

Vision-based Authentication and Registration of Facial Identity in Hospital Information System

Seok-Chan Bae*, Yon-Sik Lee*, Sun-Woong Choi*

*Professor, School of Computer Info. and Comm. Eng., Kunsan University, Kunsan, Korea

*Professor, School of Computer Info. and Comm. Eng., Kunsan University, Kunsan, Korea

*Student, School of Computer Info. and Comm. Eng., Kunsan University, Kunsan, Korea

[Abstract]

Hospital Information System includes a wide range of information in the medical profession, from the overall administrative work of the hospital to the medical work of doctors. In this paper, we proposed a Vision-based Authentication and Registration of Facial Identity in Hospital Information System using OpenCV. By using the proposed security module program a Vision-based Authentication and Registration of Facial Identity, the hospital information system was designed to enhance the security through registration of the face in the hospital personnel and to process the receipt, treatment, and prescription process without any secondary leakage of personal information. The implemented security module program eliminates the need for printing, exposing and recognizing the existing sticker paper tags and wristband type personal information that can be checked by the nurse in the hospital information system. In contrast to the original, the security module program is inputted with ID and password instead to improve privacy and recognition rate.

▶ **Key words:** Vision, Authentication, Facial Identity, Security, Hospital Information System, Recognition Rate

[요 약]

병원정보시스템은 의료계에서 병원의 전반적인 행정 업무 및 의사들의 의료 업무까지 다양한 정보를 포함하고 있다. 본 연구에서는 OpenCV를 이용해서 비전기반 얼굴인식 인증 및 등록 지원 병원정보시스템을 제안하였다. 구현한 보안 모듈 프로그램을 이용하여 병원정보시스템에서 접수 등록 시 병원관계자의 얼굴촬영을 통한 및 수납, 진료 및 처방 과정까지 보안성을 강화하고 개인 정보의 2차적인 유출 없이 처리하고자 하였다. 구현한 보안 모듈 프로그램을 통하여 병원정보시스템에서 간호사가 확인할 수 있는 기존의 스티커 종이 태그와 손목 밴드 타입의 개인정보의 출력, 노출 및 인식이 필요 없게 하였다. 보안 모듈 프로그램에서 원본과 대조하여 영상을 아이디와 패스워드로 대신 입력되어하여 개인정보보호 및 인식율을 향상시키도록 하였다.

▶ **주제어:** 비전, 인증, 얼굴식별, 보안, 병원정보시스템, 인식율

- First Author: Seok-Chan Bae, Corresponding Author: Yon-Sik Lee, Sun-Woong Choi
- *Seok-Chan Bae (scbae@kunsan.ac.kr), School of Computer Info. and Comm. Eng., Kunsan National University
- *Yon-Sik Lee (yslee@kunsan.ac.kr), School of Computer Info. and Comm. Eng., Kunsan National University
- *Sun-Woong Choi (escaco95@naver.com), School of Computer Info. and Comm. Eng., Kunsan National University
- Received: 2019. 11. 28, Revised: 2019. 12. 24, Accepted: 2019. 12. 26.

I. Introduction

병원정보시스템(HIS)은 의료기관(병원)의 진료, 진료지원, 영상정보, 접수·수납에 이르는 관리업무를 전산화한 시스템을 통틀어서 말하고 있다.

최근 병원정보시스템에서 환자와 가족에게 여러 가지 서비스, 진료 활성화 및 진료의 질 향상을 위한 노력을 많이 하고 있다. 행정기관 및 병원과 같이 사람들이 많이 모이는 환경에서 민감하고 중요한 데이터 보호를 위하여 조직체 내에서 관리되어야 한다. 또한 개인 정보도 보호되어야 한다. 그러나 병원정보시스템에 대한 정보보호 대책이 미흡한 것이 현실이다.

병원 정보시스템은 영상 데이터를 전송, 저장, 관리하는 의료영상저장 전송 시스템인 PACS(Picture Archiving and Communications System), 환자의 처방 전달 및 진료 내역을 관리하는 처방 전달 시스템인 OCS(Order Communication System), 환자의 전자업무 기록시스템인 EMR(Electronic Medical Record)로 구성되어 있다. 위의 세 가지 시스템이 병원정보 시스템으로 연동되어 있으나 병원 내에서 시스템 연계 및 연동 시 필요한 개인정보 보호를 위한 보안 모듈에 대한 연구가 필요하다.

