Journal of KIIT. Vol. 17, No. 7, pp. 95-101, Jul. 31, 2019. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2019.17.7.95

동적 영상 식별정보에 대한 접근 권한별 마스킹 메커니즘

김진수*, 김상춘**, 박남제***

Access Control Masking Mechanism to Dynamic Image Identification Information

Jinsu Kim*, Sangchoon Kim**, and Namje Park***

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 [2019-0-00203,선제적 위험대응을 위한 예측적 영상보안 핵심기술 개발]. 그리고, 이 논문은 2018년도 강원대학교 대학회계의 지원을 받아 수행한 연구임

요 약

치안 강화의 일종이며, 사후 대책의 일환으로 사용되는 영상감시 시스템은 주로 사람의 통행이 잦은 공공장소에 설치되어 촬영된 영상을 관제 센터로 전송한다. 촬영된 영상은 일반적으로 암호화되거나 영상정보 내에 존재하는 개인 인식이 가능한 데이터에 해당 영역을 시각적으로 식별이 불가능하도록 마스킹을 적용하여 저장되는데, 저장된 영상은 적법한 사용자에 의해 원본 이미지로 복원된다. 하지만 이는 해당 영상 데이터에 존재하는 모든 영역이 복원되며 영상 데이터에서 요구된 대상 이외의 피사체의 사생활 침해를 야기할 수 있다. 본 문에서는 접근하는 사용자의 권한에 따라 영상 데이터 내의 복원 가능 대상을 제한하여 영상 내의 사생활 침해를 최소화하는 메커니즘을 제안한다.

Abstract

The video surveillance system, which is used as a part of security measures, is installed in a public place where people pass frequently and transmits the captured images to the control center. The photographed image is generally stored by applying masked to the data that can be ciphered or existing in the image information so that the corresponding region cannot be visually identified. The stored image is restored to the original image by a legitimate user. However, this means that all the regions existing in the corresponding image data are restored and may cause the privacy invasion of the object other than the object requested in the image data. In this paper, we propose a mechanism to minimize the invasion of privacy in images by restricting the restorable objects in the image data according to the access rights of the users.

Keywords

the video surveillance system, control center, security, restored image, privacy, legitimate user

* 강원대학교 대학원 정보통신공학전공 석사과정
제주대학교 사이버보안인재교육원 연구원
- ORCID: https://orcid.org/0000-0003-1009-3928
** 강원대학교 정보통신공학전공 교수
- ORCID: https://orcid.org/0000-0001-9401-4232
*** 제주대학교 초등교육학과 교수
- ORCID: https://orcid.org/0000-0003-4434-8933

· Received: Feb. 25, 2019, Revised: Apr. 30, 2019, Accepted: May 03, 2019
· Corresponding Author: Sangchoon Kim and Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

Ⅰ. 서 론

저장 장치에 기록된 영상정보는 해당 영상감시 장치를 관리하는 CCTV(Closed Circuit Television) 관제센터에서 적법한 접근 권한을 가진 관리자에게 제공되어 대상 지역에서 발생할 수 있는 사건이나 사고를 예방하고, 발생한 사태의 사후조사를 위한 근원 파악이나 사태 해결의 근거를 제시할 목적으로 사용 될 수 있다[1]-[3].

피사체를 식별할 수 있는 개인정보는 대상 추적에 사용될 수 있어 복원될 수 있어야하며, 이를 위하여 영상 내의 모든 식별정보를 일괄적으로 마스킹하거나, 영상 데이터 전체를 암호화하여 제 3자에 의한 유출이 어렵도록 한다. 하지만 접근 권한이 있는 정당한 사용자에 의하여 영상이 복원될 경우, 영상정보 내의 영상이 복원되어 관리자에게 제공하게 된다. 원본으로 복원된 영상정보는 추적 대상 외의 모든 피사체에 대한 식별정보까지 복원하므로 복원된 추적 대상이 아닌 피사체에 대한 중대한 사생활 침해가 될 수 있다[4]-[6].

