2013년 6월 전자공학회 논문지 제 50 권 제 6 호
Journal of The Institute of Electronics Engineers of Korea Vol. 50, NO. 6, June 2013 http://dx.doi.org/10.5573/ieek.2013.50.6.173

논문 2012-50-6-20

스테가노그라피 기법이 적용된 QR코드 이미지 기반의 키 교환 프로토콜

(A Key Exchange Protocol based on the Steganography with the QR code)

이 길 제*, 윤 은 준**, 유 기 영*

(Gil-Je Lee, Eun-Jun Yoon, and Kee-Young Yoo©)

요 약

기존의 키 교환 프로토콜은 암호학적 방법들을 사용하여 비밀 키를 전달해왔지만, 공격자들로 하여금 다양한 공격을 받아왔었다. 이를 해결하기 위해 본 논문에서는 스테가노그라피 기법을 이용한 키 교환 프로토콜을 제안하였다. 스테가노그라피 기법은 이미지, 문서, 동영상, MP3 파일 등에 비밀 정보를 숨겨 공격자가 비밀 정보가 전달되고 있다는 것을 모르게 하는 방법으로 비밀 키를 공격자의 의심을 받지 않고 효율적으로 전달할 수 있다. 또한, 최근에 많이 사용되고 있는 2차원 바코드인 QR 코드를 비밀 키가 삽입되는 이미지로 사용하여 공격자가 QR 코드를 스캔하여도 QR코드 생성 시 사용되었던 URL로 접속하게 되며 QR 코드에 비밀 키가 삽입된 것을 인식하지 못하게 한다. 실험을 통해서 기존의 스테가노그라피에서 사용되었던 이미지와 QR코드의 이미지의 변형 정도를 측정하여 QR 코드 이미지를 사용했을 때 효율성을 검증해본다.

Abstract

The traditional key exchange protocols are transmitted by using the cryptographic. However, these protocols are compromised by the attacker. To solve this problem, this paper proposes a key exchange protocol based on the steganography with the QR code. The steganography technique embed secret information to the images, documents, videos, and MP3 files and transmit to the others. The attacker can't know that the transmission data is the secret data. Therefore, the sender transmits efficiently and safely the secret data to the others. In additional, the cover image is using the QR code image to insert the secret key. If attackers scan the QR code, then they just read the information or connect URL. They can not be recognized that the QR code image is hiding the secret key. The experiments compare the QR code image with the well-known image about the distortion and the safety.

Keywords : Key exchange protocol, Steganography, QR code, LSB, Spatial domain,

* 정회원, 경북대학교 컴퓨터공학부
(School of Computer Science and Engineering, Kyungpook National University)
** 정회원, 경일대학교 사이버보안학과
(Department of Cyber Security, Kyung-il University)
※ 본 연구는 산업통상자원부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신) [10041145, 자율군집을 지원하는 웰빙형 정보기기 내장 소프트웨어 플랫폼 개발]과 2012년도 정부(교육과학기술부)의 재원으로 한국연구재의 지원을 받아 수행된 기초연구사업임(No. 2012-008348)
© Corresponding Author(E-mail: yook@knu.ac.kr)
접수일자 2013년2월7일, 수정완료일 2013년5월21일

Ⅰ. 서 론

인터넷의 보급과 네트워크 기술의 발전으로 데이터와 멀티미디어 매체의 전달이 빈번히 발생하게 되었고, 그 과정에서 정보가 노출되는 문제가 발생하였다. 이로 인해 데이터를 안전하게 전달하는 방법이 필요하게 되었고, 그 방법으로 암호화를 많이 사용하게 되었다. 하지만, 데이터를 암/복호화하기 위해 참여자 간에 사용되는 비밀 키를 안전하게 교환하기 위한 프로토콜이 필요하게 되었다.

1976년 Diffie-Hellman[1]이 처음 비밀 키 교환 프로토콜을 제안하였으며, 이를 바탕으로 여러 가지 공격에 안전한 프로토콜이 활발히 연구되어 왔다. 비밀 키를 안전하게 교환할 수 있는 방법들로는 대칭 키 기반 기법, 공개키 기반 기법, 패스워드 기반 기법, 하이브리드 기법 등으로 나눌 수 있고, 여러 분야에서 사용되어지고 있다[2~6]. 하지만, 패스워드 추측 공격, 중간자 공격(Man-in the Middle-Attack) 등의 공격에 취약하다는 단점을 가지고 있다[7~9].