본 연구에서는 OpenCV를 이용해서 보안 모듈 프로그램을 구현하였다. 구현한 보안 모듈 프로그램을 이용하여 병원정보시스템에서 접수 시 얼굴촬영을 통한 및 수납, 진료 및 처방 과정까지 보안성을 강화하고 개인정보의 2차적인 누출 없이 처리하고자 하였다. 구현한 보안 모듈 프로그램을 통하여 병원정보시스템에서 간호사가 확인할 수 있는 기존의 스티커 종이 태그와 손목 밴드 타입의 개인정보의 출력, 노출 및 인식이 필요 없게 모듈 프로그램에서 원본과 대조하여 인식율을 향상시키도록 하였다.

2장에서는 관련연구로 병원정보시스템과 개인정보 보호의 필요성에 대해 언급하였고, 3장에서는 병원정보시스템에서 개인정보 보호를 위한 보안 프로그램 구현에 대해 설명하였다. 4장에서는 결론 및 향후 연구방향을 기술하였다.

II. Classification of Hospital Information System

2.1 Classification

병원정보시스템에서 만들어지는 정보는 의료기관 내 환자를 관리하는 의료과정과 병원의 경영 관리 활동을 중심으로 발생하고 있다. 이는 다른 조직체나 기관과는 다르게

전문 직종 간에 생성 및 교환되는 정보의 양이 방대하고 정보의 신속, 정확성, 보관 등이 필요한 점이 다른 시스템의 정보와의 차이점이다[1].

병원정보시스템은 병원의 여러 가지 업무를 수행하는데 필요한 정보를 적절히 제공하는 시스템으로 여러 형태의 기능을 수행하는 단위 시스템의 복합구성이다[2].

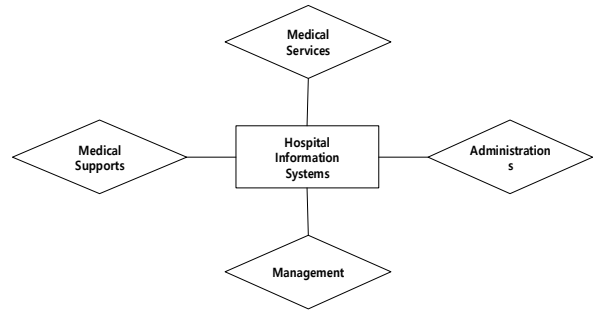


Fig. 1. Structure of Hospital Information System

Fig. 1의 병원정보시스템은 업무 성격에 따라 Table 1과 같이 분류할 수 있다[3]. Fig. 1은 병원정보시스템의 일반적 구조를 나타내었다. 병원정보시스템은 의사가 행하는 진찰 및 치료를 지원하는 진료업무, 진료를 지원하는 진료지원, 환자예약, 접수, 수납 등을 지원하는 원무 행정과 인사, 급여, 회계, 자산, 원가 등을 관리하는 의료경영관리 업무로 나눌 수 있다.

Table 1. Classification of Hospital Information System

Division	Target Tasks
Medical Services	- Diagnosis and treatment - Disease history management, education, examination, treatment management, literature search and research management
Medical Supports	- Aid Assistance Service - Inspection services, dispensing services, nursing services, central supply, food services - Patient Support Services
Administrations	- Medical service complaints - Patient schedule, medical service, storage service, medical record work
Managements	- Human resources, payment services, accounting services, hospital services, inventory management, cost management

2.2 Needs of Personal Information Security

의료인 또는 의료기관의 개설자는 진료기록부 등을 전자서명법에 의한 전자서명이 기재된 전자문서로 작성, 보관할 수 있다[4].

현재 우리가 살고 있는 실생활 내에서 개인정보 침해 유형을 살펴보면 여러 가지 유형의 개인정보 침해 가능성이 존재하기 때문에 이에 대비한 개인정보 보호가 필요하다.

