Journal of KIIT. Vol. 17, No. 6, pp. 115-122, Jun 30, 2019. pISSN 1598-8619, eISSN 2093-7571 115
http://dx.doi.org/10.14801/jkiit.2019.17.6.115

프라이버시 침해 방지를 위한 얼굴 정보 변환 메커니즘

김진수*, 김상춘**, 박남제***

Face Information Conversion Mechanism to Prevent Privacy Infringement

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

이 논문은 2019년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호:NRF-2019R1I1A3A01062789). 그리고, 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임. [2019-0-00203,선제적 위험대응을 위한 예측적 영상보안 핵심기술 개발]

요 약

CCTV(Closed-circuit Television)는 사고 예방 및 시설 안전을 위해 매년 설치대수가 증가함에 따라 1인당 CCTV에 노출되는 횟수가 증대되고 있으며, 노출되는 대상의 프라이버시 보호를 위해 지능형 영상감시 시스템 기술이 각광받고 있다. 지능형 영상감시 시스템은 촬영된 영상 데이터에 대한 단순한 식별에서 피사체의 행동 유형과 현장 상황 판단 등을 수행하거나, 촬영된 피사체의 정보가 노출될 수 있는 정보를 외부로 유출되지 않도록 프라이버시 보호를 위한 처리 과정을 진행한다. 제안된 기술은 영상감시 시스템에 적용되어 영상감시 시스템으로부터 촬영된 원본 영상 정보를 유사 영상 정보로 변환함으로서 외부에 원본 영상 정보가 유출되지 않도록 하는 기술이다. 본문에서는 미리 설정된 유사도에 근접하는 가상의 얼굴 이미지를 삽입하는 영상 변환 메커니즘을 제안한다.

Abstract

CCTV(Closed-Circuit Television) is increasingly exposed to CCTV per person as the number of installations increases every year for accident prevention and facility safety. The intelligent video surveillance system technology is attracting attention to the privacy protection of exposed subjects. The intelligent video surveillance system performs a process for the privacy protection so as to perform the action type of the subject and the judgment of the situation in the simple identification of the photographed image data, or to prevent the information, from which the information of the photographed subject is exposed. The proposed technique is applied to the video surveillance system and converts the original image information taken from the video surveillance system into similar image information so that the original image information is not leaked to the outside. In this paper, we propose an image conversion mechanism that inserts a virtual face image that approximates a preset similarity.

Keywords
closed circuit television(CCTV), intelligent video surveillance system, privacy, virtualization, virtual face image

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

· Received: Feb. 14, 2019, Revised: Apr. 30, 2019, Accepted: May 3, 2019.
· Corresponding Author: Sangchoon Kim, 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

공공장소의 사건사고를 예방을 위해 설치되는 영상감시 시스템은 매년 증가하고 있으며, 영상감시 시스템이 증대됨에 따라 촬영되는 피사체의 프라이버시에 대한 논란이 확대되고 있다[1]. 이에 따라 개인의 정보 유출을 방지하기 위한 기술을 접목시킨 지능형 영상감시 시스템의 관심도가 증대되고 있다[2]. 지능형 영상감시 시스템은 해당 장소의 상황을 판단하기 위해서 촬영지역 내의 인물을 촬영하고, 해당 인물의 얼굴을 검출하여 판단의 근거로 사용한다[3].

하지만, 인물의 얼굴을 검출하여 사용하게 될 경우 영상에 촬영된 피사체는 촬영된 원본 데이터에 본인의 개인정보가 노출될 수 있다[4]. 지능형 영상감시 시스템은 촬영된 피사체의 프라이버시를 보호하기 위해 비식별 처리를 진행하게 된다[5][6]. 하지만 비식별 처리된 영상 정보는 통계를 내거나 영상을 복원하는데 어려움을 가진다[7].

본문에서는 미리 설정된 유사도에 따라 가상의 얼굴 영상을 생성하고, 영상 정보 내에 삽입하는 메커니즘을 제안함으로서 위의 문제를 해결하고자 한다. 2장에서는 영상 비식별화와 관련된 연구 현황을 분석하고, 3장에서 제안된 얼굴 영상 변환 메커니즘을 소개하고, 4장에서 상용화되었거나, 선행 기술과 현 시스템의 차이점을 소개하도록 한다.

