가 가능한 서비스이다. 헬스케어 서비스는 유·무선 통신을 통해 사용자의 건강 상태 정보를 병원에 전달하면 의료진은 사용자의 건강 상태 정보를 분석하여 처방하는 과정을 수행한다[2].

헬스케어 서비스는 기존 의료 서비스에 비해 의료비 절감 및 원격 서비스 기술 활용을 위해서 사물인터넷 서비스를 병원 시스템에 도입하고 있다. 그러나, 유·무선을 통신을 통해 전달되는 사용자의 의료정보가 제3자에게 불법적으로 악용될 수 있는 문제점이 존재한다[3]. 최근 연구에서는 의료진의 접근권한과 관련하여 P-RBAC 모델[4], 조건 및 목적기반 접근제어 모델[5], 의무 모델[6], 작업 상태기반 모델[7], 상황기반 모델[8] 등이 연구되고 있다. 그러나, 헬스케어 서비스는 다른 의료 서비스에 비해 사용자의 의료 정보 및 프라이버시에 많은 취약점이 존재한다.

본 논문에서는 병원 환경에서 의료 서비스를 제공받는 사용자의 초기 인증 과정을 효율적으로 처리하기 위한 칼라 모델 기반의 인증 키 설립 기법을 제안한다. 제안 기법은 인증 키를 생성하기 위해서 칼라 모델에서 사용되는 칼라 정보를 랜덤하게 3개 추출하여 추출된 임의의 칼라 정보를 벡터화하여 인증 키 정보를 직교 벡터의 합으로 구함으로써 효율성을 향상시키는 것을 목적으로 한다. 또한, 제안 기법은 추가적인 암호 알고리즘을 사용하지 않으면서 헬스케어 서비스를 신속하게 처리하기 위해서 병원 의료 서비스 절차를 최소화하였다. 특히, 제안 기법은 의료 서비스 절차를 최소화하여 서버의 업무 부담을 기존 기법보다 낮춤으로써 병원 업무의 효율성을 향상시켰다.

2. 관련연구

2.1 데이터 암호 방식

텍스트 암호 방식은 가장 일반적으로 사용하는 인증 방법 중 하나이다[9]. 텍스트 암호 방식은 간단한 작업을 통해서 데이터를 암호화하거나 압축하지만 텍스트 암호 방식은 피싱, 스파이웨어 공격, 사전 공격, 무차별 공격 등과 같은 다양한 사이버 공격에 매우 취약하다.

2.2 사용자 인증 방식

사용자 인증 방식은 사용자의 이름, ID, 패스워드 등을 서버에 등록하여 사용자 인증과 관련된 정보를 일괄 관리하는 방식이다[10]. 사용자 인증 방식은 데이터 암호 방식의 문제점을 개선하기 위해서 사용자의 생체 인증을 이용하는 방법과 이미지 기반 인증 방법을 이용하는 방법이 사용되고 있다. 사용자의 생체 인증 방법은 다른 인증방법에 비해 안전성은 보장받지만 비용이 많이 소요되는 문제점이 있다. 이미지 기반 인증 방법은 이미지를 클릭하거나 드래그하여 암호화하는 방식으로 일반 텍스트를 사용하지 않는다.

2.3 OTP 인증 방식

OTP 인증 방식은 금융 기관을 중심으로 사용하고 있는 인증 방식이다[11]. OTP 인증 방식은 기존 인증 공격 방법을 통해서 OTP의 정보를 침투하는 것은 불가능하다. 그러나, OTP 인증 방식은 피싱, 스파이웨어 공격, 사전 공격, 무차별 공격과 같은 공격을 예방할 수 있는 장점은 있지만 예방 비용이 많이 들어가는 단점이 있다.

2.4 컬러 코드 행렬 암호 방식

컬러 코드 행렬 암호 방식은 행렬로 표현된 영문자와 숫자로 매트릭스 또는 그리드로 정렬하여 색상 배경을 적용하는 방식이다[12]. 각 행과 열에 표현된 색상 정보는 빨간색, 노란색, 녹색, 파란색, 흰색 및 분홍색 등 7가지 색상이 사용된다. 컬로 코드 행렬 암호 방식을 사용하면 텍스트나 이미지를 사용하는 것보다 암호를 찾아내기 어렵거나 추측할 수 없어 무차별 공격이나 사전 공격을 사전에 예방할 수 있는 장점이 있다. 또한, 컬러 코드 행렬 암호 방식은 인증 방법이 매우 복잡하기 때문에 암호를 찾아내는 시간이 많이 소요되는 문제점이 있다. 또한, 기존 암호 방식에 비해 많은 컴퓨팅 성능이 요구되는 단점이 있다.