본문에서는 영상정보의 피사체에 대해 접근하는 관리자의 접근 권한에 따라 개별적으로 마스킹을 진행함으로서 관리자가 접근할 수 없는 영상정보의 유출을 방지하여, 추적 대상이 아닌 피사체에 대한 프라이버시 침해를 최소화하고 개인의 프라이버시를 보장하는 메커니즘을 소개하도록 한다. 본문의 구성은 2장에서 기존 선행기술을 분석하고, 3장에서 제안된 동적 영상 식별정보에 대한 접근 권한별 마스킹 메커니즘을 소개하도록 한다. 4장에서 기존 방법론과 제안된 메커니즘을 비교분석함으로서 기존 방법론과의 차이점을 보이도록 한다.

Ⅱ. 기존 영상 마스킹 기법 특허 분석

노출되는 대상의 프라이버시 보호를 위해 다양한 연구가 진행되고 있으며, 국내에서는 주로 영상 반출 보안 시스템으로 상용화되고 있다. 다음은 국내 상용화된 프라이버시 보호 제품을 분석한 것이다.

2.1 동영상 마스킹 처리방법 및 장치

동영상 마스킹 처리방법 및 장치는 영상정보에 존재하는 프레임을 촬영하여 촬영된 프레임에 존재하는 하나 이상의 식별정보를 마스킹하고, 마스킹에 대한 정보를 프레임 내에 삽입하여 삽입된 프레임으로 영상정보를 저장하는 방법이다. 해당 특허는 녹화된 영상정보에 대해 마스킹을 진행하며, 마스킹에 사용된 특정 키값은 이후 언마스킹 과정에서 사용하게 된다. 마스킹 정보는 마스킹된 해당 프레임에 저장된다[7].

2.2 보행자의 얼굴 검출 기반의 동적 객체 영상 프라이버시 보호 장치 및 그 방법

보행자의 얼굴 검출 기반의 동적 객체 영상 프라이버시 보호 장치 및 그 방법은 동적으로 촬영되는 영상정보 중 마스킹을 진행할 영상정보를 프레임단위로 해당 프레임 내의 객체를 추출하여 마스킹하는 방법이다. 해당 특허에서 원본 영상정보는 마스킹된 영상정보로 치환되며, 마스킹에 대한 복호화키는 DB에 저장된다. 마스킹 영역은 원거리인 경우 보행자를 근거리인 경우에는 얼굴 검출을 통해 동적 객체를 자동적으로 검출하여 해당 영역에 마스킹을 진행한다. 마스킹된 영상은 DB에 인증키를 저장하고, 저장된 인증키는 워터마킹을 추출하여 영상을 복원하는데 사용된다[8].

2.3 개인정보 보호를 지원하는 영상정보 처리기기 및 방법

개인정보 보호를 지원하는 영상정보 처리기기 및 방법은 다수의 영상감시 시스템에 의하여 녹화된 영상이 영상감시 장치를 벗어나 외부로 전송되어야 할 경우 프라이버시를 침해하지 않도록 하는 방법으로 수사기관의 요청 등에 의해서 영상정보가 요구될 경우 해당 제어신호를 전송받았을 때 마스킹을 적용하며, 동작신호가 수신된 경우에는 카메라의 동작 상태를 규칙정보와 비교하여 일치 여부를 확인한 후, 불일치하는 경우 관리자에게 해당 내용을 전송한다. 해당 특허에서 마스킹은 저장부에 별도의 저장영역을 생성함으로서 마스킹 영상을 저장하고,

사용자에게 제공한다. 마스킹 영역은 식별정보가 포함되는 영역이나, 수동적으로 지정하는 방식을 사용한다[9].