Ⅱ. 기존 영상 프라이버시 보호 기법 분석

지능형 영상감시 시스템은 사용자의 프라이버시 보호를 위해 다양한 기법을 적용하게 된다[8]. 다음은 일반적으로 지능형 영상감시 시스템에서 사용되는 프라이버시 보호 기법을 서술한 것이다[9][10].

2.1 블러링(Blurring)

블러링 기법은 영상 데이터에 가중치가 존재하는 마스크를 이용하여 영상 데이터내의 픽셀 값과 가중치를 곱함으로서 일정 영역을 흐리게하는 기법이다. 일반적으로 블러링은 가우시안 함수를 이용해 시그마 값을 설정하여 처리하며, 이와 같이 처리된 영상 데이터는 원본데이터로의 복원이 불가능하다[11].

2.2 모자이크(Mosaic)

모자이크 기법은 영상 데이터의 일정 구간내의 픽셀 값을 합하여 평균을 낸 값을 구간 내에 동일한 값으로 입력함으로서 해당 구역의 원본 정보를 제 3자가 구별할 수 없도록 하는 기법이다. 모자이크 기법은 해당 구간에 대한 평균값을 구간 전체에 적용하므로 영상의 복원이 어렵다[12].

2.3 제거 및 변형(Removal and transformation)

제거 및 변형 기법은 영상 데이터 내의 피사체의 개인정보에 대해 해당 픽셀을 완전히 제거하거나 변형시킴으로서 원본 데이터를 고의적으로 훼손하는 방법이다.

2.4 암호화(Encryption)

암호화 기법은 영상 데이터에 대해 암호화키를 적용함으로서 이미지의 내의 영상 데이터를 암호문으로 변경하는 것이다. 이 경우 암호문에 대한 복호화키를 가진 정당한 사용자는 손쉽게 원본 정보를 습득할 수 있다. 고로 허가되지 않은 제 3자에 의한 복호화 방지 기술이 추가적으로 요구된다[13][14].

Ⅲ. 제안된 프라이버시 침해 방지를 위한 얼굴 정보 변환 메커니즘

본문에 제안된 메커니즘은 촬영된 영상정보에 존재하는 얼굴 영상을 기존의 DB에 저장되어있는 가상의 얼굴 영상으로 치환하는 방식으로 이 과정을 가상화 방식으로 명하고, DB에 저장된 가상의 얼굴 정보를 가상 얼굴 정보로 축약하여 사용하도록 한다[15]. 제안된 메커니즘은 촬영된 영상 데이터에 존재하는 얼굴 정보를 검출하고, 가상화 난수를 이용하여 가상의 얼굴 정보를 생성한 뒤, 영상 데이터 내의 얼굴 정보를 유사도에 대응하는 가상의 얼굴 영상 정보로 치환시켜 성별, 나이, 인종 등의 공공

정보만을 식별할 수 있도록 한다. 이후 적법한 사용자에 의해 가상 얼굴 영상 데이터는 원본 데이터로 복원될 수 있다. 제안된 메커니즘은 얼굴 영역 검출부, 가상 얼굴 특징값 생성부, 가상 얼굴 특징 벡터 생성부, 가상 얼굴 영상 데이터 생성부, 얼굴 특징값 복원부, 복원 얼굴 특징 벡터 생성부, 얼굴 영상 데이터 복원부로 이뤄진다[16].

3.1 얼굴 영역 검출부

얼굴 영역 검출부는 하나 이상의 카메라에 촬영된 영상 데이터에 존재하는 얼굴 영역을 검출하고, 하나 이상의 영상 데이터가 촬영된 순서에 대응하여 하나 이상의 영상 데이터마다 촬영된 카메라에 따른 촬영 회차를 할당한다[17]. 영상 데이터 내에 얼굴 영역이 검출되지 않는 경우 촬영 회차를 할당하지 않을 수 있다[18][19].

3.2 가상 얼굴 특징값 생성부

가상 얼굴 특징값 생성부는 얼굴 영역 검출부의 촬영 회차에 대응하는 발생 차수만큼 하나 이상의 영상 데이터마다 가상화 난수를 생성하고, 생성된 가상화 난수를 이용해 얼굴 영역에서 추출된 얼굴의 개인을 식별 가능한 특징 좌표를 나타내는 얼굴 특징값을 가상화 난수에 의한 노이즈값을 가산하여 가상 얼굴 특징값으로 변환하며, 난수 발생 함수의 초기값은 미리 설정된 시드값을 이용한다[20].

$$P(i)S \tag{1}$$

식 (1)은 가상 얼굴을 생성하기 위한 가상화 난수 발생 함수의 수학식이다. P는 난수 발생함수, I는 난수 발생 함수의 발행 회차, S는 미리 설정된 시드값을 의미한다. 위 식을 이용하여 발생 회차에 따른 가상화 난수를 생성한 경우, 미리 설정된 시드값과 가상화 난수 생성 범위가 동일한 난수 발생 함수를 이용하여 발생 회차에 걸쳐 생성함으로서 동일한 가상화 난수를 구할 수 있다.