이를 해결하기 위해 본 논문에서는 스테가노그라피 기법을 이용한 비밀 키 교환 방법을 제안한다. 스테가노그라피는 대게 잘 알려진 멀티미디어 객체에 비밀정보를 삽입한다. 삽입 알고리즘은 원본 객체와 삽입된 객체의 왜곡을 최소화 하여 사람이 육안으로 보았을 때 원본과 삽입된 객체와의 차이를 느끼지 못한다. 따라서, 비밀 키가 삽입된 멀티미디어 객체가 노출되어도 공격자는 전송되어지는 객체에 비밀 정보가 삽입되어있다는 것을 인지하지 못한다. 이런 스테가노그라피 기법에는 주로 잘 알려진 멀티미디어 이미지를 많이 사용한다. 스트레가노그라피를 이용한 전송 중에 공격자에 의해 비밀 키가 숨겨진 이미지가 노출이 되더라도 공격자는 비밀 키를 숨게 파악할 수 없으며, 이미지의 변형으로 인한 왜곡을 인지하여 비밀 키를 찾아 내더라도 숨긴 방법을 모르는 경우 오랜 시간이 걸리게 된다[10~13].

최근 바코드 인식으로 상품정보 또는 제품의 홈페이지 링크를 제공하는 QR 코드는 이미지의 형태로 스테가노그라피 기법을 적용할 수 있으며, 기존의 잘 알려진 이미지를 사용하는 것 보다 더 안정적이라고 할 수 있다. 기존의 스테가노그라피 기법에서 사용하는 이미지의 경우 이미지에 특정 기법들을 이용하여 삽입과 추출 과정을 거치게 되어, 이미지가 전달되는 동안 공격자가 비밀 정보의 삽입 유/무를 모르게 하였다. 하지만, QR코드 이미지의 경우, 일반적으로 URL 또는 상품정보를 이용하여 QR 코드를 생성하고 공개된 채널에서 전송을 하여도 대부분 스마트 폰이나 리더기를 이용하여 QR코드를 인식하려고 한다. 즉, 스테가노그라피 기법을 적용한 QR 코드 이미지를 공격자가 확인하더라도 QR코드의 정보만 읽게 된다.

본 논문에서는 안전한 비밀 키 교환을 위해 QR 코드 이미지에 스테가노그라피 기법을 적용한 방법을 제안하고자 한다. 논문의 구성은 다음과 같다. Ⅱ장에서는 QR 코드와 스테가노그라피 기법에 대해 기술하고, Ⅲ장에서는 QR코드 이미지 기반의 스테가노그라피를 이용하는 비밀 키 교환 프로토콜을 제안하며, Ⅳ장에서는 원본 QR코드 이미지와 삽입된 QR코드 이미지의 왜곡 비교와 안전성에 대해 실험과 분석을 한다. Ⅴ장에서는 결론 및 향후 연구를 기술한다.

Ⅱ. 관련연구

1. 비밀 키 교환 프로토콜

1976년 Diffie와 Hellman에 의해 키 교환 프로토콜이 제안되었다[14]. Diffie-Hellman 방법은 이산대수문제의 어려움에 근거하여 제안되었으며, 수학적으로 안전하다. 이런 이유 때문에 Diffie-Hellman 방법이 많이 사용되어져 왔지만, 중간자 공격에 취약하여 이를 개선한 방법들이 많이 제안되었다[2~4]. 그림 1은 D-H 방법을 나타낸 그림으로 Alice와 Bob 두 사람 간 키를 공유할 때, g와 p 두 개의 공개된 파라미터를 같는다. g와 p는 서로소이고, g는 p보다 작은 정수이다. 공유하는 과정으로는 Alice가 g에 자신이 임의로 생성한 a를 지수승하여 mod p로 나누었을 때의 값을 Bob에게 보내고 Bob도 자신이 임의로 생성한 b를 지수승하여 모듈러 연산 취한 값을 Alice에게 보내게 된다. 그리고 Alice와 Bob은 자신들이 받은 값에 임의로 생성한 a와 b를 각각 지수승하여 p로 모듈러를 취해 비밀 키를 생성한다.

