논문 2012-49-12-18

자기참조 가상 패리티 비트를 이용한 XOR기반의 고화질 정보은닉 기술

(XOR-based High Quality Information Hiding Technique Utilizing
Self-Referencing Virtual Parity Bit)

최 용 수*, 김 형 중**, 이 달 호***

(YongSoo Choi, HyoungJoong Kim, and DalHo Lee)

요 약

최근 들어 정보은닉기술에 대한 필요성이 많이 증가되고 있으며 국제치안, 군사 그리고 의료영상 등의 분야에서 그 예를 많이 볼 수 있다. 본 논문에서는 한 픽셀의 다수 MSB(MSBs: Most Significant Bits)의 Parity Bit를 이용하여 gray영상에 대해 정보를 은닉하는 방법을 제안한다. 스테가노그래피(Steganography) 분야에서 많은 연구들이 LSB 대체(Substitution), XOR연산을 채용하여 연구되어왔으며 궁극적인 목적은 낮은 복잡도와 높은 은닉용량, 동시에 화질의 저하를 최소화하는 것이다. 하지만 LSB 대체 방법은 높은 은닉용량을 가짐에도 불구하고 너무나 간단한 작업으로 인해 안전하지 못하다. 또한 XOR연산을 이용한 방법들은 픽셀 수 대비 약 75%의 은닉률을 달성하였다. 제안된 방법에서 각 픽셀의 LSB(Least Significant Bit)는 비밀메시지 1비트와 해당 픽셀의 7 MSBs의 Parity Bit와 XOR 연산된다. 제안한 방법은 대칭키 프로토콜의 개념을 스테가노그래피에 적용한 것이며 대칭키를 자기참조에 의해 생성하도록 하였다. 제시한 방법은 기존의 XOR방법들에 비해 은닉률이 25% 높으며 원본 대비 픽셀의 LSB 반전률이 약 6%정도 개선되는 효과를 보였다.

Abstract

Recently, Information Hiding Technology are becoming increasingly demanding in the field of international security, military and medical image. This paper proposes data hiding technique utilizing parity checker for gray level image. many researches have been adopted LSB substitution and XOR operation in the field of steganography for the low complexity, high embedding capacity and high image quality. But, LSB substitution methods are not secure through it's naive mechanism even though it achieves high embedding capacity. Proposed method replaces LSB of each pixel with XOR(between the parity check bit of other 7 MSBs and 1 Secret bit) within one pixel. As a result, stego-image(that is, steganogram) doesn't result in high image degradation. Eavesdropper couldn't easily detect the message embedding. This approach is applying the concept of symmetric-key encryption protocol onto steganography. Furthermore, 1bit of symmetric-key is generated by the self-reference of each pixel. Proposed method provide more 25% embedding rate against existing XOR operation-based methods and show the effect of the reversal rate of LSB about 2% improvement.

Keywords : Information Hiding, XOR Operation, Self-reference, Parity Check

I. 서 론

전통적으로 비밀통신(Secret Communication)은 크게 두 가지로 나눌 수 있다. 하나는 수학적 암호기법이며 다른 하나는 지각적 암호화인 스테가노그래피(Steganography)이다. 암호기술은 인류역사상 가장 오

* 정회원, *** 평생회원, 고려대학교 정보보호대학원
(Graduate School of Information Security, Korea University)

** 정회원, 가천대학교 전자공학과
(Dept. of Electronics, Gachon University)

※ “이 연구에 참여한 연구자(의 일부)는 ‘2단계BK21 사업’의 지원비를 받았다”

접수일자: 2012년10월25일, 수정완료일: 2012년11월26일

래된 기술로서 고대의 암호화된 상형문자 사용, 문자의 순서를 바꾸어 놓는 고전암호, 20세기 초반 전쟁에 사용되었던 암호 Disc 및 머신을 이용한 비밀통신 그리고 키교환을 이용한 현대적 암호기술 등으로 나눌 수 있다. 그 중에서도 암호문에서 필요한 조건은 암호문과 평문의 상관관계를 찾아내는 것이 어려워야 하며 키의 교환을 통해 평문의 암호화 암호문의 복호화가 실시되어야 한다. 또한 키의 분배에 있어 안전한 비밀통신이 보장되어야 한다. 위의 두 분류의 가장 목표 및 차이점은 다음과 같이 설명가능하다. 수학적 암호화는 제 3자(도청자: eavesdropper)에 의해 존재가 노출되기 싫지만 암호화된 데이터를 복구하는데 드는 노력이 최대가 되도록 하고, 제3자에 의한 공격(악의적 도청)을 가정하지 않는다. 즉, 스테가노그라피는 알고리즘이 복잡하지 않은 대신 제3자에 의해 의심을 받지 않도록 하기 위해 화질의 저하가 최소가 되도록 설계가 되어야 하는 조건을 가지게 된다.

암호 알고리즘은 크게 대칭키 암호화와 공개키 암호화로 분류되고 전자는 송수신자가 동일한 비밀 키를 분배하여야 하며 후자는 암호화 키와 복호화 키를 분리하여 암호화키는 공개하고 복호화 키는 비밀리에 보관하는 방식이다. 사전 키 공유의 문제를 해결하는 측면에서 공개키 암호방식은 수학적으로 복잡하게 되어있지만 암호 • 복호화 시간의 증가라는 단점을 가지게 된다. 사전 키 공유는 공개키 암호를 이용하여 송수신자가 공유한 후, 이후 대칭키 암호를 이용하여 비밀통신을 이용하는 하이브리드(Hybrid) 형식이 최근에 많이 사용되어진다.