2.5 RGB 컬러 코드 암호 방식

RGB 컬러 코드 암호 방식은 RGB의 3가지 색상을 조합하여 암호를 생성하는 방식이다[13]. 이 방식은 다양한 색상 조합 생성이 가능한 특징이 있다. RGB 컬러 코드

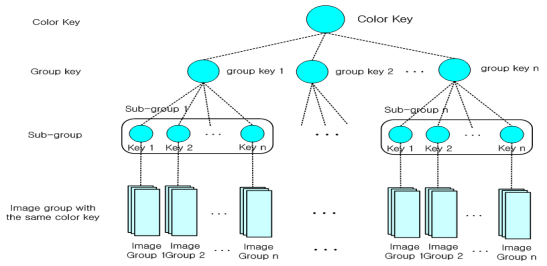
암호 방식은 영화, 전자 시스템, CRT, LCD, 플라즈마, LED TV 및 모니터 등에 사용된다. 또한, RGB 컬러 코드 암호 방식은 8 비트에서 24 비트까지 색상을 조합하여 표현하기 때문에 다른 방식에 비해 안정성이 매우 높은 것이 특징이다.

3. 칼라 모델 기반의 벡터 근사화

이 절에서는 헬스케어 정보를 안전하게 보호하기 위해서 칼라 모델에서 사용되는 칼라 정보를 랜덤하게 3개 추출하여 추출된 임의의 정보를 벡터화하여 사용자 인증에 필요한 키 정보를 직교 벡터의 합으로 구함으로써 효율성을 향상시키는 것을 목적으로 한다.

3.1 벡터 근사화를 이용한 키 생성

[Fig. 1]은 동일 칼라키를 가지는 이미지 그룹을 계층적 그룹 과정을 통해 칼라키를 생성하는 제안기법의 전체 동작 구조를 보여주고 있다.



[Fig. 1] Scalable Color Image Structure of Proposed Scheme

제안 기법은 [Fig. 1]처럼 헬스케어 사용자 인증에 필요한 키 정보를 생성하기 위해서 3 개의 서로 직교하는 칼라 정보 벡터 x_1, x_2, x_3을 이용하여 다차원의 Cartesian 벡터 공간을 생성한다. 칼라 정보 중 랜덤하게 추출된 3개의 임의의 정보를 벡터화하여 사용자 인증에 필요한 키 정보를 직교 벡터의 합으로 구하기 위해서는 우선 3차원 벡터 g를 두 개의 서로 직교하는 벡터 x_1과 x_2를 식 (1)과 같이 직교한다.

$$g \simeq c_1x_1 + c_2x_2 \qquad \text{식 (1)}$$

이때, 벡터 g를 근사화하기 위한 오류는 식 (2)와 같이 구할 수 있다.

$$e = g - (c_1x_1 + c_2x_2) \qquad \text{식 (2)}$$

여기서, e는 x_1-x_2 평면에 수직을 의미하고, c_1x_1과 c_2x_2는 각 x_1과 x_2상에서 g로 산출할 때 e의 길이가최소가 되는 값을 의미한다.

사용자 인증에 필요한 키 정보를 위해 임의로 추출된 3개의 칼라 정보의 벡터가 서로 직교하는 벡터 x_1, x_2, x_3를 사용하여 g에 대한 최적의 근사화를 식 (3)과 같다고 가정할 때, 더 이상 근사화가 아닌 항등식이 되기 위해서는 유일한 c_1, c_2, c_3의 값이 필요하다.

$$g \simeq c_1x_1 + c_2x_2 + c_3x_3 \qquad \text{식 (3)}$$

여기서, 상수 c_i는 식 (4-1)과 식 (4-2)처럼 구할 수 있다.

$$c_i = \frac{< g, x_i >}{< x_i, x_i >} \qquad \text{식 (4-1)}$$

$$= \frac{1}{\|x_i\|^2} < g, x_i > \quad i=1, 2, 3 \qquad \text{식 (4-2)}$$

제안 모델에서는 칼라 정보의 벡터 $\{x_i\}$의 집합이 서로 직교하도록 식 (5)와 같은 조건으로 서록 직교하는 벡터를 구할 수 있다.