그림 2는 DH키 교환 방법이 취약한 중간자 공격의 과정을 보여준다. 공격자(Oscar)가 Alice와 Bob이 비밀 키를 교환하는 중간에 전달되는 값을 가로채고 자신의 값을 Alice와 Bob이 보낸 것처럼 전송하고, 이 값을 받

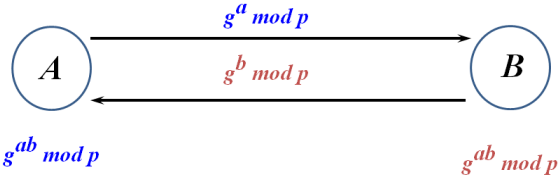

그림 1. DH 키 교환 방법
Fig. 1. Diffie-Hellman Key Exchange Protocol.

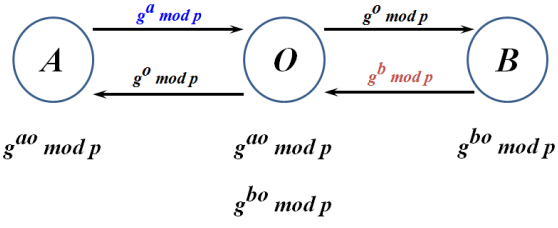

그림 2. 중간자 공격
Fig. 2. Man-in-the-Middle Attack.

은 Alice와 Bob은 Oscar와의 비밀 키를 생성하게 된다.

이런 문제점을 해결하기 위해 제안하는 알고리즘에서는 보내는 사람의 ID와 해쉬를 이용한 방법을 이용한 기법을 제안한다.

2. 스테가노그라피 기법

스테가노그라피 기법에서 가장 많이 알려진 기법은 LSB(Least Significant Bit)이다[15]. LSB의 경우 이미지의 1픽셀(pixel)을 나타내는 8-bit 중 최하위 비트를 변경시키는 방법으로 원본이미지에서 변화되는 값이 적어 최하위 1비트 변경 하더라도 인간의 시각체계(Human Visual System)에서는 변화된 점을 인지하기 힘든 점을 이용한다. 그림 3은 LSB 기법에서 픽셀이 변하는 과정을 보여준다. 원본 이미지의 픽셀 값이 200이고 비밀 정보가 1일 때, LSB - 1을 수행하면 픽셀의 최하위 1비트 값이 비밀 정보의 값으로 교체되어 픽셀 값은 비밀 정보를 포함한 201이 된다.

LSB 이외에도 연속된 두 픽셀 값의 차이를 이용하여 삽입하는 방법과 히스토그램을 이용하는 기법[11, 16~17] 등 다양한 방법이 있다.

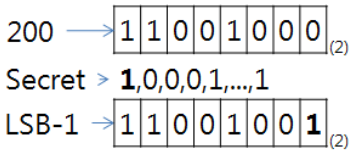

그림 3. LSB-1 실행 과정
Fig. 3. The example of LSB-1 process.

3. QR 코드

2차원 바코드는 1차원 바코드의 13자리의 상품식별 코드를 표현하는 것과 달리 작은 사각형 모양으로 점자 또는 모자이크식 코드로 표현되며, 바코드 자체에 문자, 숫자 등의 텍스트, 그래픽 형태의 정보 등을 저장할 수 있어, 바코드를 읽는 것만으로도 정보가 나타나게 된다[18~19]. 그림 4는 다양한 2차원 바코드를 보여준다[20].

그림 4. 2차원 바코드의 종류 : (a) QR Code, (b) Data Matrix, (c) Aztec code, (d) Maxi code, (e) Shot code
Fig. 4. 2-D barcodes : (a) QR Code, (b) Data Matrix, (c) Aztec code, (d) Maxi code, (e) Shot code

표 1. 2차원 바코드의 삽입량[20]
Table 1. The capacity of 2-D barcodes.

	숫자	알파벳+숫자	Byte	Kanji
QR Code	7089	4296	2953	1817
Data Matrix	3116	2355	1556	778
Aztec code	3832	3067	11914	0
Maxi code	138	93	0	0
Shot code	0	0	40	0

2차원 바코드의 경우 암호화가 가능해 멤버십 카드 등 각종 인증 시스템으로도 활용되며, 휴대폰에 바코드 이미지를 저장하여 액정으로 불러왔을 때 바코드의 기능으로 사용이 가능하게 되었다. QR코드는 2000년에 국제표준(ISO/IEC18004)으로 2차원 바코드 중 가장 널리 사용되고 있다. 표 1은 2차원 바코드에 삽입되는 문자, 숫자 등의 저장되는 삽입량을 표현한다.

