The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 2, pp.31-37, Apr. 30, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.2.31
JIIBC 2015-2-5

IoT에서 스테가노그라피와 QR 코드를 이용한 영상 정보의 보안

Security of Image Information using Steganography and QR Code in IoT

임용순*, 강은영**, 박재표***

Yong-Soon Im*, Eun-Young Kang, Jae-Pyo Park*****

요 약 사물인터넷(IoT)의 여러 분야에서 영상 정보의 보안은 매우 중요하며, 그 보안(저작권 등)을 표시하는 여러 방안을 연구하고 있다. 본 논문에서는 IoT에서 사용하는 영상 정보는 이산 코사인 변환(DCT)과 양자화를 통하여 계수 값(QC)으로 변환된다. 그리고 워터마크(메시지)는 QR Code를 통하여 새로운 부호화된 메시지(WMQR)를 만든다. QC와 WMQR은 스테가노그래피 LSB 기법을 적용하고, 영상정보의 보안(저작권 등)을 얻을 수 있다. 스테가노그래피의 LSB 기법은 위치(Secret Key)의 결정에 따라 메시지를 삽입할 수 있다. 부호화된 영상은 인터넷을 통하여 수신자에게 전송하게 된다. 역 과정에서는 영상과 QR 코드, 워터마크(Message)를 얻을 수 있다. 영상정보의 보안에서 워터마크를 추출하는 방법은 부호화된 영상과 Secret Key 만을 사용하며, DCT와 양자화 과정을 통하여 워터마크(Message)를 분리하여 얻을수 있다. 본 논문에서 우리는 영상정보의 보안의 방법을 개선할수 있었으며, 이 모의실험을 통하여 영상의 화질(PSNR), 정규화 상관도(NC)를 통하여 높은 보안성을 얻을 수 있었다.

Abstract The security of the image information is very important in many areas of the IoT(Internet of Things), and study a number of ways to display the security (copyright, etc.). In this paper, information of image that is used by the IoT is converted to a DCT(Discrete Cosine Transform) and QC(Quantization Coefficient). And watermark (message) is to create a new encoded message(WMQR) through a QR Code. QC and WMQR applies LSB steganography techniques, can get the security (copyright, etc.) of image information. LSB steganographic techniques may be inserted according to a message (Watermark) to determine the location (Secret Key). The encoded image is sent to the recipient via the Internet. The reverse process can be obtained image and a QR code, a watermark (Message). A method for extracting a watermark from the security of the image information is coded using only the image and Secret Key, through the DCT and quantization process, so obtained by separating the watermark (Message) for the image. In this paper, we were able to improve the security of the method of image information, the image quality of the image by the simulations (PSNR), in turn, benefits were also normalized correlation (NC) and security.

Key Words : IoT(Internet of Things), Watermarking, QR code, Copyright, Information security, Steganography

*종신회원, 국제대학교 IT계열
**정회원, 동양미래대학교 컴퓨터소프트웨어공학과(교신저자)
***정회원, 숭실대학교 정보과학대학원 정보보안학과
접수일자 : 2015년 2월 23일, 수정완료 : 2015년 3월 16일
게재확정일자 : 2015년 4월 10일

Received: 23 February, 2015 / Revised: 16 March, 2015
Accepted: 10 April, 2015
**Corressponding Author : eykang@dongyang.ac.kr
Dept. of Computer Software Engineering, Dongyang Mirae University, Korea

Ⅰ. 서 론

정보보안과 컴퓨터, 가전제품, 산업장비들은 우리 생활에 아주 밀접한 관계를 가지게 되었으며, 최근 사물인터넷(IoT, Internet of Things)으로도 널리 알리게 되었다.

사물인터넷을 실현하는데 필요한 요소는 센서와 디바이스, 네트워크, 플랫폼, 웹앱, 데이터 분석과 예측, 빅데이터 처리, 보안과 프라이버시 보호 기술, 영상정보의 보안 등 다양한 기술을 들 수 있다. 이러한 기술들은 사물인터넷에서 각각 기능을 제공하며, 여러 기술이 통합되어 새로운 기능을 제공하기도 한다.

