Journal of the Korea Convergence Society
Vol. 10. No. 3, pp. 7-14, 2019

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2019.10.3.007

광학문자인식 기반 보안문서 이미지 파일 관리 시스템

정필성[1], 조양현[2*]
[1]명지전문대학 정보통신공학과 조교수, [2]삼육대학교 컴퓨터·메카트로닉스공학부 교수

Optical Character Recognition based Security Document Image File Management System

Pil-Seong Jeong[1], Yang-Hyun Cho[2*]
[1]Assistant processor, Dept. of Information Technology Communication, Myongji College
[2]Processor, Division of Computer & Mechatronics Engineering, Sahmyook University

요 약 정보통신 기술의 발전으로 우리는 사무실에서 개인용 컴퓨터를 이용한 방식의 회사업무처리에서 벗어나 스마트 기기를 이용하여 언제 어디서나 편리하게 업무를 처리하는 스마트워크 환경을 경험하고 있다. 오피스 프로그램을 이용하여 작성한 문서를 이메일 서비스를 이용하여 주고받던 것을 스마트 기기를 이용하여 사진을 찍고 모바일 메신저로 전송하는 것으로 대신할 수 있다. 제조현장에서는 보안문서인 작업지시서를 스마트 기기를 이용하여 사진을 찍고 공유하는 것을 쉽게 볼 수 있다. 본 논문에서는 제조현장에서 근로자의 스마트 기기에 남겨지는 보안문서 이미지 파일을 찾아내고 삭제 처리하는 시스템을 제안한다. 제안한 시스템은 광학문자인식 기술을 이용하여 이미지의 글씨를 인식한 후 키워드화 시켜 일치하는 비율을 통해 보안문서 이미지 파일을 검색해내고 삭제 처리한다. 본 논문에서 제안한 시스템을 이용할 경우 중소기업에서도 효율성 높은 시스템을 구축하여 보안인식이 낮은 제조현장의 작업자들도 편리하게 보안문서 파일을 관리할 수 있다.

주제어 : 광학문자인식, 문서 보안, 보안 기술, 스마트 기기, 스마트워크

Abstract With the development of information and communication technology, we have been able to access and manage documents containing corporate information anytime and anywhere using smart devices. As the work environment changes to smart work, the scope of information distribution is expanded, and more efforts are needed to manage security. This paper proposes a file sharing system that enables users who have smart devices to manage and share files through mutual cooperation. Proposed file sharing system, the user can add a partner to share files with each other when uploading files kept by spliting the part of the file and the other uses an algorithm to store on the server. After converting the file to be uploaded to base64, it splits it into encrypted files among users, and then transmits it to the server when it wants to share. It is easy to manage and control files using dedicated application to view files and has high security. Using the system developed with proposed algorithm, it is possible to build a system with high efficiency even for SMEs(small and medium-sized enterprises) that can not pay much money for security.

Key Words : File Sharing System, Document Security, Information Security, Security technology, Smart Device

*This study is supported by Basic Science Research Program through the Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2017R1D1A1B03030759)
*Corresponding Author : Yang-Hyun Cho (yhcho@syu.ac.kr)
Received December 28, 2018 Revised February 18, 2019
Accepted March 20, 2019 Published March 28, 2019

1. 서론

정보화 사회로 돌입하면서 언제 어디서나 다양한 스마트 기기를 활용하여 업무를 수행하는 이른바 모바일 워크 사회가 가능하게 되었다. 평소 자주 사용하는 스마트 기기를 이용하여 클라우드 서비스를 이용하여 사내 문서에 접근할 수 있으며, 모바일 메신저를 이용하여 업무 문서를 쉽게 주고받을 수 있다[1-3]. 또한 스마트 기기의 카메라를 이용하여 문서를 쉽게 스캔하고 저장하거나 협력업체에 넘겨줄 수 있다. 이렇듯 정보기술의 발전과 클라우드 서비스의 보급화로 우리는 평소에 사용하던 스마트 기기를 이용하여 편리하게 스마트워크 환경을 누리게 되었지만 정보화 사회의 역기능 또한 존재하고 있으며 그 대표적인 사례가 바로 스마트 기기 사용으로 인한 보안사고 이다[4,5].