$$< x_m, x_n > = \begin{cases} 0 & m \neq n \\ |x_m|^2 & m = n \end{cases} \qquad \text{식 (5)}$$

그리고 식 (5)의 기저 집합이 완전하다면, 이 공간에서 사용자 인증 키 벡터 g는 식 (6)과 같이 나타낸다.

$$g = c_1x_1 + c_2x_2 + c_3x_3 \qquad \text{식 (6)}$$

제안 기법에서는 식 (6)에서 생성된 사용자 인증 키 벡터 g를 유한체 상에 정의된 키로 이용한다.

3.2 초기 인증 프로토콜

제안 기법에서는 사용자의 초기 인증 키를 생성하기

위해서 우선 사용자 인증 키 벡터를 근사화한 후 사용자에게 헬스케어 서비스를 제공하기 위한 인증 프로토콜 과정을 수행한다. 제안기법의 초기 인증 프로토콜에서는 다음과 같이 크게 4단계로 인증 프로토콜 과정을 구성한다.

- 1 단계 : 사용자는 인증을 수행하기 전 식 (7)처럼 [2, n-2] 정수 중에 개인키 d_S 를 임의로 하나 선택한 후 정수 중 가장 큰 솟수와 함께 식 (8)와 같이 비밀키와 공개키 쌍을 생성한다.

$$d_S \in [2,\ n-2] \tag{7}$$

$$Q_S = d_S \times P \tag{8}$$

- 2 단계 : 사용자는 식 (8)에서 생성된 공개키를 인증서버에 전달한다. 서버는 수신된 공개키 Q_S를 이용하여 식 (9)~ 식 (11)의 과정을 통해 칼라 키를 생성한다. 이때, 키 동의에 사용되는 키는 식 (9)처럼 키 벡터 g를 사용하여 서버와 사용자간 사전 동의한 키 R_S를 구한다.

$$Compute\ \ R_S = g \times P \bmod n \tag{9}$$

$$t_S \fallingdotseq R_S \cdot x \tag{10}$$

$$K_S = g^{-1}(H(Q_S \cdot x, I_S,\ t_S)+d_s \cdot R_S) \tag{11}$$

여기서, I_S는 사용자의 원활한 관리를 위해서 사용자의 임시 인식자를 의미하고, t_S는 인증서 만기 시간을 의미한다.

식 (4)에서 $R_S \cdot x$는 사전에 서버와 동의한 R_S로 대치하여 사용한다. 칼라 키 K_S는 사전에 서버와 동의한 키 R_S와 함께 인증서를 (R_S, K_S) 쌍으로 표현하여 사용된다.

- 단계 3 : 식 (12)에서는 사용자는 서버의 공개키 Q_S와 함께 I_S, (R_S, K_S) 그리고 t_S를 서버에게 전달한다.

$$Q_S,\ I_S,\ (R_S,\ K_S),\ t_S \tag{12}$$

- 단계 4 : 서버가 수신한 정보 중 $Q_S \cdot x$, I_S, t_S의 정보를 해쉬한 값에서 추출한 e_S 값을 서버의 데이터베이스에 (14)처럼 저장한다.

$$e_s \in H(Q_S,\ Q_S \cdot x,\ I_S,\ t_S) \tag{13}$$

$$Store\ \ Q_S,\ I_S,\ t_S,\ e_S,\ (R_S,\ K_S) \tag{14}$$

3.3 평가

이 절에서는 사용자와 서버간 헬스케어 정보를 안전하게 전달하기 전에 사용자와 서버간 안전한 통신이 이루어진다고 가정한다. 제안 기법의 성능평가는 처리율과 오버헤드를 평가하며, 보안 평가는 최근 다양화되고 지능화된 보안 공격을 중심으로 기존 기법들과 비교 평가한다.

3.3.1 실험환경

이 절에서는 제안 기법의 실험을 위하여 <Table 1>의 실험 환경을 설정한다. <Table 1>처럼 제안 기법의 성능평가를 위해서 사용자의 헬스케어 정보를 송·수신하는 센서의 수는 s = {1, 2, 5, 10}으로 설정하고 threshold th는 {1, 3, 5}로 설정한다. 센서로부터 생성되는 헬스케어 정보의 생성 간격은 0.01 ms으로 헬스케어 정보를 n= {25, 50, 75, 100, 200}으로 생성되며, 센서로부터 생성된 헬스케어 정보가 서버로 전달할 경우 4 pkts/s의 트래픽이 발생한다고 가정한다.