여러 기술들이 통합됨에 따라 각각의 기능에서 보안 기술에 대한 문제가 발생할 수 있다. 사물인터넷을 구성하는 개별 기술이 기본적인 보안 기능(기밀성과 무결성, 인증/인가)을 제공하더라도 해당 보안 기술은 서로 연결되지 못하거나, 연동시 새로운 보안 취약성이 발생할 수 있었다. 이와 같이 사물인터넷에서는 근본적으로 영상의 보안/프라이버시를 보호하는데 어려움이 있었다.

사물인터넷[7]에서 개인정보의 하나인 영상정보(Image Information)는 모바일 영상, 영상 통신 등의 여러 기술이 발달하게 되어 밀접한 정보들이 서로 공유하고 있다. 영상 정보에 따른 정보량의 증가, 정보의 구분이 불분명해질 수 있다는 점, 정보의 보안으로 저작권 침해 및 불법 복제라는 문제점이 발생되었다.

영상 정보의 보안을 위해 암호화 방법, 방화벽을 구축하는 방법과 영상 정보의 소유권을 보호하기 위한 디지털 워터마크(digital watermark), 스테가노그라피 기법을 들 수 있다. 그중 디지털 워터마크 기법 분야와 스테가노그라피 기법에서 많은 연구가 필요하게 되었다.

본 논문의 구성은 5개의 장으로 구성되었다. Ⅱ장에서는 워터마킹 기법과 영상에서 QR 코드, 스테가노그라피 기법에 대하여 기술하였다. Ⅲ장에서는 제안된 QR 코드, 워터마킹와 스테가노그라피를 이용한 디지털 영상 부호화에 대하여 설명하였다. Ⅳ장에서는 모의실험 결과의 특성을 보여준다. 끝으로 Ⅴ장에서는 결론을 맺는다.

Ⅱ. 영상정보의 보안 기법

1. 영상정보에서 본 워터마킹 기법

워터마킹 기법은 사용자의 ID (Identification)나 자신만의 영상정보를 넣음으로써 불법적인 복제를 막고 데이터 소유자의 저작권과 소유권을 효율적으로 보호하기 위한 방법이다.[1][2][3][4]

영상정보에 삽입한 워터마크가 보이지 않아야 하고, 일반적인 컨텐츠 변형으로써 압축, 저역통과필터, 확대, 축소, 회전등을 가해도 워터마크의 특징은 살아있어야 한다. 저작권 보호에 워터마크가 효율적으로 이용되기 위해서는 비가시성(invisibility), 강인성(robustness), 명확성(unambiguity)등의 특성을 갖추어야 한다. 비가시성이란 삽입 후에도 원본의 변화가 거의 없어, 워터마크의 삽입여부를 감지하지 못하는 것을 말한다. 강인성은 워터마크를 신호의 중요한 부분에 삽입하여 여러 가지 형태의 변형이나 공격에도 추출이 가능한 것을 말하며, 명확성은 추출된 워터마크가 확실한 소유권을 주장할 수 있도록 정확성을 유지하는 것이다.

영상정보의 워터마킹은 크게 두 가지인 공간영역(spatial domain)과 주파수 영역(frequency domain)에서 워터마크를 삽입한다. 공간영역에서의 워터마킹은 간단한 알고리즘으로 인하여 빠른 수행 시간을 갖는 장점이 있지만, 일반적으로 주파수영역에서의 워터마킹에 비하여 잡음 및 필터링이나 손실 부호화 등에 약하다는 단점이 있다.

주파수영역에서는 공간영역의 취약점을 보완하기 위하여 FFT(Fast Fourier Transform), DCT(Discrete Cosine Transform), DWT(Discrete Wavelet Transform) 등의 기법을 들 수 있다. 영상정보의 변환을 통하여 중간대역의 주파수 성분 값에 워터마크를 삽입하는 방법이다. Koch는 영상 분할과 DCT한 후 저주파 성분에 삽입한 방법을 제시하였다. Swanson은 Legge와 Foleg의 콘트라스트 마스킹 모델을 이용하여 DCT값을 구한후 워터마킹하는 방법을 제시하였다. Kundur, Xia와 Hus등은 DCT대신 Multiresolution을 이용한 DWT로 워터마킹하는 방법을 제시하였다. 그리고 Cox와 Barni 등은 주파수 영역에서 오디오, 비디오, 멀티미디어 등의 데이터에 중요한 계수를 추출해 워터마크를 삽입하는 방법을 제시하였다. Ruanaidh등은 DFT (Discrete Fourier Transform)를 이용하여 위상에 워터마크를 삽입하는 방법 등을 제안하였다.