구해진 가상화 난수는 미리 설정된 가상화 난수 생성 범위의 중간값 간의 차이값을 미리 설정된 유사도값에 가산하여 노이즈값을 생성하는데 사용된다[21].

$$N(i) = (100\% - T) + \left(P(i)S - \frac{R1r}{2}\right) \tag{2}$$

식 (2)는 가상 얼굴 특징값 생성을 위한 노이즈값이다. $N(i)$는 가상 얼굴을 생성하기 위한 노이즈이며, T는 미리 설정된 유사도값이다. $P(i)S$는 가상화 난수를 의미하며, $R1r$은 미리 설정된 가상화 난수 생성 범위를 의미한다[22].

$$T = 50\%, R1r = 50 \tag{3}$$

$$P(1)S = 15, P(2)S = 40, P(3)S = 25 \tag{4}$$

생성 범위에 대한 예시로 식 (3)과 같이 유사도값이 50%이고, 가상화 난수 생성 범위가 50일 경우 3회의 촬영 회차에 따른 노이즈 연산을 진행하면, 식 (1)에 의해 50 이내의 가상화 난수값이 3차례 생성된다. 본문에서는 식 (4)와 같이 임의로 15, 40, 25로 설정한다.

$$N(1) = (100\% - 50\%) + \left(15 - \frac{50}{2}\right) = 40 \tag{5}$$

$$N(2) = (100\% - 50\%) + \left(40 - \frac{50}{2}\right) = 65 \tag{6}$$

$$N(3) = (100\% - 50\%) + \left(25 - \frac{50}{2}\right) = 50 \tag{7}$$

식 (5)부터 식 (7)은 촬영 회차에 따른 노이즈 연산 과정을 보였다. 이와 같이 미리 설정된 유사도값에 노이즈값은 서로 반비례하며, 유사도값을 높일수록 보다 원본에 근접하며, 반대로 유사도값을 낮출수록 원본과 상이한 결과를 나타낸다[23].

3.3 가상 얼굴 특징 벡터 생성부

가상 얼굴 특징 벡터 생성부에서는 가로와 세로의 2차원 행렬로 구성된 좌표값인 가상 얼굴 특징값으로부터 가상 얼굴 특징 벡터를 추출한다.

3.4 가상 얼굴 영상 데이터 생성부

가상 얼굴 영상 데이터 생성부는 가상 얼굴 특징값 생성부에서 변환된 가상 얼굴 특징값이 벡터화된 가상 얼굴 특징 벡터에 기초하여 얼굴 정보 데이터베이스에서 공분산 행렬을 이용하여 벡터간 유사도를 분석하는 주성분 분석법(PCA, Principal Component Analusis), 클래스 사이(between-class) 분포와 클래스 내(Within-class) 분포의 비율을 최대화하는 선형 판별 분석법(LDA, Linear Disciminant Analysis) 등을 통해 가상 얼굴 정보를 검색하고, 영상 데이터의 얼굴 영역에 치환할 검색된 가상 얼굴 정보를 삽입하여 가상 얼굴 영상 데이터를 생성한다. 삽입된 가상 얼굴 정보는 원본 얼굴 정보와 동일한 유사도를 가지는 경우에도 촬영 회차마다 상이한 가상 얼굴 정보가 삽입될 수 있다[24].