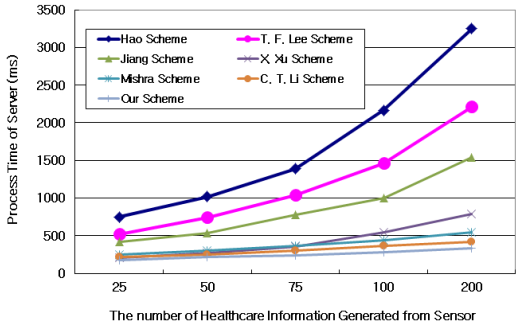
〈Table 1〉 Experiment Setting

Number of Sensor	s = {1, 2, 5, 10}
Buffer	50 packet
Number of Healthcare Information	n= {25, 50, 75, 100, 200}
Information Generation Interval	0.01 ms
Simularity threshold	th = {1, 3, 5}
Traffic	4 pkts/s

3.3.2 성능평가

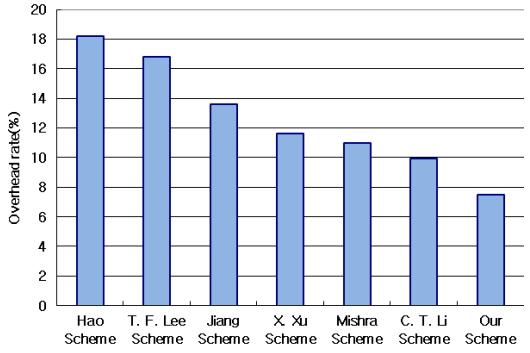
센서로부터 수집된 사용자의 헬스케어 정보를 서버가 처리하는 시간은 수집된 센서 정보의 수에 따라 다르게 나타난다. [Fig. 2]은 사용자의 신체에 부착된 센서로부

터 수집된 헬스케어 정보를 서버가 처리하는데 소요되는 시간을 기존 기법과 비교한 결과를 나타내고 있다.



[Fig. 2] Process Time of Server using Healthcare Inforamtion Generated from Sensor

[Fig. 2]의 실험 결과, 헬스케어 정보 수 증가에 따라 센싱된 정보를 서버가 처리하는 시간이 기존 기법보다 평균 8.1% 낮게 나타났다. 이 같은 실험 결과는 센싱된 정보를 칼라 정보로 추출된 임의의 정보로 벡터화한 키 정보를 통해 직교 벡터의 합으로 구성하여 추가적인 암호 알고리즘을 사용하지 않았기 때문에 서버에서 처리하는 시간을 단축하였다.



[Fig. 3] Overhead rate for bioinformation analysis of implantable device

[Fig. 3]은 헬스케어 정보수에 따른 센서와 서버간 헬스케어 정보를 통해 발생되는 오버헤드를 기존기법과 비교한 결과이다. [Fig. 3]의 실험 결과, 제안 기법은 기존기법보다 오버헤드가 7.7% 낮은 결과를 얻었다. 이 같은 결과는 센서로부터 생성된 헬스케어 정보를 서버로 송・수신할 때, 칼라 모델에서 사용되는 칼라 정보를 랜덤하게 3개 추출하여 추출된 임의의 정보를 벡터화하는 과정만이 사용되었기 때문에 나타난 결과이다.