주파수영역에서의 워터마킹은 FFT, DCT, DWT등으로 변환을 한 다음 주파수 영역의 계수에 워터마크를 삽입하는 과정과 역 변환을 하게 되어 워터마크를 추출하

는 과정을 의미한다. 주파수 영역의 방법은 공간영역의 방법보다 공격에 강하다는 특징을 가지고 있다. 또한 주파수영역의 저주파 영역에서는 계수의 변화에 민감한 영향을 받으며 고주파 영역에서는 계수의 변화에 둔감한 영향을 받는 의미를 가지므로 일반적으로 저주파 영역에 워터마크를 삽입을 하는 방법을 많이 사용한다.

$$F(u,v)=\frac{2}{N}C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\frac{(2x+1)u\pi}{2N}\cos\frac{(2y+1)v\pi}{2N} \quad (1)$$

$$f(x,y)=\frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}C(u)C(v)F(u,v)\cos\frac{(2x+1)u\pi}{2N}\cos\frac{(2y+1)v\pi}{2N} \quad (2)$$

워터마크의 삽입을 위해 DCT를 수행하여 원 영상과 워터마크를 주파수영역으로 변환하였으며 DCT식은 식 (1)과 같다. 또한 IDCT 수행으로 주파수 대역별 워터마킹 영상을 얻는다. IDCT 식은 (2)와 같다.

2. 영상정보에서 본 QR 코드 기법

1차원 바코드는 다수의 수직선으로 구성되어 있으며 수직선의 굵기와 간격을 이용하여 데이터를 표현하기 때문에 1차원 바코드라고 부르며, 표준화된 1차원 바코드(ISO/IEC 15417)와 바코드 검증기(ISO/IEC 15426-1)가 있다. 다음 그림 1은 “barcode”의 문구를 바코드화한 결과이다.

바코드는 인식 속도와 정확성, 단순한 조작성 등의 특징으로 널리 보급되었다. 정보량을 높이기 위하여 바코드의 자릿수를 늘리거나 여러 바코드를 나열한 대안책도 있었다. 그러나 대안책은 표시 면적을 크게 하거나, 독해 작업의 복잡성 증가, 장비의 변경으로 비용이 상승될 수 있다.

그림 1. 1차원 바코드
Fig. 1. 1-D Bar Code

이러한 해결 방안으로 2차원 코드가 출현했다. 2차원 코드도 바코드를 적층/중복한 타입(stack barcode방식)에서 보다 정보밀도를 높인 Matrix방식으로 진화하고 있다. QR(Quick Response) 코드[5][6]는 1994년 일본의 덴소사에 의해 개발된 2차원 바코드이다. 기존 1차원 바코드의 정보량 제한을 해결하기 위해 2차원으로 확장함으로써 저장할 수 있는 정보량은 증가되었고, 물리적으로 차지하는 공간은 최소로 줄일수 있는 장점이 있다.

표 1. QR 코드의 데이터 용량
Table 1. Data capacity of QR code

데이터 종류	용량(최대)
숫자	7,089 문자
숫자 + 알파벳	4,296 문자
바이너리(8비트)	2,953 바이트
한자	1,817 문자

QR 코드는 1차원 바코드보다 많은 데이터를 기록할 수 있고, QR 코드의 데이터 용량은 최대값은 표 1과 같이 표현된다.

그림 2. QR 코드의 구성
Fig. 2. QR code structure

QR 코드의 구성은 그림 2와 같이 위치 찾기 심볼, 데이터영역, 셀(Cell)로 구성되어 있다.

3. 영상정보에서 본 스테가노그라피 기법

스테가노그라피[8][9][10] 기법은 여러 가지 기법이 있으나 LSB (Least Significant Bit)기법이 잘 알려져 있다. LSB의 경우 영상정보의 1픽셀(pixel) 데이터를 2진수로 표현하고, 8비트중 1비트에 나타내는 값으로 8비트 중 최하위 1비트를 변경시키는 방법으로 영상정보에서 변화되는 값이 적어 최하위 1비트를 변경하더라도 인간의 시각체계(HVS, Human Visual System)에서는 커다란 변화를 인지하기 힘들다는 점을 이용하고, LSB로 표시한다.