모바일 보안 사고는 계속적으로 증가하고 있으며 개인정보를 포함하는 중요정보 뿐만 아니라 회사의 중요한 문서가 유출되어 영업 기밀을 노출하는 문제가 발생하고 있다. 이로 인하여 개인의 정신적, 물질적 피해뿐만 아니라 회사의 존폐위기를 초례할 수도 있다. 정부는 개인정보 보호법을 개정하고 스마트폰 백신 이용 안내서를 배포하는 등의 홍보를 하고 있으며 스마트폰 제조업체는 스마트폰 판매 초기부터 백신을 탑재하여 판매하는 등의 개인정보 보호를 위한 조치를 취하고 있지만 회사에서 공용으로 사용되는 스마트 기기의 경우 많은 경우가 취약한 상황에 놓여 있다[6-8].

중소기업의 경우 비용의 문제로 별도의 보안관리 인력을 배치하기 어려우며 전문적인 보안 교육을 받기가 어려운 것이 현실이다. 특히 제조업의 경우 작업자의 보안 교육 수준이 낮고 외국인 작업자가 근무하는 경우도 있기 때문에 보안인식이 낮은 경우가 많다. 제조업체의 경우 발주업체로부터 작업지시서 및 작업발주서를 정식으로 발급받기 이전에 스마트 기기나 이메일을 통해 작업지시서를 미리 공유하는 형태가 이루어질 수 있으며 이로 인하여 제조상의 중요한 기밀문서가 외부로 쉽게 노출 될 수 있으며, 작업 공정에서 공정 전산화를 위해 공정 기록을 남기는 경우에 사용하는 공용 스마트 기기에 작업지시서의 일부분 또는 전체를 찍은 사진이 고스란히 남아있고 OTG(On-The-Go) 메모리를 이용하면 외부로 쉽게 유출이 가능하다[9-11].

업무상의 보안 사고를 막기 위한 제일 좋은 방법은 업자가 교육을 통해 보안 안전을 숙지하고 업무를 진행하고 보안관리 인력을 배치하여 상시적, 주기적으로 공용 스마트 기기 및 개인 스마트 기기를 점검하고 관리하는 일이다. 하지만 앞서 논의하였듯이 중소기업에서는 보안관리를 위한 전문요원을 배치하기 어려우며, 전문적으로 주기적인 교육을 진행하기가 어렵다[12,13].

본 논문에서는 스마트 기기에 설치하여 몇 번의 클릭만으로 스마트 기기에 저장된 쉽게 회사 문서를 찾아내어 외부로 유출되기 전 미리 관리 및 삭제할 수 있는 시스템을 제안한다. 제안하는 시스템은 광학문자인식 기술을 이용해 보안문서 이미지 파일을 추적하고 삭제 및 암호화를 진행하여 외부에서 이용하지 못하도록 하는 기능을 가진다. 제조업에서는 성능이 제한적인 스마트 기기를 사용하는 경우가 많으며 이미지로 문서를 관리하는 업무가 많다. 따라서 본 논문에서는 스마트 기기의 이미지 파일을 서버로 전송하여 고성능의 서버에서 이미지 파일을 분석하고 관리하도록 처리하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로서 구글 클라우드 비전 서비스와 아파치 코도바에 관하여 알아본다. 3장에서는 광학문자인식 기술을 이용한 보안문서 이미지 관리 알고리즘을 알아보며 4장에서는 광학문자인식 기술을 이용한 보안문서 이미지 관리 시스템 구현에 대해서 알아본다. 5장에서는 효용성에 대해서 평가를 진행하며 마지막으로 6장에서는 결론을 맺는다.

2. 관련 연구

2.1 구글 클라우드 비전

구글 클라우드 비전 서비스는 구글에서 제공하는 머신러닝 기반 이미지 분석 서비스로서 구글에서 제공하는 기본 모델을 이용한 이미지 인식과 사용자가 직접 업로드한 이미지를 이용하여 생성한 모델을 이용한 이미지 인식 서비스를 제공한다. 기본적으로 제공하는 구글 모델을 사용할 경우 이미지를 수천 가지의 카테고리로 분류할 수 있으며, 성인 콘텐츠에서부터 폭력적인 콘텐츠에 이르기까지 다양한 유형의 부적절한 콘텐츠를 감시하는 기능까지 사용 가능하다. 사용자가 로컬 또는 원격으로 이미지 분석 기능을 손쉽게 사용할 수 있도록 REST API를 제공하며 분석된 결과를 JSON 정보로 받을 수 있기 때문에 파싱과 분석이 쉽다는 장점을 가진다. 또한 이

미지에 포함된 한글을 처리할 수 있도록 한글 OCR 기능을 제공하고 있기 때문에 딥러닝이나 OCR 기술에 대한 전문가가 아니더라도 손쉽게 기능을 이용할 수 있다. 본 논문에서는 구글 비전 서비스의 OCR 기능을 이용하여 사용자의 스마트폰에 불필요하게 보관하는 보안문서를 찾아낸다. Table 1은 구글 클라우드 비전에서 제공하는 서비스를 나타낸다[14].