Ⅲ. 제안하는 방법

본 장에서는 안전한 비밀 키 교환을 위해 QR 코드 이미지에 스테가노그라피 기법을 적용한 방법을 제안한다. 제안하는 기법은 비밀 정보를 삽입하고 추출하는 과정과 교환하는 키를 전송과정으로 나누어진다. 삽입과 추출과정에서는 스테가노그라피 기법 중 많이 사용하고 있는 LSB 기법을 이용하여 키 교환 프로토콜에서 전달되는 값을 QR코드에 삽입하고 추출한다.

그림 5와 그림 6은 삽입과정과 추출과정을 보여준다. 삽입과 전달과정은 Alice와 Bob이 비밀 키를 교환하는 과정에 전달되는 값을 URL을 통해 생성한 QR코드에

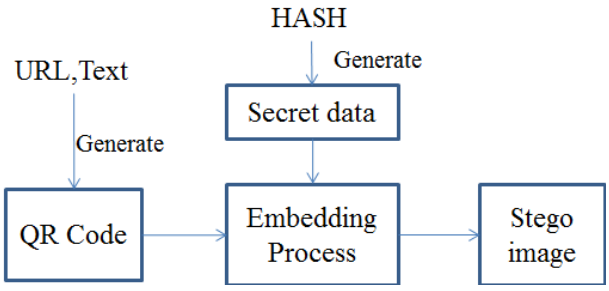

그림 5. 삽입과정 흐름도
Fig. 5. The flowchart of embedding phase.

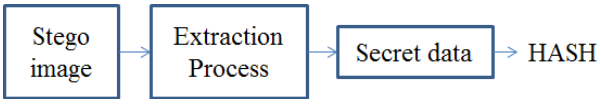

그림 6. 추출과정 흐름도
Fig. 6. The flowchart of extraction phase.

삽입하고 전달받은 QR코드를 통해 비밀 키를 추출한 뒤 검증하는 과정을 거치게 된다.

1. 키 공유 과정

Alice와 Bob이 공유하는 과정은 URL을 이용해 생성된 QR 코드 이미지에 Alice와 Bob이 공유하기 위한 키를 삽입하여 전송한다. 전송하는 과정은 다음과 같다.

① Alice는 자신의 ID와 타임스탬프(t_a) 그리고 비밀키를 해쉬한 값 (ID_a, t_a, g^a, h($ID_a||t_a||g^a$))을 스테가노그라피 기법을 이용해 QR코드에 삽입하여 Bob에게 전송한다.

② Bob은 Alice로부터 전송 받은 값을 검증하기 위해 QR코드로부터 데이터를 추출한다. 이때, 카메라를 통해서 추출하는 것이 아닌 삽입에 사용된 스테가노그라피 기법을 이용하여 추출한다. 추출해낸 값과 Bob이 계산한 (ID_a, t_a, g^a, h($ID_a||t_a||g^a$))값을 비교하여 Alice가 맞는지 검증하고 Alice가 아니면 통신을 종료하고, 맞으면 Bob이 메시지를 보낸다.

③ Bob은 Alice가 보낸 내용과 같이 자신의 ID와 타임스탬프(t_a) 그리고 비밀 키를 해쉬한 값 (ID_b, t_b, g^b, h($ID_b||t_b||g^b$))을 QR코드에 입력하여 보내게 된다. 이때, 사용하는 QR코드는 A와 같은 URL 이나 데이터를 사용하거나 다른 데이터를 이용해 생성하여도 된다.

④ Bob으로부터 받은 QR코드에서 데이터를 추출하여 Bob이 맞는지 (ID_b, t_b, g^b, h($ID_b||t_b||g^b$))을 검증한다.

위의 과정을 마치고 나면 Alice와 Bob은 상호간에 공통된 키인 g^{ab}를 얻을 수 있게 된다. 그림 7은 Alice와 Bob이 키교환하는 과정을 보여주고 있다.