그림 3은 LSB 기법에서 픽셀이 변화되는 과정을 보여준다. 원 영상정보의 픽셀 값이 102이고 비밀 정보(Security Information)가 1일 때, LSB(1)을 실행하면 픽셀의 최하위 1비트 값이 비밀 정보의 값으로 교체되어 픽셀 값은 비밀 정보를 포함한 103이 된다.

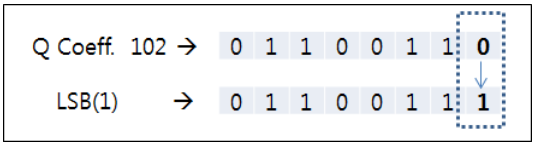

그림 3. LSB 실행 과정의 예
Fig. 3. The example of LSB process.

III. 제안한 방법

본 논문에서는 워터마크와 QR 코드의 연구를 위하여 워터마크(메시지)를 QR 코드화하여 원 영상정보 내에 은닉(삽입)한다. 그림 4와 같이 일반적으로 영상정보의 안쪽 혹은 바깥쪽의 위치에 QR 코드를 표시한다.

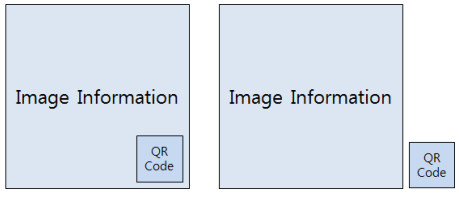

그림 4. 기본 구성도(QR 코드)
Fig. 4. Based structure (QR Code)

본 논문에서는 그림 5와 같이 제안한 방법을 표현할 수 있다. 기본적인 구성은 영상(Cover image) 정보를 주파수 영역의 DCT 및 양자화(Q) 과정을 통하여 얻는다. 워터마크 메시지(Message)를 QR 코드로 변환하여 얻게 된다. 얻은 신호는 Steganography 방법을 적용하여 부호화된 영상을 만들 수 있다.

Steganography는 DCT/Q를 통해 얻은 영역을 DC(Direct Current)와 AC(Alternating Current)로 분리하였다. 그리고 본 연구에서는 워터마크의 삽입(은닉) 및 추출방법은 널리 알려진 방법을 확장하여 각각의 대역에 적용하였다.

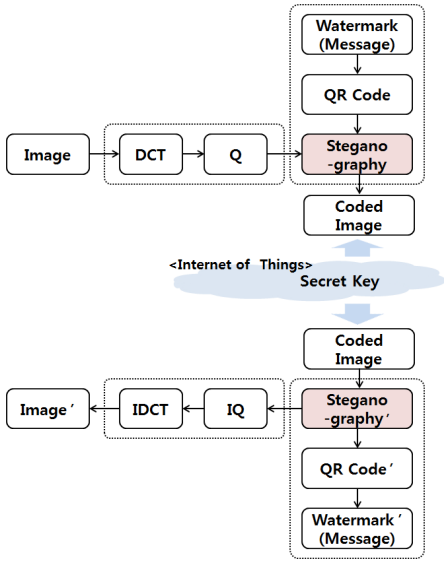

그림 5. 워터마크 삽입(은닉)과정과 추출과정
Fig. 5. Watermark insert and extract process

1. 영상정보에 메시지의 은닉(삽입)과정

그림5의 윗 부분은 제안한 메시지를 삽입과정의 기본 구성도이다.

워터마크 은닉(삽입)과정은 다음과 같다.

1. 원 영상을 블록으로 분리한다.
2. DCT/Q(양자화)를 통하여 부호화 한다.(QC)
3. 영상의 워터마크 Secret Key를 결정한다.
4. 워터마크 메시지를 QR 코드화한다.(WM_{QR})
5. 블록단위로 부호화된 QC와 WM_{QR} 값을 스테가노그피 LSB를 적용한다.
6. 부호화된 영상의 정보를 인터넷을 통하여 전송한다.