개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다[8]

의료기관의 개인정보 유출에 대한 대책 마련도 미흡하지만 외부의 해킹에 의한 개인 정보 유출보다 병원 내부 근무자나 의료 정보 업체 직원들에 의한 정보 유출이 더 심각하다. 사례에 따르면 병원사무장이 전자처방전을 통해 환자 수 천 명의 개인정보를 누출하여 다른 사이트를 개설 및 운영하다 적발한 경우뿐만 아니라 의료 정보 업체 직원들에 의한 정보 유출도 심각하다. 병의원 진료차트 관리 프로그램을 제작 및 공급하는 업체 대표 등 직원이 국내 수 십 개 병의원으로부터 수백만 건에 해당하는 환자 진료 정보를 외부로 유출한 사례도 있다. 또한 의료정보 시스템 개발업체에서는 7억2000만 건의 환자 진료 정보를 동의 없이 저장하여 다국적 의료통계회사에 제공한 사실도 있다. 그리고 프로그램 업데이트 및 유지보수가 필요하다는 이유로 병원에서 환자의 진료정보가 포함된 수십만 건의 차트를 넘겨받은 사실도 있다[9][10].

병원정보시스템의 PACS, OCS, EMR 프로세스 과정중의 관리자의 관리소홀 및 해킹에 의한 정보 보호에 대한 연구가 필요하다.

의사가 직접 컴퓨터에 환자의 임상진료에 대한 모든 정보를 조회 및 입력하면 환자의 자료를 모두 데이터베이스를 통하여 검색, 새로운 정보의 생성도 가능한 의료정보시스템으로 HIS(Hospital Information System, 병원정보시스템)의 일부분이다. 이 시스템은 소프트웨어와 접속센터, 진료실, 검사실, 서버 등 하드웨어로 구성되어 있으며 이를 통해 일일이 수작업으로 종이에 환자기록을 정리 하는 방식보다 온라인 서버를 통하여 의료기관의 업무를 대폭 줄일 수 있다. 특히 환자의 진료기록을 찾아서 진료실에 전달하고 다시 처방전을 받아 조제하는 일련의 과정이 네트워크를 통하여 처리함으로써 환자 대기시간이 줄었다.

전자기록시스템을 구현함으로써 원격지 환자 또는 협력 병원 간에 원격진료 서비스의 기본 토대를 갖추 수 있다. 그러나 개인의의료정보들이 디지털화와 더불어 중앙관리 체계로 진화하고 원활한 진료, 교육, 연구 등의 목적으로 다른 시스템 또는 다른 기관들과의 시스템 간 연동체제로 확장 및 확대됨에 따라, 외부에서의 해킹 및 바이러스의 위협뿐만 아니라 무단 유출, 유출된 정보의 오용 및

남용 등의 내부 위협 등으로 개인 의료 정보보호에 대한 우려가 제기되고 있다[11].

병원정보시스템에서 생산되는 의료정보는 신체와 관련된 전문적이고 공익 정보이므로 개인 정보 중에서도 특별한 보호가 필요하며, 이러한 개인정보는 복제가 쉬워 의료 정보가 유출되거나 부정확한 정보가 생산될 경우 개인의 사생활이 침해될 가능성이 있다.

2.3 Expansion of Existing Research

병원에서 환자 진료 접수 시 저장된 데이터베이스 사용자 그룹에 접근하고자 하는 서버의 환자의무기록 사항에 대해 보안정책의 인증체계를 비교 검토하여 접근 가능한 범위 내에서만 접근하도록 한다. 사용자 그룹의 접근 정도를 고려하여 등급을 생성 및 접근 가능하게 한다. 사용자가 서버에 있는 데이터베이스에 접근을 요청하면 보안정책의 인증체계를 비교 검토하여 질의문에 따라, 추출하여 처리한다. 접근 요청 시 병원 데이터베이스 서버에 있는 환자의무기록 사항과 접근하고자 하는 사용자 그룹의 등급을 비교하여 보다 높은 등급을 소유하고 있는 그룹이면 열람이나 기타 연산이 가능하도록 한다. 더 높은 등급이더라고 환자의 개인정보 유출에 대비하여 가능한 한 최소의 자료만 공개되도록 한다[6].