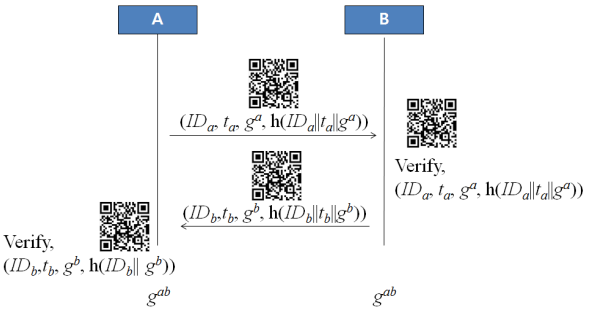

그림 7. 키 교환 과정
Fig. 7. The Key Exchange process of the proposed scheme.

Ⅳ. 안전성 분석

본 장에서는 제안한 프로토콜에 대한 보안성을 분석한다. 먼저, 제안한 프로토콜의 안전성 분석을 위해 필요한 보안 항목을 다음과 같이 정의한다.

[정의 1] 사용자 ID와 g^a, g^b는 높은 엔트로피를 가지는 값으로 다항식 시간 내에 계산될 수 없다.

[정의 2] 안전한 단방향 해쉬 함수(secure one-way hash function)는 y=h(x)와 안전한 메시지 인증 코드 함수는 y=M(x)에서, 주어진 x를 이용하여 y를 계산하는 것은 쉽지만, 주어진 y를 이용하여 x를 계산하는 것은 어렵다.

[정의 3] 동기화된 시간은 오차 허용 범위가 있으며, 해당 범위를 초과할 경우 받은 데이터는 폐기한다.

위 정의들은 기반으로 제안하 인증 시스템은 다음과 같이 상호인증을 명시적으로 제공하며, 중계 공격, 재전송 공격 등에 안전하다.

1. 상호인증

제안한 프로토콜의 단계 2에서 Bob는 자신이 계산한 h($ID_a||t_a||g^a$)이 Alice로부터 수신한 h($ID_a||t_a||g^a$) 값과 동일한지 검증하여 Alice를 인증하고, 단계 4에서 Alice는 자신이 계산한 h($ID_b||t_b||g^b$)과 Bob으로부터 수신한 h($ID_b||t_b||g^b$)과 동일한지 인증한다. Alice와 Bob 사이에 공유된 비밀키 g^{ab}를 모르는 공격자는 Alice 또는 Bob으로 위장하여 다른 공격들을 할 수 없다.

2. 중계 공격

공격자는 Alice와 Bob 간에 전송되는 값을 이용해 제안한 인증 프로토콜에서 ID와 타임스탬프, 랜덤값을 얻어낼 수 있다. 하지만 공개채널에 전해지는 값을 알고 있더라도, 공유한 키인 g^{ab}를 계산하는 것은 이산대수문제에 의해 polynomial time 안에 연산하는 것은 불가능하다. 또한, 타임스탬프를 이용하여 허용 오차를 벗어나는 시간에 데이터가 도착하게 되면 인증이 되지 않는다. 따라서, 제안한 프로토콜은 중계 공격에 강하다고 할 수 있다.

3. 재전송 공격

제안한 프로토콜에서 동기화된 타임스탬프 값을 이용하여 Alice와 Bob간의 상호인증을 수행하기 때문에, 과거에 공격자에 의해 재전송된 값은 상호인증 과정 중에 쉽게 검출된다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

V. 실 험

본 장에서는 실험을 통해서 QR코드 이미지와 기존의 이미지의 왜곡 정도와 비밀 정보가 정상적으로 추출이 되는지와 QR코드를 인식 시켰을 때 정상작동 되는 지를 실험한다. 실험을 위해 QR 코드 이미지는 URL을 http://infosec.knu.ac.kr 로 하여 생성하였다. 그림 8은 그레이스케일 256 X 256 픽셀로 생성된 QR 코드 이미지와 삽입과정에 비밀 키를 대신하여 사용하게 될 그레이스케일 128 X 128 픽셀의 이미지를 보여준다.

그림 9는 비밀 정보(b)를 LSB-2 기법을 이용하여 QR코드(a)의 각 픽셀마다 2bit씩 삽입하였을 때의 결과로 공격자에게 쉽게 공격당하는 것을 예방하기 위해 비밀 정보를 마스터키를 이용해 치환한 다음 삽입하였다.