Table 1. Google Cloud Vision API Feature

Feature	Description
Label Detection	Detect broad sets of categories within an image, ranging from modes of transportation to animals
Explicit Content Detection	Detect explicit content like adult content or violent content within an image
Logo Detection	Detect popular product logos within an image
Landmark Detection	Detect popular natural and man-made structures within an image
Optical Character Recognition	Detect and extract text within an image, with support for a broad range of languages, along with support for automatic language identification
Face Detection	Detect multiple faces within an image, along with the associated key facial attributes like emotional state or wearing headwear
Image Attributes	Detect general attributes of the image, such as dominant colors and appropriate crop hints
Web Detection	Search the Internet for similar images

2.2 아파치 코도바

아파치 코도바는 어도비에서 서비스하는 스마트 기기에 적합한 개발 프레임워크이다. 안드로이드용 애플리케이션 개발을 위해서 자바, 코틀린을 이용하고 iOS용 애플리케이션 개발을 위해서 스위프트, 오브젝티브-C를 이용하는 것을 네이티브 개발 방식이라고 한다. 아파치 코도바는 HTML5, CSS3, Javascript를 이용하여 표준 웹 개발 방식과 플러그인을 이용하여 애플리케이션을 개발하는 방식을 말한다. HTML5, CSS3, Javascript로 개발되는 웹 프로그램을 안드로이드, iOS에서 동작하는 웹 뷰를 이용하여 화면에 표현하며, 내부적인 기기 제어는 네이티브 개발 방식으로 개발한 API 플러그인을 이용하여 제어한다. 아파치 코도바에서 제공하는 API 플러그인 서비스는 Table 2와 같다[15].

Table 2. Apache Cordova Plugin API Services

API	Description
Accelerometer	Read measurement value of 3-axis acceleration sensor (motion sensor) of device
Camera	Capture photos using device camera
Capture	Capture media files using the device's media capture function
Cmpass	Read direction information of device
Connection	Check device network status and read network information
Contact	Can work with device's contact list database
Device	Device-specific information such as device name, platform, version, etc
Events	JavaScript can detect events that occur on the device
File	Javascript can use the device's file system
Geolocation	Read device's current location information
Media	Ability to play and record audio files on the device
Notification	Device notification function is available
Storage	The device's database is available

3. 제안 시스템 알고리즘

3.1 제안 서비스 모델

제안 시스템의 네트워크 모델은 Fig. 1와 같다. 제안 시스템에서 보안 관리자는 문서 보안 검색에 사용되는 키워드를 추출하기 위해서 보안점검이 필요한 이미지 샘플을 웹 브라우저를 이용하여 업로드 한다. 웹 서버는 백엔드 서비스에서 구글 클라우드 비전의 광학문자인식 기술을 이용하여 업로드한 이미지에서 문자열을 추출한다. 문자열을 추출 후 단어로 분리하여 키워드로 사용하기 위해 데이터베이스에 저장한다. 이후 보안 점검이 필요한 스마트 기기를 가지고 있는 사용자는 스마트 기기에 설치되어있는 애플리케이션을 실행 후 API 서버로 이미지 파일을 전송하여 보안점검을 실행한다. API 서버는 스마트 기기에서 들어오는 이미지를 분석하여 데이터베이스에 저장된 키워드가 들어있는 이미지 파일을 식별하게 된다. 스마트 기기에는 많은 이미지 파일들이 있을 수 있으므로 이미 보안점검을 진행한 이미지는 넘기기 위해서 이미지 해시파일을 생성 후 서버에 별도로 저장하여 관리한다.