3.5 얼굴 특징값 복원부

얼굴 특징값 복원부는 미리 설정된 유사도값에 복원 난수의 편차를 가산하여 가상 얼굴 특징값을 생성하는데 사용된 노이즈값을 역산하고, 가상 얼굴 특징값에 역산된 노이즈값을 감산하여 얼굴 특징값으로 복원된 복원 얼굴 특징값을 생성한다. 이때, 복원 난수 발생 함수의 초기값은 미리 설정된 시드값을 이용한다.

$$P'(i)S \tag{8}$$

식 (8)은 가상 얼굴을 복원하기 위한 복원 난수 발생 함수의 수학식이다. P는 난수 발생함수, I는 난수 발생 함수의 발행 회차, S는 미리 설정된 시드값을 의미한다. 위 식은 가상 영상 데이터를 생성하는 과정에서 사용된 유사도값에 복원 난수의 편차를 가산함으로서 노이즈값을 계산하고, 가상 얼굴 특징값에 노이즈값을 가산함으로서 복원 얼굴 특징값을 생성할 수 있다.

$$N'(i) = (100\% - T) + (P'(i)S - \frac{R1r}{2}) \tag{9}$$

식 (9)는 가상 얼굴 정보를 역산하기 위한 노이즈 수학식이다. N'(i)는 가상 얼굴을 복원하기 위한 노이즈이며, T는 미리 설정된 유사도값이다. P'(i)S는 복원 난수를 의미하며, R1r은 미리 설정된 가상화 난수 생성 범위를 의미한다.

3.6 복원 얼굴 특징 벡터 생성부

복원 얼굴 특징 벡터 생성부는 얼굴 특징값 복원부로부터 생성된 복원 얼굴 특징값을 벡터화하여 복원 얼굴 특징 벡터로 생성한다.

3.7 얼굴 영상 데이터 복원부

복원 얼굴 특징값이 벡터화된 복원 얼굴 특징 벡터에 기초하여 얼굴 정보 데이터베이스에서 복원 얼굴 정보를 검색하고, 가상 얼굴 영상 데이터의 얼굴 영역에 검색된 복원 얼굴 정보를 삽입하여 영상 데이터로 복원된 복원 영상 데이터를 생성한다. 영상 복원을 위해 필요한 정보는 적법한 관리자에게만 제공되며, 허가되지 않은 제 3자에 의한 복원을 방지한다.

Ⅳ. 제안된 메커니즘과 기존 기법의 비교 분석

제안된 메커니즘은 입력된 영상 데이터에 존재하는 하나 이상의 얼굴 정보를 검출하여 가상 얼굴 정보로 치환함으로서 영상에 촬영된 대상을 특정할 수 없도록 하는 메커니즘이다. 촬영된 피사체의 얼굴 정보는 얼굴 정보 데이터베이스에 저장되며, 이후 적법한 사용자의 요청이 있을 경우 가상 얼굴 정보로 치환된 영상정보를 원본 데이터로 복원함으로서 사용자에게 제공될 수 있다. 본문에서 제안된 기술은 얼굴 영상 변환 메커니즘과 기존의 블러링, 모자이크, 영상 정보 제거 및 변형, 암호화 기법의 4개의 기법과의 차이는 다음과 같다.

블러링 기법은 영상 데이터의 픽셀을 가중치와 연산함으로서 영상 정보를 흐릿하게 만드는 기법으로 디블러링을 통한 복원이 가능하나 대상의 공공정보의 식별 또한 불가능하다[25].

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

Comparison item	Blurring	Mosaic	Removal and transformation	Encryption	The proposed mechanism
De-Identification	O	O	O	O	O
Unable to restore an image by the illegal user	X	X	O	X	O
Image Restoration by Legitimate Users	O	X	X	O	O
Identification of de-identified public information	X	X	X	X	O

(A) Original (B) Encryption (C) Restored

그림 1. 제안된 메커니즘 비교 영상
Fig. 1. Proposed mechanism comparison image

다음으로 모자이크 기법은 영상 데이터 내의 비식별화가 요구되는 얼굴 정보에 대해 일정 구역 내의 픽셀값을 합산하고, 평균치를 구역 내의 모든 픽셀에 동일한 값을 적용하는 것으로 대상을 식별할 수 없도록 한다. 이 경우에도 대상의 공공 정보 식별은 불가하지만 최근 구글에서 발표된 내용에 따르면 AI(Artificial Intelligence)를 이용하여 원본과 유사한 이미지를 유추해내어 복원하는 기술을 제작하였다[26].

제거 및 변경 기법은 영상 데이터 내에 존재하는 얼굴 영역에 대한 픽셀값을 제거하거나 변경함으로서 해당 정보를 식별할 수 없도록 하는 방식으로 영상 데이터가 왜곡됨에 따라 대상의 공공 정보 식별이 불가능해지며, 영상 정보 내의 데이터를 삭제하므로 복원 또한 어렵다[27].