PSNR[21]을 이용하여 원본 QR코드 이미지와 비밀 정

(a) 생성된 QR코드 (b) 비밀 이미지

그림 8. 생성된 QR 코드와 비밀 데이터
Fig. 8. (a) the generated QR code and (b) the secret image.

(a) 삽입된 QR코드 (b)추출된 비밀 정보

그림 9. LSB-2 삽입된 QR 코드와 추출한 비밀 정보
Fig. 9. (a) the embedded QR code using LSB-2 and (b) the extracted secret image.

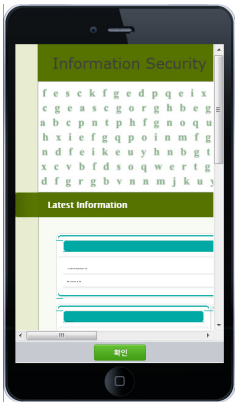

그림 10. 비밀 정보가 삽입된 QR코드의 인식
Fig. 10. The recognition of the embedded QR code.

보가 삽입된 QR코드 이미지의 왜곡정도를 실험하여, 측정한 결과는 기존 42.82 db이 나타났다. 기존의 잘 알려진 Airplane, Lena, Baboon과 같은 이미지에이미지의 경우는 44.02 db의 결과가 나타났다.

이는 QR코드의 픽셀값은 0과 255를 이루는 것에 비해, 기존에 알려진 이미지의 경우 다양한 픽셀 값을 가져 이미지 픽셀 값의 차이가 QR코드 이미지 보다 적게 변경되기 때문이다. 하지만, PSNR 측정치가 30db이상일 경우 인간의 시각 특성상 화질 저하로 판단하기 쉽지 않아, 안전한 비밀 교환에 사용할 때 안전하다 할 수 있다.

또한, 그림 10과 같이 비밀정보가 삽입된 QR코드 이미지를 스마트폰에 인식시켰을 때, 비밀 정보가 아닌 생성된 QR 코드의 URL로 정상적으로 접속되었다. 이런 결과를 얻을 수 있는 것은 QR코드의 특징으로 소재와 상관없이 문양과 음영만 구분된다면 스마트 폰이나 리더기를 이용하여 바코드를 읽을 수 있기 때문입니다.

VI. 결 론

비밀 키 교환 기법에서는 키를 교환할 때 사용하는 방법이 매우 중요하며, 키 교환에 사용되어야 하는 프로토콜은 상호인증을 제공하고, 중계공격, 재전송 공격 등 으로부터 안전해야 한다. 따라서, 본 논문에서는 키 교환시 발생할 수 있는 위협에서 비밀 정보를 안전하게 지키기 위해, QR코드 이미지를 사용하는 스테가노그라피 기법을 이용하여 키 교환 프로토콜을 제안하였다. 그 결과, 생성된 QR 코드에 전송되는 비밀 키를 삽입하여 공격자의 관심을 끌지 않도록 하였으며, 중간에 QR 코드가 노출되어 스마트폰과 같은 기기로 코드를 스캔하여도 생성시 사용한 URL로 이동되기 때문에 비밀 키

는 안전하게 보호된다. 또한, QR코드에 비밀 정보를 많이 삽입하면서도 왜곡을 줄여 육안으로 확인하여도 쉽게 판별하지 못하였다.

그 외 여러 가지 공격들에 대해서 분석한 결과 제안하는 방법은 상호인증을 제공하면서도, 중계공격과 재전송공격에 안전하였다.

REFERENCES

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

[2] 김선종 외, “금융 보안 서버의 개인키 유출 사고에 안전한 키 교환 프로토콜”, *정보보호학회지*, 제19권 제3호, pp. 120-131, 2009

[3] 변진욱, “강화된 키 교환 프로토콜의 안전성 모델에 관한 연구”, *정보보호학회지*, 제20권, 제2호, pp. 78-84, 2010.

[4] 은선기 외, “안전한 M2M 통신 구축을 위한 상호 인증 및 키 교환 프로토콜”, *정보보호학회지*, 제20권, 제1호, pp. 73-83, 2010

[5] 최재탁 외, “ID 기반의 그룹 키 교환 기법에 대한 연구 동향”, *정보보호학회지*, 제19권, 제4호, pp. 36-43, 2009

[6] B.LaMmacchia, K.Lauter, and A.Mityagin, “Stronger Security of Authenticated Key Exchange.” *ProvSec 2007*, LNCS 4784, pp..1-16, 2007.