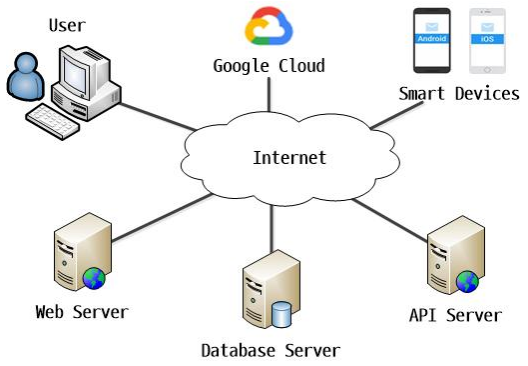

Fig. 1. Proposed network model

3.2 이미지 업로드 및 키워드 등록

Fig. 2는 문서보안 관리에 사용할 키워드를 등록하기 위한 절차를 나타낸다. 키워드를 추출하기 위한 이미지 파일을 웹 서버로 전송하고 웹 서버는 구글 클라우드 서비스의 광학문자인식 기술을 이용하여 문장을 추출 후 분리하여 키워드를 생성한다. 생성된 키워드는 데이터베이스 서버에 저장한다. 이미지 업로드 및 키워드 등록을 위한 세부 동작은 다음과 같다.

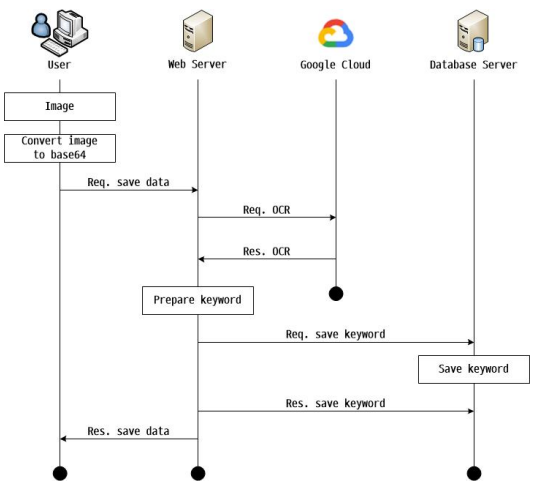

Fig. 2. Image upload and save keyword

① 사용자는 웹 브라우저를 이용하여 키워드를 추출할 이미지를 선택하여 base64로 인코딩한 후 웹 서버로 전송한다.

② 웹 서버에서 구글 클라우드 서비스의 광학문자인식 기술을 이용하기 위해서 base64 인코딩 정보와 이용할 서비스를 JSON 형태로 구글 클라우드 서비스로 전송한다.

③ 구글 클라우드 서비스에서 인식한 텍스트 정보를 웹 서버로 반환한다.

④ 웹 서버에서 텍스 정보를 개행 문자 단위로 분해하여 키워드를 생성한다. 이때 작은 따옴표, 큰 따옴표 같은 정보는 없애고 순수 문자 단위로 추출한다.

⑤ 추출한 문자를 데이터베이스 서버에 저장하고 사용자에게 정상 처리 응답을 전송한다.

3.3 보안문서 검색

Fig. 3은 사용자의 스마트 기기에서 보안문서 이미지를 검색하기 위한 절차를 나타낸다. 스마트 기기에 설치된 애플리케이션이 주기적으로 이미지 파일을 웹 서버로 전송하여 보안문서와 관련된 이미지 파일인지 검사한다. 이때 이미 검사가 완료된 이미지 파일은 검사를 생략하기 위하여 서버에서 내려 받은 이미지 해시 정보를 비교한다. 보안문서 이미지를 검색하기 위한 세부 동작은 다음과 같다.