마지막으로 암호화 기법은 영상 데이터를 암호화 키를 이용하여 암호문으로 변경한 후 적법한 사용자에 의해서만 영상 데이터를 복호화하여 원본 데이터를 제공하는 기법이다. 암호화 방식에 따라 원본 정보의 형태는 유지하되, 식별이 불가능하게 하는 방식부터 영상 데이터의 단위를 조정하여 영상 데이터에 대한 식별 자체를 불가능하게 하는 방식이 존재한다. 이와 같은 암호화 기법은 복원할 경우 공공 정보를 식별할 수 있고, 복원 또한 복호화키를 가진 적법한 사용자만이 사용할 수 있다[28].

본문에서 제안된 메커니즘은 영상 데이터 내의 얼굴 정보를 가상 얼굴로 치환하는 것으로 영상 데이터의 식별이 가능하며, 피사체의 기본적인 공공 정보를 구분할 수 있다. 또한 적법한 사용자의 경우 가상 얼굴 영상 데이터를 복원하여 원본 데이터로 복원할 수 있다. 피사체의 얼굴 정보는 얼굴 정보 데이터베이스에 기록되어 얼굴 정보 데이터베이스와 가상 얼굴 영상 데이터가 유출된 경우에도 가상 얼굴 영상 데이터로 변환된 정보에서 원본 정보의 얼굴 정보를 찾아내기 힘들다는 보안상 장점을 가진다.

V. 결 론

영상감시 시스템의 증가에 따라 1인당 촬영 노출 횟수가 증가되며 기술의 발전에 따라 영상감시 시스템은 특징적인 사람이나 사물에 대한 인식이나 움직이는 피사체의 행위를 인식하며, 분산된 기기간의 정보 공유를 통해 상황을 이해하는 수준에 이르렀다. 이로 인해 영상감시 시스템을 통한 관제는 수월해 졌으나, 영상감시 시스템에 노출되는 피사체는 사생활 침해에 대한 우려가 증대되고 있다.

본문에서는 기존 영상 프라이버시 보호 기법과 제안된 메커니즘과의 차이를 분석하고, 기존 영상 프라이버시 보호 기법이 가지는 문제점을 보완할 수 있는 메커니즘을 제안하였다. 본문의 메커니즘은 촬영된 영상 정보에 존재하는 얼굴 영역을 검출하고, 검출된 얼굴 영역의 특징 벡터를 찾아 이와 유사한 가상 얼굴로 치환하는 것을 특징으로 한다. 치환된 영상 정보의 식별 정보는 유사도 설정에 따라 변경할 수 있다.

영상감시 시스템 시장은 매년 증가하는 추세이며, 영상감시 관제소가 확대되고 있다. 하지만 프라이버시 보호 기술이 적용되지 않고 적용된 경우에도 기법에 따라 원본 데이터를 유추할 수 없거나, 암호화키 노출에 의해 원본 데이터가 유출될 수 있다. 이후 영상 유출에 의한 사생활 침해는 큰 이슈가 될 수 있으며, 이를 예방하기 위한 방법이 연구되어야 한다.

References

[1] Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, and Howon Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment", Advanced Web and Network Technologies, and Applications, pp. 741-748, Jan. 2006.

[2] Donghyeok Lee and Namje Park, "Institutional Impro vements for Security of IoT Devices", Journal of KIISC, Vol. 27, No. 3, pp. 607-615, Jun. 2017.

[3] Donghyeok Lee and Namje Park, "Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment", Personal and Ubiquitous Computing, Vol. 22, No. 1, pp. 3-10, Feb. 2018.

[4] Namje Park, Hongxin Hu, and Qun Jin, "Security and Privacy Mechanisms for Sensor Middleware and Application in Internet of Things (IoT)", Journal of Distributed Sensor Networks, Vol. 2016, No. 1, pp. 1-3, Jan. 2016.

[5] Donghyeok Lee and Namje Park, "A Study on Metering Data De-identification Method for Smart Grid Privacy Protection", Journal of KIISC, Vol. 26, No. 6, pp. 1593-1603, Dec. 2016.

[6] Donghyeok Lee and Namje Park, "Legislative Reform of Smart Grid Privacy Act", Journal of KIISC, Vol. 26, No. 2, pp. 415-423, Apr. 2016.

[7] Donghyeok Lee and Namje Park, "Smart Grid Privacy Protection Measures According to the Change of IT Paradigm", Journal of MSCAH, Vol. 6, No. 3, pp. 81-90, Mar. 2016.