III. 제안된 접근 권한에 따른 접근 가능 영상정보를 제한하는 마스킹 메커니즘

본문에 제안된 메커니즘은 촬영된 영상을 녹화하고, 녹화된 영상을 저장하는 DB에 저장하여 해당 영상 내에 존재하는 특정 개인을 유추할 수 있는 식별정보를 가진 객체를 추출하고 추출된 정보에 식별 DB에 존재하는 개인 식별정보와 비교하여 객체가 실제로 식별정보를 가지고 있는지 확인한다. 이후 영상을 요청한 적법한 사용자의 권한에 따라 권한을 벗어나는 객체에 대해 마스킹을 적용하고, 권한 내의 객체는 원본영상으로서 사용자에게 제공한다. 제안된 메커니즘은 영상 수집 모듈, 영상 DB 모듈, 영상 서비스 모듈, 오브젝트 추출 모듈, 식별 DB 모듈, 오브젝트 식별 모듈, 권한 DB 모듈, 마스킹 처리 모듈로 구성된다[10]-[12]. 그림 1은 제안된 메커니즘의 구상도를 보이는 것이다.

3.1 영상 수집 모듈

영상 수집 모듈은 영상정보를 전송하는 영상촬영매체로부터 영상정보를 수집하며, 영상정보에는 동영상과 이미지가 포함될 수 있다. 영상정보를 전송하는 대상에는 영삼감시 시스템에 포함되는 다수의 CCTV나 USB(Univeral Serial Bus), IP(Internet Protocol) 카메라 등이 사용될 수 있다[13][14].

3.2 영상 DB 모듈

영상 DB 모듈은 영상 수집 모듈의 영상촬영매체로부터 수신된 영상정보를 저장하는 스토리지로 이후 마스킹 처리를 위한 영상정보를 저장하며, 영상정보 내의 개인정보를 식별할 수 있는 객체의 인식을 위해 원본 영상정보를 가진다. 해당 모듈은 마스킹 처리된 영상정보를 영상 DB에 저장되지 않으므로 사용자의 요청에 의해 마스킹 처리된 영상정보를 저장하지 않으므로 추가적인 저장공간을 요구하지 않는다[15][16].