[7] V.Boyko, P.MacKenzie, and S. Patel, “Provably Secure Password Authenticated Key Exchange Using Diffie-Hellman,” *EUROCRYPT 2000*, LNCS 1807, pp. 156-171, 2000.

[8] 신성철, 이성운, “동일 서버를 사용하는 두 사용자 간 효율적인 패스워드 기반의 키 교환 프로토콜,” *정보보호학회논문지*, 제15권, 제6호, pp.127-133, 2005

[9] 박호상, 정수환, “패스워드 기반의 상호 인증 및 키 교환 프로토콜,” *정보보호학회논문지*, 제12권, 제5호, pp. 38-43, 2002.

[10] K. Curran, K. Bailey, “An Evaluation of Image based Steganography Method”, *International Journal of digital Evidence*, Vol. 2, pp 1-40, 2003

[11] S. Katzenbeisser and F. A. P. Petitcolas, “Information hiding techniques for steganograpy and digital watermarking,” *Artech House*, 2000.

[12] Jiri Fridrich, “A New Steganographic Method for Palette-Based Images,” in Proceedings of *the IS&T PICS conference*, Savannah, Georgia, pp. 285-289, Apr. 1998.

[13] C.F. Lee, H.L. Chen, and H.K.Tso, “Embedding capacity raising in reversible data hiding based on prediction of difference expansion”, *The Journal of Systems and Software 83*, pp.1864-1872, 2010.

[14] Diffie, W., and Hellman, M. “New Directions in Cryptography.”, I*EEE trans on Information Theory*, vIT-22 n6, p.359-376, November 1976.

[15] D.K Andrew, “Steganalysis of Embedding in Two Least-Significant Bits”, *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, Vol.2, NO.1, pp. 46-54, 2007

[16] 김대수, 유기영, “모듈러 연산과 히스토그램 이동에 기반한 새로운 가역 정보 은닉 기법,” *멀티미디어학회논문지*, 제15권, 5호, pp. 639-650, 5월, 2012.

[16] 최장희, 윤은준, 유기영, “DE 기반의 적응적인 가역정보은닉기법,” *전자공학회논문지*, 제49권 CI편, 제2호, pp. 103-114, 3월, 2012.

[18] www.denso-wave.com

[19] H. Morris, I.M. El-Ddin, and M. Eyadat, “BarcodeWatermarking”, *Information Technology : New Generations 2009*, pp.1296-1300, 2009.

[20] www.wikipia.org

[21] Huynh-Thu, Q. and Ghanbari, M. “Scope of validity of PSNR in image/video quality assessment,” *Electronics Letters* 44 (13), pp. 800 - 801, 2008.

저 자 소 개

이 길 제(정회원)
2007년 경일대학교 컴퓨터공학과 (공학사)
2010년 경북대학교 정보통신학과 (공학 석사)
2011년～현재 경북대학교 컴퓨터공학부 박사과정
<주관심분야 : 암호학, 네트워크보안, 스테가노그라피, 디지털 워터마킹>

유 기 영(정회원)-교신저자
1976년 경북대학교 수학교육과 (이학사)
1978년 한국과학기술원 컴퓨터공학과 (공학석사)
1992년 미국 뉴욕 Rensselaer Polytechnic Institute 컴퓨터과학과 (공학박사)
1978년～현재 경북대학교 컴퓨터공학과 교수
1997년～1998년 한국정보과학회 영남지부장
1999년～현재 한국정보과학회 영남지부장
1999년～현재 한국 정보과학회 이사
2006년～현재 제12대 한국 정보보호학회 부회장
<주관심분야 : 암호학, 정보보호, 네트워크보안, 스테가노그라피>

윤 은 준(정회원)
1995년 경일대학교 졸업(공학사)
2003년 경일대학교 컴퓨터공학과 (공학 석사)
2004년 경북대학교 컴퓨터공학과 (공학 박사)
2007년～2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2009년～2011년 경북대학교 대학원 전자전기컴퓨터학부 계약교수
2011년～현재 경일대학교 사이버보안학과 교수
<주관심분야 : 통신, 컴퓨터, 신호처리, 반도체>