2. 영상정보에 메시지의 추출과정

워터마크의 역 과정은 그림5의 아래 부분과 같다. 부호화된 영상을 블록으로 분리하여, 미리 얻게된 Secret Key를 가지고 Steganography LSB를 통하고, 양자화와 DCT된 역 과정을 통하여 영상을 얻을 수 있다. 또한 Steganography LSB를 통하여 QR 코드와 워터마크의 역과정을 통하여 워터마크 메시지를 얻을수 있다.

워터마크 추출 과정은 다음과 같다.

1. 부호화된 영상정보를 블록으로 분리한다.
2. 미리 얻은 Secret Key를 가지고 Steganography LSB를 통하여 정보를 분리한다.

3. IQ/IDCT를 통하여 역 부호화하여 영상을 얻는다.
4. Steganography LSB에서 분리된 QR 코드에서 정보를 추출한다.
5. 워터마크 메시지를 얻게 된다.

Ⅳ. 모의실험

본 논문에서 제안하는 알고리즘의 실험은 Core i5 3.4GHz, RAM 4.00GB의 Window 7에서 Visual C++를 이용하여 시뮬레이션 프로그램을 작성하였다. 그리고 NxN(256*256) 그레이 레벨의 정지 영상과 nxn(32*32) 그레이 레벨의 영상인 워터마크(메시지)를 사용하여 실험하였다. 그림 6에서는 실험에 사용된 QR Code의 워터마크(메시지) 정보이며, "Yong-Soon Im, Kookje University, Dept. of IT, Korea"의 정보이다.

Yong-Soon Im, Kookje University,
Dept. of IT, Korea

그림 6. QR 코드에서 사용된 워터마크된 메시지
Fig. 6. Watermarked Message using QR code

그림 7에서는 원 QR 코드와 제안한 방법을 통하여 얻은 결과 이다. 그림과 같이 원영상과 같은 결과를 얻게 되었다.

(a) Original QR (b) Result

그림 7. QR 코드
Fig. 7. QR code

(a) Lena (b) Couple

(c) Airplane (d) Girl

그림 8. 원 영상
Fig. 8. Original image

(a) Lena (b) Couple
(c) Airplane (d) Girl

그림 9. QR 코드로 워터마크된 영상
Fig. 9. Watermarked Image using QR code

그림 8에서는 실험에서 사용된 4개의 영상 Lena, Couple, Airplane, Girl을 보여주고 있다. 그림 9는 그림8에서 사용된 영상의 결과이다. 표 2는 모의실험에서 얻은 결과이며 평균 PSNR을 향상시켰으며, 보다 객관적으로 증명하기 위해서 PSNR (Peak Signal to Noise Ratio)을 사용한다.

$$PSNR = 10 \times \log_{10}\left(I_{\max}^2 \;/\; MSE\right) dB \tag{3}$$

$$MSE = \frac{1}{MN}\sum_{i=1,j=1}^{M}\sum^{N}(|I_{i,j} - I'_{i,j}|)^2 \tag{4}$$

여기서 PSNR와 MSE는 원 영상 I와 스테고나그라피, QR 코드, 워터마크를 통한 영상 I′의 차이 값을 표현한다. M은 이미지의 가로/세로의 값이다.

사용된 정규화 상관도(NC, Normalized Correlation)를 사용하였고, NC의 계산식은 다음과 같다. 원 워터마크와 추출된 워터마크의 NC값은 모두 100을 얻게 되었다.

$$NC = \sum_{i=1}^{m \times n} w_i \cdot w_i^{ex} \; / \; \sum_{i=1}^{m \times n} w_i^2 \qquad (5)$$

여기서 W_i는 원 워터마크, W_i^{ex}는 추출된 후 복호화한 워터마크를 각각 나타내며, m×n은 워터마크의 크기를 나타낸다.

표 2. 모의실험 결과
Table 2. Simulation Resulr

Image	Original PSNR	Watermarked PSNR	NC
Lena	29.17	29.05	100
Couple	28.15	28.07	100
Airplane	28.83	28.73	100
Girl	30.46	30.32	100

V. 결 론

본 논문에서는 IoT에서 사용하는 영상 정보는 부호화 방법과 워터마크(메시지), QR Code를 통하여 새로운 부호화된 메시지를 구성할 수 있다. 스테가노그라피 LSB 기법을 적용하여, 영상정보의 보안(저작권 등)을 얻을 수 있다. QR 코드는 삭제, 변경을 통해서 다른 의미를 표현할 수 있지만, 본 논문에서 QR 코드를 원 영상에 은닉(삽입)함으로써 영상의 중요한 정보를 은닉함으로써 위조여부를 확인할 수 있다. 이 방법은 여러 분야에 적용 가능하며 영상정보의 보안의 방안으로 이용하면 정확한 위조여부를 인증할 수 있다.