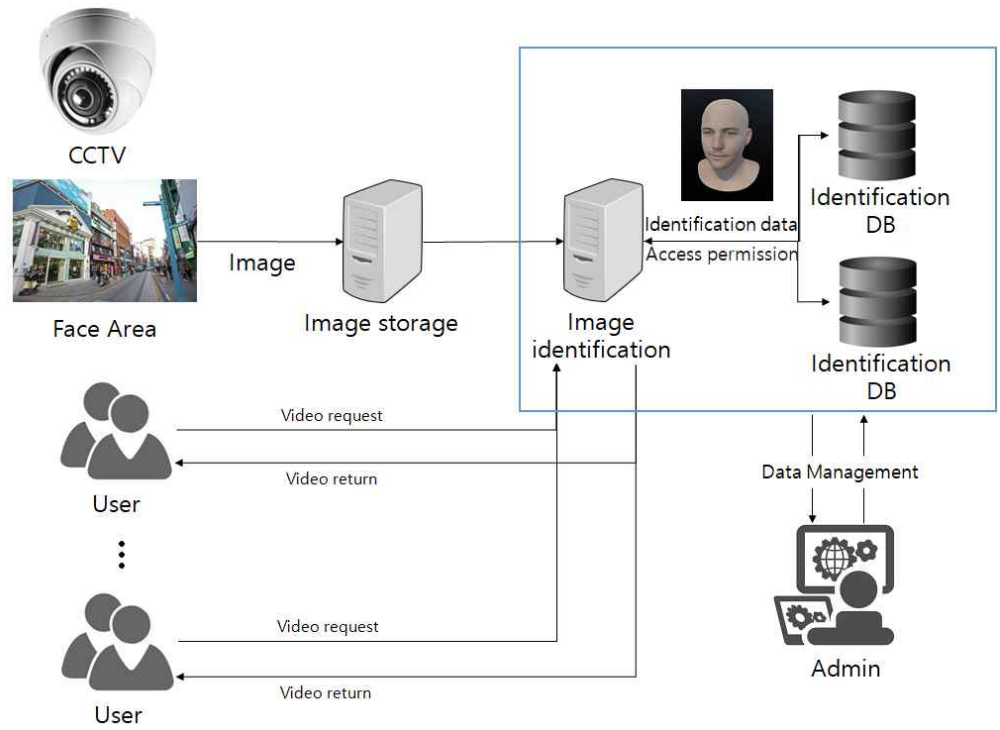


그림 1. 제안된 메커니즘의 구상도
Fig. 1. Conception of proposed mechanism

3.3 영상 서비스 모듈

영상 서비스 모듈은 적법한 사용자에 의한 영상정보 재생요청을 수신할 경우, 영상정보에 대한 재생을 요청한 사용자의 접근 권한에 따라 마스킹 처리 모듈에서 영상정보에 포함된 요청한 사용자의 접근권한을 벗어나는 식별정보를 마스킹 처리 모듈로부터 마스킹 처리받은 영상정보를 제공받아 사용자에게 응답으로서 전송하는 역할을 가진다. 영상 서비스 모듈은 사용자의 접근권한에 따라 제공되는 영상정보의 개수, 접근 가능한 영상감시 장치를 조절할 수 있다[17]-[19].

3.4 오브젝트 추출 모듈

오브젝트 추출 모듈은 사전에 정의된 특정한 개인임을 유추할 수 있는 개인 식별정보를 추출하며, 식별정보에는 피사체의 얼굴 영역이나 차량의 번호판을 포함될 수 있다. 오브젝트 추출 모듈에서는 정지된 영상 내에서 영상정보에 존재하는 피사체에 대해 식별정보에 대한 특징점을 찾아 해당 영역에 존재하는 피사체의 식별정보가 포함된 것으로 추정되는 모든 객체를 추출한다. 이때, 사용 가능한 특징 추출 기법에는 지식기반 방법, 특징기반 방법, 템플릿 매칭 방법(Template based matching), 외형기반 방법 등이 있으며, 이 방법을 적용하여 영상정보 내에 존재하는 개인 식별정보를 추출한다[20][21].

3.5 오브젝트 식별 모듈

오브젝트 식별 모듈은 오브젝트 추출 모듈에서 특정한 개인을 식별할 수 있다고 추측되는 식별정보로서 추출된 객체에 대한 데이터를 식별정보를 저장하고 있는 식별 DB 모듈에 저장된 데이터와 비교함으로서 오브젝트 추출 모듈에서 추출된 영상정보 내의 식별정보에 대한 영역과 식별 DB 모듈에 저장되어 있는 식별정보의 유사성을 계산하고, 일정 이상의 유사도를 가지는 객체를 식별한다. 오브젝트 식별 모듈은 오브젝트 추출 모듈에 의해 추출된 모듈에 대해서만 식별을 진행함으로 영상정보 전체에 대한 식별을 진행하는 방식보다 적은 시스템 리소스를 사용한다.

3.6 식별 DB 모듈

식별 DB 모듈은 객체와 비교하여 특정한 개인임을 유추 가능한 영상정보를 식별할 수 있는 식별 데이터가 저장된 스토리지이다. 식별 DB 모듈에 저장되는 식별정보는 오브젝트 추출모듈에서 추출된 특징점에 비교하여 특정 오브젝트임을 인식할 수 있도록 하는 정보를 말하며, 식별할 수 있는 특정한 인물, 범죄자로 등록된 인물 혹은 남자나 여자를 구분하기 위한 정보, 특정 번호의 자동차 번호판에 대한 정보 등을 포함하여 오브젝트에 대한 식별정보를 제공한다.

3.7 마스킹 처리 모듈

마스킹 처리 모듈은 권한 DB 모듈에 대해 사용자의 접근 권한을 확인하기 위한 권한 조회의 권한을 가지며, 접근하는 사용자의 접근 권한을 추출된 오브젝트 각각에 대해 권한 DB 모듈에서 확인하고, 접근 권한에 따라 객체에 대한 개별적인 마스킹 처리를 진행할 수 있다. 마스킹 처리 모듈은 영상 서비스 모듈에서 영상 요청이 인가된 경우 접근한 사용자의 접근 권한을 권한 DB 모듈에 적시되어 있는 접근 권한을 벗어난 객체에 대해 마스킹 처리를 진행하고, 마스킹된 영상을 영상 서비스 모듈로 반환한다. 마스킹 처리 기법에는 색상 처리, 음영 처리, 명도 처리, 채도 처리, 그림자 처리, 모자이크, 블렌딩, 블러링 기법이 사용될 수 있다. 마스킹 처리 모듈에서 진행하는 마스킹 처리는 추출된 모든 객체에 대하여 사용자의 권한에 따른 허가 여부를 판별하며, 사용자에게 허가되지 않은 객체에 대해서만 마스킹을 진행한다. 마스킹 처리 모듈에서 진행되는 마스킹은 기존의 기법과 달리 접근권한에 따라 단계적으로 영상정보에 존재하는 식별정보를 마스킹하는 과정을 진행한다.