4. 고찰 및 논의

최근 연구되고 있는 헬스케어 인증 관련 기법은 생체 인증 기반 암호 기법에서 chaotic map을 이용한 암호 기법까지 다양하게 사용되고 있다[12]. chaotic map 기반 기법은 암호 생성에 효율성은 있지만 분실될 스마트 카드의 정보를 취소 시키거나 임시 또는 일시적인 정보 유출 공격을 예방하는 시나리오는 제공하지 않는다[12]. chaotic map 기반 기법의 문제점을 개선하기 위해서 사용자 로그인 과정에서 이미지를 클릭하여 인증을 수행하는 연구가 진행되고 있다[14]. Wiedenbeck, Susan, et. al 방식[15]과 J. Thorpe et. al 방식[16]은 텍스트 기반 암호보다 암호를 매우 효과적으로 암기할 수 있는 특징이 있다. 텍스트 기반 암호와 비교할 때 [17] 기법은 아이콘 세트를 사용하여 볼록 선체를 화면에 생성하기 때문에 안정성이 높다. D. Rachna이 제안한 방식은 챌린지 응답 시스템을 사용하는 방식으로 사용자가 올바른 응답을 할 경우 각 라운드마다 인증이 수행된다[18]. 이 방식은 한 번에 25개의 이미지를 사용하여 비밀번호를 5개를 생성하는 인증 방식을 사용한다. 이때, 비밀번호는 5개의 이미지를 사용하여 비밀번호를 생성한다. Sobrado et. al. 기법은 세 개의 객체를 사용하여 등록 과정에서 사용자를 인증할 수 있도록 식별하는 인증 과정을 사용한다[19]. 이 기법은 세 개의 객체를 이용하여 2 단계 인증을 수행하여 어깨 서핑 공격을 예방한다. S. Balaji et al. 기법은 색상 텍스트 기반의 인증 체계를 제안하였으며 2 레벨을 사용하여 인증을 수행한다[20]. 1 레벨에서는 텍스트를 기반으로 인증하며 2 레벨에서는 그래픽 기법을 사용하여 인증을 수행한다. M. Sreelatha. et. al 기법은 색상과 이미지를 사용하여 인증을 수행한다. 이 기법은 안전성을 높이기 위해서 하이브리드 텍스트 기반의 인증 방식을 제공하는 특징이 있다[21].

제안 기법은 헬스케어 서비스를 사용자에게 제공하기 위한 사용자와 서버간 초기 인증 키를 생성하는데 필요한 정보를 제공한다. 대부분의 기존 기법들은 인증 키 생성보다는 사용자의 헬스케어 정보를 암호화하여 사용자의 프라이버시를 보호하는 연구에 초점이 맞추어지고 있다. 제안 기법에서는 인증 처리 속도를 향상시키기 위해

서 칼라 모델에서 사용되는 칼라 정보를 랜덤하게 3개 추출하여 추출된 임의의 정보를 벡터화하여 사용자 인증에 필요한 키 정보를 직교 벡터의 합으로 구한 후 인증 키를 생성하는 키 정보를 활용한다. 제안 기법은 각 이미지에 대한 칼라키 추출을 계층적으로 그룹화하여 그룹키 영역 1부터 n까지 각 영역의 값을 묶어 비교 분석 후 추출한다. 그룹 키는 동일 칼라키 값을 갖는 이미지 그룹을 서브 그룹화하여 그룹키 영역 1부터 영역 n까지 각 영역의 이미지를 비교 검색하여 칼라키를 구한다.

5. 결론

최근 병원을 중심으로 헬스케어 서비스를 제공받는 사용자의 수가 증가하고 있는 추세이다. 본 논문에서는 칼라 모델에서 사용되는 칼라 정보를 랜덤하게 3개 추출하여 벡터화한 후 사용자 인증에 필요한 키 정보를 직교 벡터의 합으로 구하는 키 설립 기법을 제안하였다. 재안 기법은 추가적인 암호 알고리즘을 사용하지 않고 사용자 정보를 안전하게 전달 할 수 있는 키를 생성하는 것이 특징이다. 성능 평가 결과, 제안 기법은 사용자의 헬스케어 정보의 수가 증가할수록 생성된 정보를 처리하는 서버의 시간이 기존 기법보다 평균 8.1% 낮게 나타났으며, 오버헤드는 기존 기법보다 7.7% 낮은 결과를 얻었다. 향후 연구에서는 본 연구의 결과를 응용하여 사용자 의료 정보를 실제 병원에 적용할 계획이다.

ACKNOWLEDGMENTS

본 연구는 산업통상자원부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음.

REFERENCES

[1] Y. S. Jeong, “Medical Information Management Scheme of Healthcare Service Patient through 2-way Access Control”, Journal of Digital Convergence, Vol. 14, No. 7, pp. 185-191, Jul. 2016.

[2] Y. S. Jeong, “A Study of An Efficient Clustering Processing Scheme of Patient Disease Information for Cloud Computing Environment“, Journal of IT Convergence Society for SMB, Vol. 6, No. 1, pp. 33-38, Mar. 2016.