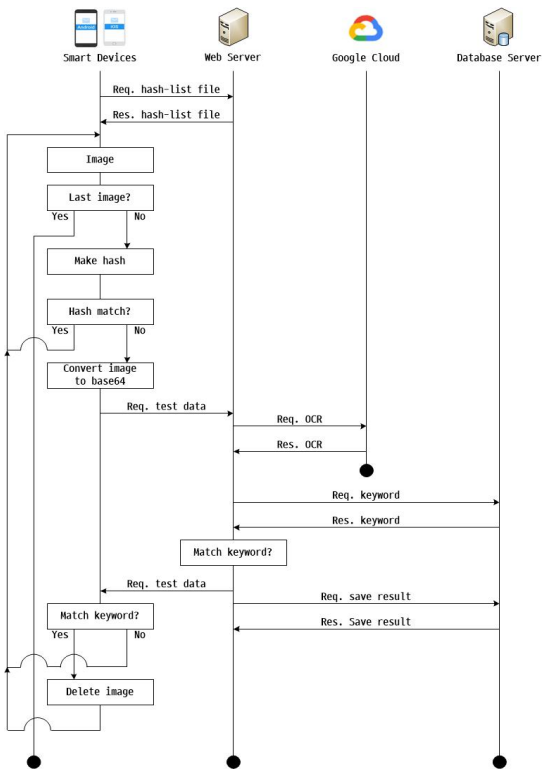

Fig. 3. Search and find image that has keyword

① 서버로부터 이미지 파일의 해시를 기록한 파일을 다운로드 받는다. 스마트 기기에 있는 이미지 파일의 보안검색이 진행될 때마다 이미지 해시 코드를 생성한다. 이후 이미지 해시를 비교해서 해시 로그에 있을 경우 보안 검색을 생략하여 불필요한 검색이 진행되는 것을 막는다.

② 보안검색이 필요한 이미지 파일이 없을 경우 애플리케이션을 종료한다. 보안검색이 필요한 파일이 있을 경우 이미지 파일을 base64로 인코딩한 정보를 서버로 전송한다.

③ 웹 서버에서 구글 클라우드 서비스의 광학문자인식 기술을 이용하기 위해서 base64 인코딩 정보와 이용할 서비스를 JSON 형태로 구글 클라우드 서비스로 전송한다.

④ 구글 클라우드 서비스에서 인식한 텍스트 정보를 웹 서버로 반환한다.

⑤ 데이터베이스 베이스에 저장된 키워드를 불러와서 인식한 텍스 정보와 일치율을 비교한다. 3개 이상 연속된 순서로 키워드가 일치하는 문장이 존재하거나 키워드가 5개 이상 검출된 경우 보안문서 이미지 파일로 간주한다. 제조공정 특징상 일상적인 생활에서 사용되는 용어와 수치가 작업지시서에 들어있을 확률이 적기 때문에 키워드 검색만으로도 충분히 보안문서 검색이 가능하다.

4. 제안 시스템 구현

제안 광학문자인식 기반 보안문서 관리 알고리즘을 적용한 시스템을 구현하기 위해서 파이썬 기반의 플라스크 웹 프레임워크를 이용하여 웹서버와 API 서버를 구현하였다. 사용자 인증과 보안문서 관리를 처리하기 위한 키워드 및 로그 기록을 위해서 MariaDB를 이용하여 데이터베이스 서버를 구성하였다. 스마트 기기에서 동작하는 보안문서 관리 애플케이션은 아파치 코도바를 이용하여 하이브리드 방식으로 개발하여 동일한 소스코드를 이용하여 안드로이드, iOS에서 실행이 가능하도록 구현하였다.

Table 3은 사용자 정보를 관리하는 테이블로서 사용자 인증에 사용된다. 사용자 구분자로 사용되는 id, 이름을 저장하는 name, 로그인에 사용하는 이메일, 비밀번호를 저장하는 password 필드, 정보 생성한 연월일을 저장하는 created, 정보 수정한 연월일을 저장하는 updated 필드로 구성된다.

Table 3. USER table scheme

Field	Type	Etc
id	INTEGER	PRIMARY KEY AUTO INCREMENT NOT NULL
name	VARCHAR(10)	NOT NULL
email	VARCHAR(100)	NOT NULL
password	VARCHAR(255)	NOT NULL
created	DATETIME	NOT NULL
updated	DATETIME	NOT NULL

Table 4는 보안문서를 검색하는데 사용되는 키워드를 추출하기 위한 이미지 파일 정보를 저장해 놓는 테이블의 구조를 보여준다. 이미지 관리 테이블은 정보 구분자인 id, 원본 이미지의 base64 정보 필드 original_base64, 썸네일 이미지의 base64 정보 필드 thumbnail_base64 , 원본 파일 정보 필드 original_filename, 썸네일 파일 정보 필드 thumbnail_filename, 정보 생성한 연월일을 저장하는 created, 정보 수정한 연월일을 저장하는 updated 필드로 구성된다.

Table 4. IMAGE table scheme

Field	Type	Etc
id	INTEGER	PRIMARY KEY AUTO INCREMENT NOT NULL
original_base64	LONGTEXT	NOT NULL
thumbnail_base64	LONGTEXT	NOT NULL
original_filename	VARCHAR(100)	NOT NULL
thumbnail_filename	VARCHAR(100)	NOT NULL
created	DATETIME	NOT NULL
updated	DATETIME	NOT NULL

Table 5는 보안문서를 검색하는데 사용되는 키워드를 추출하기 위한 이미지 파일 정보를 저장해 놓는 테이블의 구조를 보여준다. 키워드 관리 테이블은 정보 구분자인 id, 키워드를 저장하는 keyword, 외래키로서 이미지 구분자를 나타내는 image_id, 정보 생성한 연월일을 저장하는 created, 정보 수정한 연월일을 저장하는 updated 필드로 구성된다.