3.8 권한 DB 모듈

권한 DB 모듈은 인가된 사용자의 접근 권한을 가지고 있는 스토리지로, 접근 권한에 따라 제공되는 영상에 대한 마스킹 처리 규칙을 가진다. 권한 DB 모듈은 마스킹 처리 모듈에서 오브젝트 식별 모듈에 의해 식별된 오브젝트에 대한 마스킹 처리를 진행하는 과정에서 각각의 오브젝트에 대한 사용자의 접근 허가 또는 불가를 선별하기 위한 권한 정보를 가지고 있으며, 마스킹 처리 모듈의 요청에 따라 각각의 오브젝트에 대해 권한 정보를 제공한다. 권한 DB 모듈에 저장되어있는 접근권한에 의해 영상정보 요청자들은 같은 영상정보에 대해 서로 다른 마스킹 영역을 가진 영상정보를 얻을 수 있다.

Ⅳ. 제안된 메커니즘과 기존 메커니즘의 비교 분석

본 장에서는 영상정보에 존재하는 식별정보에 대한 마스킹 처리, 사용자의 요청에 의한 영상 제공, 영상 DB의 영상정보 저장 구분, 권한에 다른 마스킹 객체 선별의 항목을 대상으로 제안된 메커니즘와 기존의 메커니즘을 비교하여 보이도록 한다.

3.1 동영상 마스킹 처리방법 및 장치와의 비교 분석

영상정보 내에 존재하는 식별정보를 자동적으로 추출하여, 해당 정보를 마스킹하고, 영상정보를 마스킹된 영상정보로만 저장하게 된다. 또한 해당 메커니즘은영상의 원본을 마스킹된 영상으로 저장하므로 추가적으로 저장하기 위한 스토리지가 요구되며, 접근권한에 관계없이 모든 식별정보를 마스킹 처리한다.

3.2 보행자의 얼굴 검출 기반의 동적 객체 영상 프라이버시 보호 장치 및 그 방법과의 비교분석

해당 메커니즘은 사용자의 요청이 없는 경우 촬영되는 영상정보를 자동적으로 마스킹하고, 언마스킹키를 별도의 DB에 저장한 뒤, 마스킹된 영상정보만을 저장한다. 이후 사용자의 영상정보 요청이 들어올 경우, 마스킹 영상을 저장되어있는 언마스킹키를 이용하여 복호화한 뒤 사용자에게 제공한다. 이 과정에서 언마스킹 영역은 요청된 영상정보의 모든 식별정보에 대해 진행되므로 요청자에게 요구되는 최저한의 식별정보 이상을 제공하게 된다.

3.3 개인정보 보호를 지원하는 영상정보 처리기기 및 방법과의 비교 분석

해당 메커니즘은 식별정보가 포함된 영상정보가 외부에 유출되어야하는 경우 영상정보 내의 식별정보를 마스킹한 후 전송하는 방식이다. 이 과정에서 마스킹된 영상은 마스킹되지 않은 원본 영상정보와 별도로 저장되며, 이에 따른 추가적인 저장소가 요구된다. 이 과정에서 마스킹 영역은 영상정보 요청자의 권한에 관계없이 이뤄지게 된다.