위의 연구에서는 접근 제어 정책에 따라 사용자의 등급을 비교하여 데이터베이스의 자료에 등급 분류에 맞는 뷰만을 접근하도록 하여 개인정보에 대한 보안을 유지하였다. 병원정보시스템을 사용하는 사용자의 권한, 의료정보의 보안 요구사항, 의료정보를 취급자의 권한에 맞는 보안 요구사항을 분석한 법적인 요구사항을 만족하도록 제시한 요구사항이다[4]. 의료정보시스템에 위협이 되는 요소 및 보안대책을 제시하여 의료정보화에 따른 보안 기술 및 보안 연구가 진행되고 있다[5].

사용자의 인증에서부터, 의료정보를 관리하고 안전한 전송을 보장하도록 하는 개인정보보호와 더불어 보안을 강화하는 시스템이 필요하다. 이에 본 연구에서는 병원 시스템에 저장할 수 있도록 환자의 접수 시 동의 후 얼굴을 촬영, 데이터베이스에 등록하여 환자의 진료 및 처방, 검사 등에서 필요한 제반 인식 절차가 생략되게 하여 개인정보 노출을 방지하였다. 위에서 제시한 절차상 편의성과 개인정보 노출이 필요 없도록 하는 보안성을 제공하게 된 점이 본 연구의 차별성과 독창성이라고 할 수 있겠다.

III. Design of The Proposed System

3.1 Customer Authentication

먼저 외부자의 접속 현황이다. Fig 2는 병원에 진료받기 위해 처음 오는 환자 및 재진환자의 접수 현황 구조를 보여주고 있다. 병원의 재진환자 중에 성형으로 원래의 이미지와 차이가 나는 부분이 있으면 재등록을 하도록 한다.

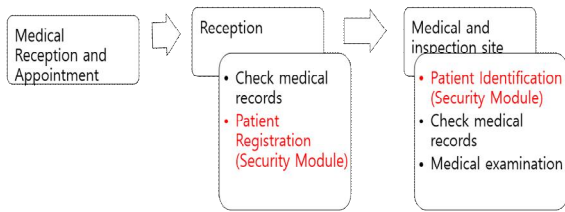


Fig. 2. Outsider Receipt

다음으로 병원 관계자의 접속이다. Fig. 3은 병원관계자로서 접수직원, 간호사, 의사, 등 병원에서 실제로 시스템을 접속하여 데이터를 입력하는 관계자를 모두 총칭한다.

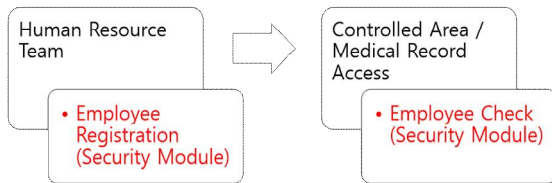


Fig. 3. Connection of Hospital Staff

Open cv 그래픽 라이브러리를 활용, 사람의 얼굴의 특징점을 이용하여 환자의 이름과 환자번호 등의 정보를 아이디와 패스워드로 대신하는 프로그램을 설계 및 구현하였다.

Fig. 4.는 환자 초진 및 재진과 병원관계자의 신원을 확인할 수 있는 데이터베이스 등록 전부터 등록 후 인증절차에 대한 과정을 보여주고 있다.

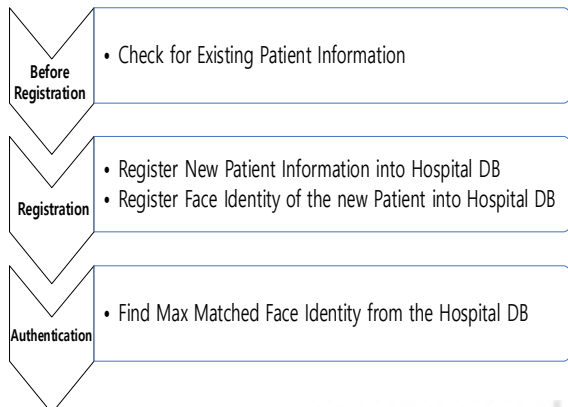


Fig. 4. Process of Face Identity Registration and Authentication

3.2 Algorithm of Facial Identity Authentication

환자 진료 접수 시 접수창구에서 얼굴을 인식하고, 등록 및 얼굴의 특징점을 찾아서 스크린 샷을 하여 특징점으로 이루어진 부분의 해당하는 이미지를 추출 후 그 이미지를 데이터베이스에 저장한다.