[3] Y. S. Jeong and S. H. Lee, “A User Privacy Protection Scheme based on Password through User Information Vir tuality in Cloud Computing”, Journal of IT Convergence Society for SMB, Vol. 1, No. 1, pp. 29-37, Nov. 2011.

[4] Y. S. Jeong, “An Efficient m-Healthcare Service Model using RFID Technique”, Journal of Digital Convergence, Vol. 13, No. 11, pp. 149-156, 2015.

[5] J. E. Lee and S. G. NAh, “An Emprircal Study of Usr Perrceptions on EMR Standardization Leading Medical & IT Convergence”, Journal of Digital Convergence, Vol. 13, No. 5, pp. 111-118, 2015.

[6] A. T. Barth, M. a. Hanson, H. C. Powell, and J. Lach, “TEMPO 3.1: A body area sensor network platform for continuous movement assessment”, Proc. - 2009 6th Int. Work. Wearable Implant. Body Sens. Networks, BSN 2009, pp. 71-76, June. 2009.

[7] Y. S. Jeong, “An Efficiency Management Scheme using Big Data of Healthcare Patients using Puzzy AHP”, Journal of Digital Convergence, Vol. 13, No. 4, pp. 227-233, 2015.

[8] Z. Shelby, K. Hartke, C. Bormann, The Constrained Application Protocol (CoAP), IETF RFC 7252, June 2014.

[9] C. Wanpeng, B. Wei, “Adaptive and dynamic mobile phone data encryption method”, Chian Communications, Vol. 11, Issue. 1, pp. 103-109, Jan. 2014..

[10] R. Madhusudhan, M. Hegde, “Cryptanalysis and Improvement of Remote User Authentication Scheme Using Smart Card”, 2016 International conference on Computer and Communication Engineering(ICCCE), pp. 84-89, 2016.

[11] C. Chen, Y. Wang, H. Yu, x. H. Qiang, “The RFID mutual authentication scheme based on ECC and OTP authentication”, 2016 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), pp. 1-4, 2016.

[12] G. Yu, Y. Shen, G. Zhang, Y. Yang, “A

Chaos-based Color Image Encryption Algorithm", 2013 Sixth International Symposium on Computational Intelligence and Design, pp. 92-95, 2013.

[13] S. Som, A. Kotal, A. Chatterjee, S. Dey, S. Palit, "A colour image encryption based on DNA coding and chaotic sequences", 2013 1st International Conference on Emerging Trends and Applications in Computer Science, pp. 108-114, 2013.

[14] Man, Shushuang, D. Hong and M. M. Matthews, "A Shoulder-Surfing Resistant Graphical Password Scheme-WiW", Security and Management, 2003.

[15] Wiedenbeck, Susan, et. al, "PassPoints: Desing and logigudinal evaluation of a graphical password system", International Journal of Human-Computer Studies Vol. 63, No. 1, pp. 102-127, 2005.

[16] J. Thorpe, P. C. van Oorschot, "Grphical Dictionaries and the Memorable Space of Graphical Passwords", USENIX Security Symposium, 2004.

[17] Wiedenbeck, Susan, et al. "Design and evaluation of a shoulder-surfing resistant graphical password scheme", Proceedings of the working conference on Advanced visual interfaces, ACM, 2006.

[18] D. Rachna, "Hash visualization in user authentication", CHI'00 Extended Abstracts on Human Factors in Computing Systems, ACM, 2000.

[19] S. Leonardo and J. C. Birget, "Graphical passwords", The Rutgers Scholar, an electronic Bulletin for undergraduate research 4, 2002.

[20] S. Balaji, "Authentication techniques for engendering session passwords with colors and text", Advances in Computer Science and its Applications 1.3, pp. 189-195, 2012.

[21] M. Sreelatha et. al, "Authentication schemes for session passwords using color and images", International Journal of Netow가 Security & Its Applications 3.3, pp. 111-119, 2011.

저자소개

정 윤 수 (Yoon-Su Jeong) [정회원]

- 2000년 2월 : 충북대학교 전자계산학과 이학석사
- 2008년 2월 : 충북대학교 전자계산학과 이학박사
- 2009년 8월 ~ 2012년 2월 : 한남대학교 산업기술연구소 전임연구원
- 2012년 3월 ~ 현재 : 목원대학교 정보통신융합공학부 조교수

<관심분야> : 유·무선 통신 보안, 정보보호, 빅 데이터, 헬스케어 서비스, IoT