3.4 제안된 메커니즘의 차별성

제안된 메커니즘은 앞선 방법론과 같은 영상정보 내의 식별정보 마스킹 메커니즘이나 기존의 메커니즘과는 달리 영상정보 요청 예상자의 접근권한을 별도의 모듈에 저장하여 저장하며, 접근권한 외의 요청자에게 영상이 유출되지 않도록 한다는 차별성이 존재한다. 또한, 허가된 요청자의 경우에만 접근이 허가된 식별정보만을 획득할 수 있도록 허가되지 않은 식별정보에 대한 마스킹을 진행한다.

표 1은 기존의 선행기술과 제안된 메커니즘의 차이를 보이는 것이다.

표 1. 제안된 메커니즘과 기존 기법의 비교 분석
Table 1. Comparative analysis of proposed mechanisms and existing techniques

Comparison item	Patent 1	Patent 2	Patent 3	Proposed mechanism
Apply to mask	O	O	O	O
Processing by user request	X	O	O	O
Store only the original image in the repository	X	X	O	O
Partial masking according to the access authority	X	X	X	O

Ⅳ. 결 론

영상감시 시스템에 의해 촬영된 영상은 관제 시스템을 관리하는 관리자에 의해 사용된다. 이 과정에서 영상정보에 포함된 개인의 식별정보가 유출될 수 있으며, 관리자의 필요 이상의 식별정보를 제공할 수 있다.

일반적으로 사용되고 있는 일괄 언마스킹 방식은 식별정보의 유출경로를 늘릴 수 있으며, 매년 증가하는 영상감시 시스템에 의해 사생활 침해의 목소리가 높아져가고 있다. 이와 같은 문제를 해결하기 위해 영상정보 내의 식별정보를 영상 사용자에게 요구되는 최소한의 정보만을 제공해야한다. 본문에서 제안된 접근권한에 따른 식별정보 마스킹 방식은 영상정보 내의 식별정보를 최소화함으로서 유출경로를 최소화할 수 있다.

현재 영상감시 시스템은 공공의 안전성이라는 목적 하에 묵시적으로 피해를 이해하고 있으나, 빅데이터 분석 기술의 발전에 의해 영상내의 식별정보를 통해 피사체의 개인정보가 유출되는 경로를 최소화할 수 있는 방법이 연구되어야 한다.

References

[1] N. Park, H. Hu, and Q. Jin, "Security and Privacy Mechanisms for Sensor Middleware and Application in Internet of Things (IoT)", International Journal of Distributed Sensor Networks, Vol. 12, No. 1, Jan. 2016. https://doi.org/10.1155/2016/2965438.

[2] D. Lee and N. Park, "Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment", International Journal of Personal And Ubiquitous Computing, Vol. 22, No. 1, pp. 1-30, Feb. 2018.

[3] Donghyeok Lee and Namje Park, "Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance", International Journal of Supercomputing, Vol. 73, No. 3, pp. 1103-1118, Mar. 2017.

[4] N. Park and M. Kim, "Implementation of load management application system using smart grid privacy policy in energy management service environment", International Journal of Cluster Computing, Vol. 17, No. 3, pp. 653-664, Sep. 2014.

[5] N. Park, "Design and Implementation of Mobile VTS Middleware for Efficient IVEF Service", Journal of KICS, Vol. 39, No. 6, pp. 466-475, Jun. 2014.

[6] N. Park, "Implementation of inter-VTS data exchange format protocol based on mobile platform for next-generation vessel traffic service system", International Journal of INFORMATION (Japan), Vol. 17, No. 10, pp. 4847-4856, Oct. 2014.

[7] S. Park and S. Jung, "Video masking processing method and apparatus", K. R. Patent No.102014 0168097, Jul. 2016.

[8] Y. Park, "Dynamic Image Object Privacy Protection Device And The Method Of Detecting The Face Of The Pedestrian Based", K. R. Patent No.1020160030090, Mar. 2016.

[9] Y. Park and J. Park, "Apparatus and method for processing image information to support protection of personal information", K. R. Patent No.1020150175134, Dec. 2015.

[10] N. Park, "The implementation of open embedded S/W platform for secure mobile RFID reader", Journal of KICIS, Vol. 35, No. 5, pp. 785-793, May 2010.