본 논문에서 영상정보의 보안 방법을 제안할 수 있고 앞으로 여러 분야에서 영상정보의 보안에 대하여 연구될 수 있다.

References

[1] X. Xia, C. G. Boncelet and G. R. Arce, "A Multiresolution Watermark for Digital Images," IEEE Int. Conf. on Image Processing, vol. 1, pp. 548~551, 1997.

[2] D. Zheng, Y. Liu, J. Zhao, and A. E. Saddik, "A survey of RST invariant image watermarking algorithms," ACM Computing Surveys, vol. 39, issue 2, no. 5, 2007.

[3] M. Yesilyurt, Y. Yalman, A. T. Ozcerit, "A New DCT Based Watermarking Method Using Luminance Component," Elektronika Ir Elektrotechnika, Vol. 19, No. 4, pp. 47-52, 2013.

[4] Ji-in Kim, Jeong-Sig Kim, and Goo-Rak Kwon, "A Robust Watermarking using Quantized AC Coefficients," Journal of KIIT. Vol. 11, No. 6, pp. 85-90 June 30, 2013.

[5] QR Code, http://www.denso-wave.com/qrcode/ko/index.html

[6] Y. S. Im, E. Y. Kang, "MPEG-2 Video Watermarking in Quantized DCT Domain," The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), Vol. 11, No. 1, pp. 81-86, 2011.

[7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internat of things (IoT): a vision, architectural elements and future directions," Future Generation Computer Science, vol. 29, no. 7, pp. 1645 - 1660, 2013.

[8] I. Jeon, S. Kang, H. Yang, "Development of Security Quality Evaluate Basis and Measurement of Intrusion Prevention System," Journal of the Korea Academia-Industrial cooperation Society (JKAIS), Vol. 11, No. 1, pp. 81-86, 2010.

[9] Diffie, W., and Hellman, M. "New Directions in Cryptography," IEEE trans on Information Theory, vIT-22 n6, p.359-376, November 1976.

[10] Anant M.Bagade and Sanjay N.Talbar, "A High Quality Steganographic Method Using Morphing", J Inf Process Syst(JIPS), Vol.10, No.2, pp.256~270, June 2014.

저자 소개

임 용 순(종신회원)

- 1988년 : 성균관대학교 공학사
- 1993년 : 성균관대학교 공학석사
- 1999년 : 성균관대학교 공학박사
- 2014년 : 숭실대학교 정보과학대학원 정보보안학과
- 2000년 ~ 현재 : 한국인터넷방송통신학회 부회장
- 1998년 ~ 현재 : 국제대학교 IT계열 교수

<주관심분야 : 영상압축부호화, 영상워터마킹, QR code, Steganography, 모바일앱 &보안, 정보보안 등>

- Email : ysim@kookje.ac.kr

강 은 영(정회원)

- 1988년 : 숙명여자대학교 공학사
- 1999년 : 숙명여자대학교 공학석사
- 2008년 : 성균관대학교 공학박사
- 2009년 ~ 현재 : 동양미래대학교 컴퓨터소프트웨어공학과 교수

<주관심분야 : 모바일애드-혹 네트워크, 임베디드소프트웨어, 서비스디스커버리, 영상 워터마킹 & QR code 등>

- Email : eykang@dongyang.ac.kr

박 재 표(정회원)

- 1996년 2월 : 숭실대학교 컴퓨터학부 공학사
- 1998년 8월 : 숭실대학교 컴퓨터학과 공학석사
- 2004년 8월 : 숭실대학교 컴퓨터학과 공학박사
- 2008년 9월 ~ 2009년 8월 : 숭실대학교 정보미디어기술연구소 전임연구원
- 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학원 교수

<주관심분야 : 컴퓨터통신, 보안 등>

- Email : pjerry@ssu.ac.kr