Fig. 5는 병원에서 환자 및 관계자 등록 및 인증 과정의 보안 모듈 프로그램의 입출력 흐름이다.

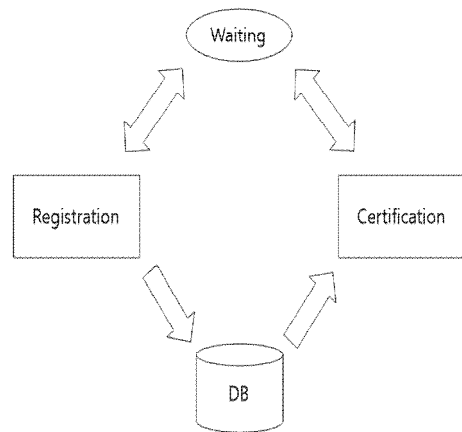


Fig. 5. Input/Output flow

Fig. 6은 사용자가 Textbox에 불러올 이미지를 경로를 입력하여 영상장치로부터 이미지를 취득하고 이를 제한한 보안 모듈 프로그램(FaceVault) 탐색기를 통하여 특징점을 패스워드로 정하여서 사용자가 인증 버튼을 누름으로써 탐색된 영역을 절삭하여 데이터베이스에 저장한다.

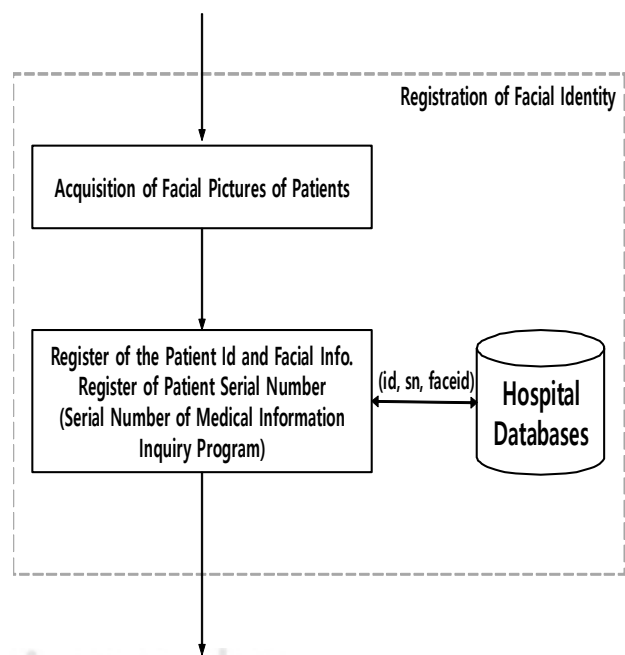


Fig. 6. Registration of Facial Identity

Fig. 7은 Threshold값에 대한 내용으로 FVFaceMatcher Module을 나타내고, 본 논문에서는 Threshold 0.80은 인식 폭이 넓으나, 안경을 써도 동일인물로 인식하고 있어 얼굴이 조금 다르거나, 위장을 해도 인식할 가능성이 있다는 것을 나타내고 Threshold 0.90는 액세서리를 착용할 경우 인식하지 않는다는 보안상의 장점이 존재하나 인식 폭이 너무 좁고 배경의 변화에 민감함을 알 수 있다는 것을 나타낸다.

환자 진료 시 데이터베이스에 있는 원본과 환자의 얼굴을 대조 후 template matching 작업 및 coeff 방식을 이용하여 0과 1로 사이의 값으로 정규화하나 유사도 Threshold 값 0.85로 정하였다.