Table 5. KEYWORD table scheme

Field	Type	Etc
id	INTEGER	PRIMARY KEY AUTO INCREMENT NOT NULL
image_id	INTEGER	FOREIGN KEY(IMAGE.id) NOT NULL
keyword	VARCHAR(50)	NOT NULL
created	DATETIME	NOT NULL
updated	DATETIME	NOT NULL

Fig. 4는 광학문자인식 기술을 이용하여 키워드를 추출하기 위해서 이미지를 등록하는 화면이다. 등록된 이미지는 구글 클라우드 서비스를 이용하여 키워드를 추출하고 향후 관리를 위해서 데이터베이스에 저장한다. 이미지 등록은 보안문서를 아무나 관리할 수 없도록 관리자가 직접 등록한다.

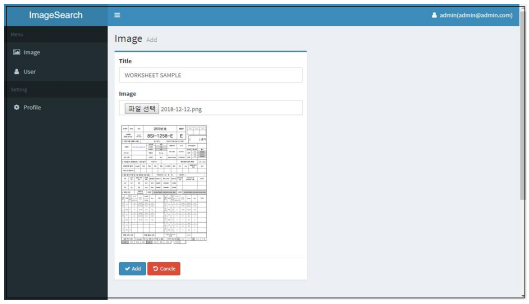

Fig. 4. Image upload screen

Fig. 5는 등록된 이미지 파일을 보여주는 목록 화면이다. 이미지 파일의 썸네일, 원본 파일명, 썸네일 파일명, 등록일자를 보여준다. 목록에서 키워드 관리를 누르면 이미지를 통해 추출되어 등록된 키워드를 보여준다.

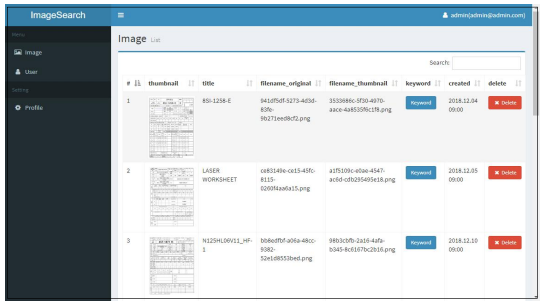

Fig. 5. Image list screen

Fig. 6은 애플리케이션을 이용하여 보안문서 이미지를 찾아내고 처리하는 화면이다. 검색 버튼을 누르면 보안문서 이미지 검색을 진행하고 기록 버튼을 누르면 그동안의 처리된 이미지 파일의 목록과 처리 결과를 보여준다. 사용자의 편의성을 고려하여 애플리케이션은 버튼 클릭만으로 바로 동작하도록 구성하였으며 사용자에게 불편을 주지 않고 자동으로 백그라운드에서 처리할 수 있도록 실행 주기를 등록할 수 있도록 하였다.

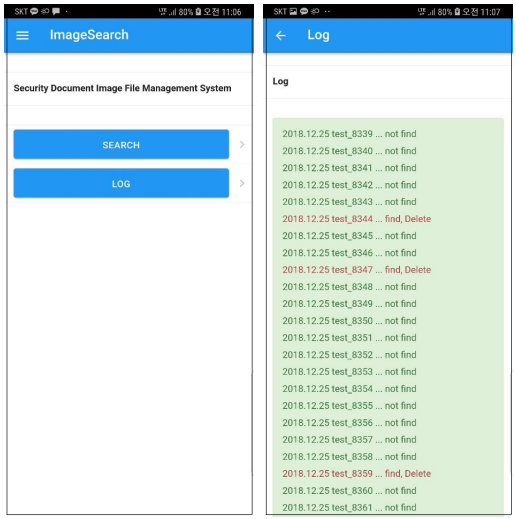

Fig. 6. Smart device application screen

5. 제안 시스템 평가

본 장에서는 광학문자인식 기술을 이용한 보안문서 이미지 파일 관리 시스템의 성능을 평가하고 제안 시스템에 대한 효용성 평가를 논의한다. 효용성 평가의 기준으로 처리시간, 편의성을 통해 제안 시스템의 효용성을 평가한다.