[11] N. Park, "Privacy-Enhanced Deduplication Technique in Closed Circuit Television Video Cloud Service Environment", International Journal of Engineering & Technology, Vol. 7, No. 24, pp. 65-66, May 2018.

[12] J. Kim, N. Park, G. Kim, and S. Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia", International Journal of ELECTRONICS, Vol. 8, No. 4, pp. 412, Apr. 2019.

[13] N. Park and N. Kang, "Mutual Authentication

Scheme in Secure Internet of Things Technology for Comfortable Lifestyle", International Journal of Sensors(Basel), Vol. 16, No. 1, pp. 1-16, Dec. 2015.

[14] N. Park, "UHF/HF Dual-Band Integrated Mobile RFID/NFC Linkage Method for Mobile Device-based Business Application", Journal of KICS, Vol. 38, No. 10, pp. 841-851, Oct. 2013.

[15] N. Park, "Implementation of Terminal Middleware Platform for Mobile RFID Computing", International Journal of AHUC, Vol. 8, No. 4, pp. 205-219, Nov. 2011.

[16] N. Park, J. Kwak, S. Kim, D. Won and H. Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment", Conference of Advanced Web and Network Technologies, and Applications, pp. 741-748, Jan. 2006.

[17] N. Park and H. Bang, "Mobile middleware platform for secure vessel traffic system in IoT service environment", International Journal of Security And Communication Networks, Vol. 9, No. 6, pp. 500-512, Apr. 2016.

[18] D. Lee, N. Park, Geonwoo Kim, and Seunghun Jin, "De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment", International Journal of Peer-to-Peer Networking and Applications, Vol. 11, No. 6, pp. 1299-1308, Nov. 2018.

[19] D. Lee and N. Park, "A Proposal of SH-Tree Based Data Synchronization Method for Secure Maritime Cloud", Journal of KIISC, Vol. 26, No. 4, pp. 929-940, Aug. 2016.

[20] N. Park, "Analysis of privacy weakness and protective countermeasures in smart grid environment", Journal of KIIT, Vol. 8, No. 9, pp. 189-197, Sep. 2010

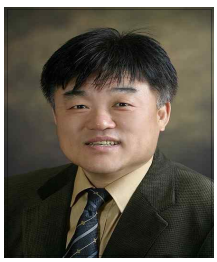
[21] N. Park, B. G. Kim, and J. Kim, "A Mechanism of Masking Identification Information regarding Moving Objects Recorded on Visual Surveillance Systems by Differentially Implementing Access Permission", Journal of Electronics, Vol. 8, No 7, Jun. 2019. https://doi.org/10.3390/electronics8070735

저자소개

김 진 수 (Jinsu Kim)

2017년 2월 : 강원대학교 정보통신공학전공 학사
2017년 3월 ~ 현재 : 강원대학교 전자정보통신공학전공 석사과정
2018년 9월 ~ 현재 : 제주대학교 사이버보안인재교육원 연구원
관심분야 : 클라우드, 지능형 영상감시 시스템, IoT 등

김 상 춘 (Sangchoon Kim)



1999년 8월 : 충북대학교 전자계산학과 박사
1983년 4월 ~ 2001년 3월 : 한국전자통신연구원 선임기술원
2001년 7월 ~ 2010년 6월 : 한국전자통신연구원 초빙연구원
2001년 4월 ~ 현재 : 강원대학교 공학대학 전자정보통신공학부 교수,
관심분야 : IoT 보안, 개인정보보호 관리 및 정책, 융합보안, 금융보안, 네트워크 보안 등

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과 박사
2003년 4월 ~ 2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월 ~ 2009년 12월 : 미국 UCLA대학교 공과대학 Post-Doc, WINMEC 연구센터 Staff Researcher
2010년 1월 ~ 2010년 8월 : 미국 아리조나 주립대학교 컴퓨터공학과 연구원
2010년 9월 ~ 현재 : 제주대학교 교육대학 초등컴퓨터교육전공, 융합정보보안학과 교수
2011년 9월 ~ 현재 : 과학기술사회(STS)연구센터장, 정보영재 주임교수, 초등교육연구소장
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등