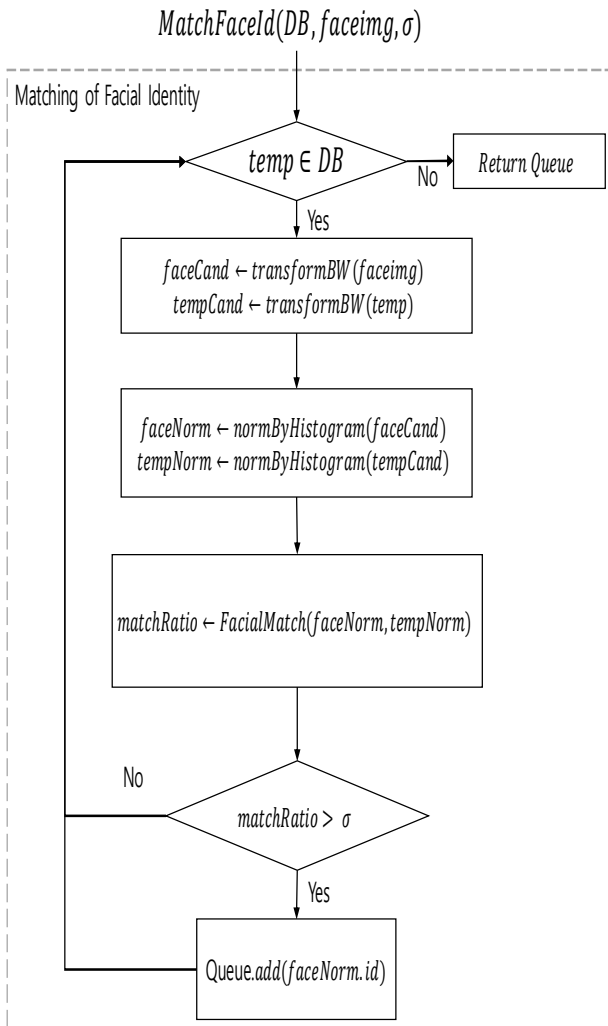


Fig. 7. Matching of Facial Identity

논문의 흑백이미지를 히스토그램 평활화를 통하여 다단계 스케일하는 모듈은 FVFaceDetector 모듈이다[12,13].

Fig. 8은 그림 6의 데이터베이스에 등록된 정보와 영상 장치로부터 인식된 식별정보가 일치하는지 인증하는 과정이다.