5.1 처리시간

Table 6은 스마트폰에 설치된 애플리케이션으로 이미지 파일을 처리하는데 걸린 시간을 나타내며 100개, 1,000개, 10,000개 파일의 처리 시간을 보여준다. 사용된 스마트폰은 LTE에 연결되어 있는 갤럭시 노트8을 사용하였다. 이미지 파일의 크기는 100kbyte에서부터 최대 3MByte 크기로 다양하게 존재한다. 보안문서 이미지와 일반 이미지는 1:9의 비율로 존재한다. 일일 1,000개 이상의 파일을 찍고 보관할 상황은 없을 것으로 판단되지만

개발시스템의 성능을 평가하고는 것을 목적으로 하여 최대 10,000개까지의 이미지 파일을 처리하는 것으로 성능평가를 진행하였다. 처리시간은 보안문서 이미지 검색, 보안문서 이미지 백업 및 스마트 기기에서 삭제, 해시 생성을 포함하는 시간이다. 평균시간은 전체 처리시간을 전체 이미지 파일수로 나눈 시간을 의미한다. 성능평가 결과 1000장의 이미지 파일을 처리하는데 걸린 시간은 약 1091.6초로서 평균처리 시간은 약 1.1초이다. 백그라운드로 처리하는 것을 감안한다면 20분 주기로 10,000장을 처리하는 것이 가능한 것을 알 수 있다.

Table 6. Image file processing time

Number [EA]	Processing time [seconds]	Average time [seconds]
100	117.8734574	1.178734
1,000	1091.6410079	1.0916410
10,000	11423.0117130	1.1423011

5.1 편의성

편의성이란 휴대가 용이하고 언제 어디서나 쉽고 간편하게 서비스를 이용할 수 있는 기술인지를 말한다. 본 논문에서 제시한 보안문서 이미지를 검색하고 처리하는 시스템은 아파치 코도바를 이용한 하이브리드 개발 방식으로 개발되어 안드로이드, iOS에 설치가 가능하며 스마트폰에 애플리케이션을 설치하고 버튼 클릭 한번만으로 쉽게 검색이 가능한 기술로 평가할 수 있다. 또한 구동서버는 파이썬 플라스크 기반으로 제작하여 소스코드 수정 없이 다양한 운영체제에서 실행이 가능한 기술로 평가할 수 있다.

6. 결론

정보통신 기술의 발달로 스마트 기기가 널리 보급되고 많은 제조현장에서 스마트 기기를 사용하여 업무에 활용하고 있다. 제조현장에서는 사무업무와는 다르게 컴퓨터를 이용하여 작업관련 정보를 저장하기가 어렵기 때문에 작업 환경 특성상 쉽고 편하게 업무를 진행하기 위해서 문서를 사진으로 찍고 타인과 공유하거나 시스템에 업로드하는 일로 업무를 처리하는 경우가 많다. 이러한 특이성 때문에 작업자가 의도하지 않게 작업자의 스마트폰에 보안문서 이미지가 보관되어 있는 경우가 많으며 외부로 쉽게 노출될 수 있는 환경에 놓이게 된다. 제조업은 작업자의 보안에 대한 낮은 인식수준과 외국인 작업자와의 의사소통 문제 때문에 보안문서 이미지를 철저하게 관리가 어려우며 많은 작업자의 스마트기기 사용을 일률적으로 통제할 경우 작업시간 관리 및 실적관리에 어려움이 발생할 수 있다. 본 논문에서는 스마트폰을 이용하여 보안문서 이미지를 관리하는 제조공정에서 필요한 광학문자인식 기반 보안문서 관리 시스템을 제안하였다. 사용자의 스마트 기기에 애플리케이션을 설치해놓고 실행주기를 맞춰놓으면 자동으로 주기적으로 백그라운드에서 동작하며 이미지 파일을 찾아내고 삭제한다. 애플리케이션 동작에 특별한 관리가 필요 없기 때문에 작업자의 업무에 지장을 주지 않고 보안문서 이미지 파일을 쉽게 검색하고 처리할 수 있으며 의사소통에 문제가 있는 외국인 작업자도 쉽게 이용이 가능한 시스템이다. 향후 스마트 팩토리 구축을 위해서 사용되는 생산관리시스템에 본 연구 결과물을 적용하여 제조현장에서의 보안성을 향상시킬 수 있는 추가 연구를 진행할 계획이다.