[8] Donghyeok Lee and Namje Park, "A Study on COP-Transformation Based Metadata Security Scheme for Privacy Protection in Intelligent Video Surveillance", Journal of KIISC, Vol. 28, No. 2, pp. 417-428, Apr. 2018.

[9] Namje Park, "Privacy-Enhanced Deduplication Technique in Closed Circuit Television Video Cloud Service Environment", Journal of KINGC, pp. 65-66, May 2018.

[10] Donghyeok Lee and Namje Park, "Privacy Enhanced CCTV Video Security Framework using Metadata De-identification", Journal of ICICT, pp. 199-200, 2018.

[11] Hyungil Kim, "A Data Blurring Method for Dollaborative Filtering", Department of Computer Engineering, The Graduate School of Dongguk University.

[12] Seokjin Hong, Seokho Lee, and Jinwook Bae, "Efficient Execution of Range Mosaic Queries", Journal of KIISE, Vol. 32, No. 5, pp. 487-497, Oct. 2005.

[13] Byounghyun Jeon, Sangho Shin, Kihyun Jung, Joonho Lee, and Keeyoung Yoo, "Reversible Secret Sharing Scheme Using Symmetric Key Encryption Algorithm in Encrypted Image", Journal of KMS, Vol. 18, No. 11, pp. 1332-1341, Nov. 2015.

[14] Shouqiang Liu, MengjingYu, Miao Li, and Qingzhen Xu, "The research of virtual face based on Deep Convolutional Generative Adversarial Networks using TensorFlow", Journal of Physica A:SMA, Vol. 521, pp. 667-680, May 2019.

[15] Jinsu Kim, Namje Park, Geonwoo Kim, and Seunghun Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia", Journal of Electronics, Vol. 8, No 4, Apr. 2019. doi:10.3390/electronics8040412.

[16] Donghyeok Lee, Namje Park, Geonwoo Kim, and

Seunghun Jin, "De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment", Journal of Peer-to-Peer Networking and Applications, Vol. 11, No. 6, pp. 1299-1308, Nov. 2018.

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

[18] Namje Park and Namhi Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle", Journal of Sensors (Basel), Vol. 16, No. 1, pp. 1-16, Dec. 2015.

[19] Donghyeok Lee and Namje Park, "ROI-based efficient video data processing for large-scale cloud storage in intelligent CCTV environment", Journal of IJET, Vol. 7, No. 2.33, pp. 151-154, Mar. 2018.

[20] Donghyeok Lee and Namje Park, "Differential Level CCTV Video Access Control based on RFID", Conference of ICCT, pp. 224-225, Jul. 2018.

[21] Namje Park and Hyochan Bang, "Mobile middleware platform for secure vessel traffic system in IoT service environment", Journal of Security and Communication Networks, Vol. 9, No. 6, pp. 500-512, Nov. 2014.

[22] Donghyeok Lee and Namje Park, "CCTV Privacy Protection Method using Similarity based Virtual Face", Conference of ICCT, pp. 267-268, Jul. 2018.

[23] Donghyeok Lee and Namje Park, "Multi-Object Recognition Access Control based on CCTV Video Learning", Conference of KCC 2018, Jun. 2018.

[24] Donghyeok Lee and Namje Park, "Similarity-based Virtual Facial Generation Method for Privacy Protection of Intelligent CCTV Environment", Journal of CISC 2017, Jun. 2017.

[25] Minso Jeong and Jechang Jeong, "Uniform Motion Deblurring using Shock Filter and Convolutional Neural Network", Journal of KSBE, Vol. 23, No. 4, pp. 484-494, Jul. 2018.

[26] Ryan Dahl, Mohammad Norouzi, and Jonathon Shlens, "Pixel Recursive Super Resolution", Journal of ICCV, Mar. 2017.

[27] Dongeun Leeoung and Kyu Choi, "Background Subtraction Algorithm Based on Multiple Interval Pixel Sampling", Journal of KIPS, Vol. 2, No. 1, pp. 27-34, Jan. 2013.

[28] Namjin Kim, Donghwan Seo, Sunggeun Lee, Changmok Shin, Kyubo Cho, and Soojoong Kim, "Hierarchical image encryption with orthogonality", Journal of KJOP, Vol. 17, No. 3, pp. 231-239, Jun. 2006.

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