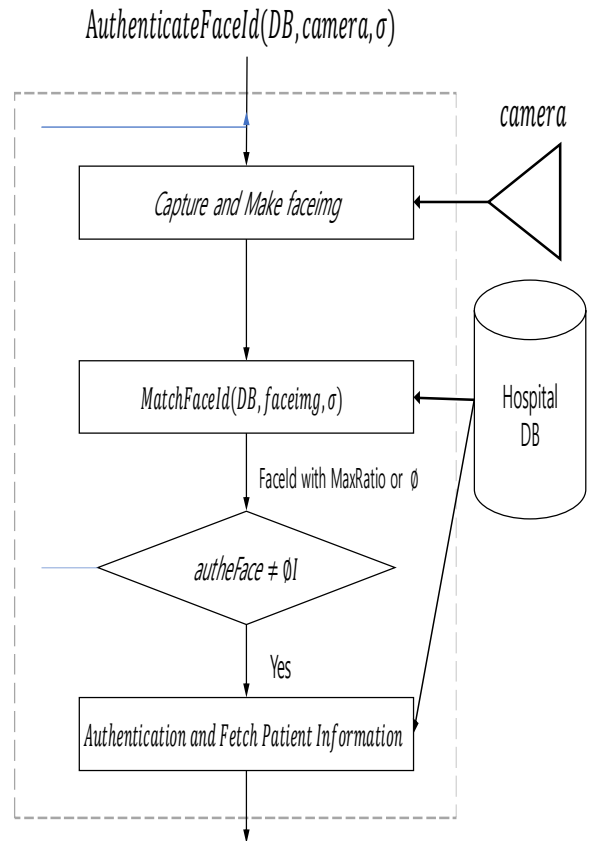


Fig. 8. Authentication of Facial Identity

본 논문에서 실험 부분은 제시하지 않았으나 Fig. 7의 얼굴식별 매칭 알고리즘 제시와 Fig. 8의 얼굴식별을 위한 인증 알고리즘 내용을 본 논문의 연구 방법으로 제시한다. 본 연구에서는 병원관계자 및 접수창구에서 수납 담당자가 FV '인증' 모드 진입하도록 설정하여 환자가 자기 식별 정보(생년월일 또는 이름)를 입력하고, FaceVault가 식별 정보에 저장된 '촬영된 얼굴' 이미지와 현재 카메라에 비친 환자의 얼굴을 비교한다.

본 논문에서는 의료정보 접근하는 확인으로서 얼굴이 85% 이상 일치하면 병원관계자 및 접수창구의 PC에 의료 정보 접근 ID/PW를 입력하고, 접수창구 및 진료과에서는 시스템에 인증 결과로 시스템에 보인 의료정보를 확인할 수 있다. 또한 피사체와 카메라의 거리를 고려하여 얼굴이 원본과 유사함을 점검하는 기준 값 내에 들면 원본임을 증명할 수 있게 되어 보안 및 편의적이어서 지금 시스템보다는 차별적인 요소라고 할 수 있다.

그리고 특징점을 패스워드로 처리하여 본인인지 확인하는 것으로 대체하여 창구에서 굳이 말하지 않아도 되고, 창구에서 개인정보가 출력된 스티커나 밴드를 환자가 부착하거나 착용하지 않아도 되어 개인정보 보호를 위한 기반이 될 것으로 판단이 된다.

IV. Conclusions

병원정보시스템을 이용하는 환자와 간호사, 의사 및 병원관계자의 개인정보 보호를 위하여, 시스템 접근 시 인증 절차에 대한 확인을 통하여 보안성을 강화할 수 있었다.

프로그램에서는 환자 진료 시 데이터베이스에 있는 원본과 환자의 얼굴을 대조 후 template matching 작업 및 coeff 방식을 이용하여 0과 1로 사이의 값으로 정규화를 하여 유사도 threshold 값 0.85로 정하였다. 본 연구에서는 병원관계자 및 접수창구에서 수납 담당자가 FV '인증' 모드 진입하도록 설정한다. 환자의 식별 정보(생년월일 또는 이름)을 입력하고, FaceVault가 식별 정보에 저장된 '촬영된 얼굴' 이미지와 현재 카메라에 비친 환자의 얼굴을 비교한다. 85% 이상 일치하면 병원관계자 및 접수창구의 PC에 의료정보 접근 ID/PW를 입력하고, 접수창구 및 진료과에서 시스템에 인증 결과로 본인 여부가 확인되어 시스템에 의료정보가 보인다.

피사체와 카메라의 거리를 고려하여 얼굴이 원본과 유사함을 점검하는 기준 값 0.85 내에 들면 원본임을 증명하여 촬영된 얼굴 이미지와 현재 카메라로 촬영된 얼굴을 본인임을 확인하는 것으로 본인 이외에 다른 사람이 개인정보를 유용한다든지, 병원정보시스템 서버에 접근할 수 없게 하였다. 이처럼 시스템에서 본인임을 확인할 수 있도록 하는 검증 시스템을 이용함으로써 개인정보보호를 위한 기반을 마련할 수 있었다.

개인 정보 보호를 위한 보안 모듈 프로그램을 통하여 보안성을 강화하고 더불어 개인정보를 보호할 수 있도록 연구하였다. 병원정보시스템에서 진료 시 보안 프로그램을 통하여 신원확인이 된다면 본인 확인이 2차적으로 불필요하게 되어 보안이 강화되고, 부차적인 개인정보를 출력물의 손실 및 유실에 대한 문제점을 해결할 수 있을 수 있어 개인정보 보호를 높일 수 있었다.