REFERENCES

[1] S. U. Kang & Y. S. Choi. (2014). Design of Open Collaboration Solution's Server for Smart Work. Journal of the Institute of Electronics and Information Engineers, *51(7).* 133-141.

[2] J. S. Kim & K. S. Han. (2016). The key technology factors of Smart work and the situations in Korea and overseas. The Korea Contents Association Review *14(1)*, 14-20.

[3] S. E. Yoo & S. Y. Lee. (2013). An Analysis on Types of Smart Workplace and its Planning Strategies. Journal of Korea Design Knowledge, 25, 279-288.

[4] S. H. Lee, H. J. Jun & T. S. Kim. (2018). A Study on Cyber Security Risk Management for Diffusion of Korean Smart Factories. The Journal of Korean Institute of Communications and Information Sciences, *43(10)*. 1741-1750.

[5] S. H. Paik, S. K. Kim & H. B. Park. (2010). Design and Implementation of Network Access Control for Security of Company Network, The Institute of Electronics Engineers of Korea - Telecommunications, *47(12)*, 90-96.

[6] W. R. Jeon, J. Y. Kim, Y. S. Lee & D. H. Won. (2011). Analysis of Threats and Countermeasures on Mobile

Smartphone, Journal of the Korea Society of Computer and Information, *16(2)*, 153-163.

[7] B. I. Kang & S. J. Kim. (2014). Study on Security Grade Classification of Financial Company Documents, Journal of the Korea Institute of Information Security & Cryptology, *24(6),* 1319-1328.

[8] Y. J. Lee, Y. H. Jang & S. C. Park (2016). Design and Implementation of App Control System for Improving the Security of the Mobile Application, Journal of The Korea Contents Association, *16(2),* 243-250.

[9] J. H. Lee, D. H. Lee & H. K. Kim. (2012). Decision Support System to Detect Unauthorized Access in Smart Work Environment. Journal of the Korea Institute of Information Security & Cryptology, *22(4),* 797-808.

[10] C. Kwan. (2015). Rethinking of Situational Context and Characteristic of Industrial Secrets Leakage: Some National Security and Psychological Perspectives. The Korean Journal of Forensic Psychology, *6(1),* 1-11.

[11] J. S. Park & J. C. Ha. (2012). Vulnerability Analysis of Security Document Management in Multi Function Peripheral and Its Countermeasure, Journal of Korean Institute of Information Technology, *10(6),* 133-143.

[12] K. S. Sung, D. Y. Oh, J. J. Kim, W. S. Na & H. S. Oh. (2008). Study on the Efficiency System Design for Minimize the Information Leak of the E-Document Store Service, The Journal of The Korean Institute of Communication Sciences, *33(10)*, 350-358.

[13] B. H. Kang. (2018). 5 Topics for Education and Research in Business Ethics. Journal of Digital Convergence, *16(8),* 137-150.

[14] Google. (2018). Firebase Documentation. Firebase(Online). https://firebase.google.com/docs

[15] Apache Cordova. (2018). Apache Cordova Documentation. Apache Cordova Documentation(Online). https://cordova.apache.org/docs/en/latest

정 필 성(Jeong, Pil-Seong) [정회원]

- 2014년 2월 : 서울과학기술대학교 전자공학과(공학사)
- 2007년 8월 : 광운대학교 전자통신공학과(공학석사)
- 2013년 8월 : 광운대학교 전자통신공학과(공학박사)
- 2018년 3월 ~ 현재 : 명지전문대학 정보통신공학과 조교수
- 관심분야 : 사물인터넷, WSN, 임베디드 시스템
- E-Mail : ibetter.kr@gmail.com

조 양 현(Cho, Yang-Hyun) [정회원]

- 1982년 2월 : 광운대학교 전자통신공학과(공학사)
- 1985년 2월 : 광운대학교 전자통신공학과(공학석사)
- 2012년 2월 : 광운대학교 전자통신공학과(공학박사)
- 1987년 9월 ~ 1997년 8월 : LG정보통신 전송기술개발실 과장
- 1997년 9월 ~ 현재 : 삼육대학교 컴퓨터·메카트로닉스공학부 교수
- 2014년 3월 ~ 2016년 2월 : 삼육대학교 산학협력단장/연구처장
- 관심분야 : 컴퓨터네트워크, 통신망(BcN), GMPLS, IoT
- E-Mail : yhcho@syu.ac.kr