그리고 앞으로의 연구방향으로는 병원시스템을 실무환경에 적용하여 시스템에서 발생하는 문제점을 검토하고 개선점을 도출한 내용을 연구하도록 하고, 병원 관계자, 간호사, 의사 및 병원관계자들도 시스템에 개인정보 보호 및 서버에 있는 모든 병원 데이터 보호를 위한 보안 요구 사항 정책을 수시로 적용할 수 있는 교육 및 연구가 필요하다.

REFERENCES

- [1] B. C. Mun, D. S. Kim, H. W. Kim, "The Audit Model for efficient Hospital Information System Construction," Korea Society of IT Services, Vol.11, No. 2, pp.197-211, Jun. 2012. Doi: <https://doi.org/10.9716/KITS.2012.11.2.197>
- [2] Sung-Hyun Park, "The Suggestion of the Medical ISMS for the Small and Medium Hosiptals and the Study on the Consulting Method Regarding to the Technical Protection," Master of Engineering dissertation, Graduate School of International Information of Dongguk University, 2013.
- [3] Hye-Jung Kim, "A Study on Indicator Development to Evaluate Hospital Information System : based on Balanced Scorecard Method, Master of Public Health dissertation, Graduate School of Public Health of Yonsei University, 2006.
- [4] J. M. Hong W. Shin, "Security Requirements of Order Communication System in Hospitals for Compliance with Personal Information Protection Act" J. of Security Eng. Vol. 10, No. 5, pp. 513-526, Oct. 2013.
- [5] K. H. Han, "Smart Medical Security Forum", TTA-18100-SA, Dec. 2018.
- [6] Scbae, "Personal Information Security in Hospital Information System Using Degree of Key." Proceedings of Information Processing Society 2005, pp.587-590, Nov. 2005
- [7] Ministry of Science and ICT(Information Security Industry Division), Digital Signature Laws, <http://www.law.go.kr/lsInfoP.do?lsiSeq=195204&efYd=20170726#0000>
- [8] Ministry of the Interior and Safety(Privacy Policy Division), Personal Information Protection Act, <http://www.law.go.kr/lsInfoP.do?lsiSeq=195062&efYd=20171019#0000>
- [9] Korean National Police Agency Cyber Bureau, Hospital Patient Care Information Unprotected, https://cyberbureau.police.go.kr/board/boardView.do?board_id=all&id=3825
- [10] JTBC, 44 million patient information...9 out of 10 records leaked, http://news.jtbc.joins.com/article/article.aspx?news_id=NB10975204
- [11] Electronic Medical Record, encyclopedia of knowledge, Korean Economics Dictionary, <https://terms.naver.com/entry.nhn?docId=2075181&cid=42107&categoryId=42107>
- [12] OpenCV, Image Register Process, https://docs.opencv.org/4.1.0/d7/d8b/tutorial_py_faFig.6.ImageRegisterProcessce_detection.html
- [13] OpenCV, Template Matching, https://docs.opencv.org/2.4/doc/tutorials/imgproc/histograms/template_matching/template_matching.html

Authors



Seok-Chan Bae received the B.S. M.S, and PhD. degrees in Computer Science from Chonnam National University, Korea, in 1983, 1988 and 1995, respectively. Dr. Bae joined the faculty of the School of Computer

Information and Communication Engineering, Kunsan National University, Kunsan, Korea, in 1995. He is interested in database systems security, Hospital Information Systems, Big Data Analytics, Digital forensic.



Yon-Sik Lee received the B.S. and M.S. degrees in Computer Science from Chonnam National University, Korea, in 1982 and 1984, respectively. And, his Ph.D. degree in Computer Application Engineering from

Chonbuk National University, Korea, in 1994. Dr. Lee joined the faculty of the School of Computer Information and Communication Engineering, Kunsan National University, Kunsan, Korea, in 1986. He is interested in sensor network middleware, active rule system, agent system and cloud computing.



Sun-Woong Choi studying in School of Computer Information and Communication Engineering, Kunsan National University, Kunsan, Korea. He joined the student of the School of Computer Information and

Communication Engineering, Kunsan National University, Kunsan, Korea, in 1995. He is interested in Tensonflow, PyTorch, Keras, Machine learning, Interactive Program Design.