스테가노그라피 기술은 정보은닉 (Data Hiding, Information Hiding, Steganography)의 한 종류로 인식되며 오랜 기간 동안 연구가 이어져 왔으며 최근에는 낮은 연산량을 기반으로 하는 LSB 대체, XOR 연산 그

리고 패리티검사 기반의 기술들로 많이 발표되어져 왔다^[3~8]. 위에 열거한 방법들은 픽셀 내 또는 픽셀간의 아주 간단한 연산을 기반으로 하며 그에 비해 삽입할 수 있는 정보의 양은 적지 않음이 발표되어져 왔다^[2~7,9].

II. Technical Steganography Methods

Venkatesan et al.과 Byun et al. 등은 이진 영상을 블록별로 나누어 블록내의 패리티검사를 수행하며 정보를 은닉하는 기술을 발표하였다. 하지만 블록기반 기법은 픽셀 당 정보량이 적은 이진영상에서는 효과를 보이지만 정보량이 풍부한 그레이 영상 또는 컬러영상에서는 그다지 효과적이라고 할 수 없다. 이 방법들은 비밀 메시지를 삽입하기 위해 이진영상을 일정크기의 블록으로 나누고 블록의 픽셀 값에 대한 패리티검사를 수행하여 '0'삽입 시 짝수 패리티, '1'삽입 시 홀수 패리티로 각각 변형함으로써 메시지를 삽입하는 방법을 사용하였으며 동일 픽셀 값의 군집에 따라 변형되는 픽셀의 위치를 조정하여 영상의 화질을 제안하는 방법들이 제안되었다^[1~2].

Chan et al.은 가장 많은 연구에서 참조하고 있는 LSB 대체 방법을 제안하였으며 매우 간단하고 정보은닉 용량도 뛰어나지만 삽입되는 데이터의 임의성을 보장할 수 없어 LSB 시각적 공격과 같은 간단한 훼손에 대해서도 정보 검출이 어려우므로 보안성이 높다고 할 수 없었다^[3].

Meilikainen은 두 개의 픽셀 쌍(y_1, y_2)에 2 비트의 비밀메시지(s_1, s_2)를 삽입하기 위해 y_1 의 LSB와 s_1 의 동일 여부에 따라 y_1 또는 y_2 의 값이 stego-pixel(y_1 으로 가정)로 지정되고 stego-pixel(y_1)과 y_2 값의 이진화 연산 결과와 s_2 의 동일성 여부에 y_2 값을 변화시키는 방법이 제안하였다. 이 방법은 픽셀 수만큼의 은닉용량을 가지지만 LSB 반전율이 약 37.5%로 측정되었다^[4].

C. S. Chan은 [4]의 방법을 개선하여 i-1번째 픽셀의 7th MSB와 i번째 픽셀의 LSB와 XOR 연산을 하며 그 결과와 비밀메시지 비트를 비교하여 i번째 픽셀의 LSB를 대체하는 방법을 고안하였다. 이 방법은 비트 반전율 저하에 따른 삽입 효율성이 [4]보다 소폭 증가하였다^[5].

최근 많은 논문들에서 XOR 연산을 이용한 LSB 변형 기반의 방법들을 다루고 있으며 높은 은닉용량과 낮

그림 1. 대칭 키 알고리즘
Fig. 1. Symmetric Key Algorithm.

그림 2. XOR 기반 비밀메시지 은닉 개념

Fig. 2. Concept of XOR Based Secret Message Hiding.

은 화질저하를 동시에 이루기 위한 진보를 거듭하고 있다. C. S. Chan et al.의 논문에서는 커버영상의 연속하는 네 픽셀의 LSB를 데이터 비트라 칭하며 $d_1 \sim d_4$ 명명한다. 또한 그림 2와 같이 $P_1 \sim P_3$ 는 영역 내에 각각 3개의 데이터 비트를 포함하게 된다. 짝수 또는 홀수패리티검사를 가정한 후 P_1 은 d_1, d_4, d_2 의 패리티 비트가 된다. P_1 은 s_1 (Secret bit)으로 대체되고 s_1 은 고정한 채 $\{s_1, d_1, d_4, d_2\}$ 의 패리티검사를 위해 데이터 비트는 변형한다. 이 방법은 4개의 데이터 비트에 3 비트의 비밀메시지를 숨기는 것이 가능하며 [5]의 방법보다 비트 반전율이 감소한다^[6~7].

본 논문에서는 하나의 픽셀 내에서 MSB들을 데이터 비트로 이용하여 발생한 패리티 비트를 통해 정보은닉을 수행하는 알고리즘을 제안하고자 한다. 현재 공개된 많은 방법들은 LSB를 이용하는 Matrix Encoding 또는 2nd LSB를 이용하여 XOR 연산을 수행하는 것이 대부분이나 본 논문에서는 LSB를 제외한 픽셀의 7 MSB(이후 MSBs로 칭함) 전체 또는 일부를 암호화 킷값으로 이용하게 되므로 자기참조를 통해 픽셀 당 1 비트를 숨기는 것이 가능하고 Steganogram의 화질저하(비트 반전률의 최소)가 적게 나타난다.

III. 제안하는 스테가노그래피 기술

기존의 LSB 대체, XOR 기반 LSB변형 방법들이 가진 삽입데이터의 임의성 부족, 비트 반전에 따른 화질저하 등의 단점을 극복하기 위해 본 논문에서는 은닉될 메시지의 시각적 암호화 그리고 비트 반전 최소화를 통한 매개 이미지의 화질개선을 목표로 대칭키 암호의 프로토콜을 정보은닉 기법에 적용하여 알고리즘을 개발하였다.

대칭키 암호화의 개념을 고려해본다면, 이진으로 된

그림 3. 대칭키 암호 프로토콜 요소의 Steganographic 요소화

Fig. 3. Converting Symmetric Key Cryptography Protocol Elements into Steganographic Elements.

그림 4. Proposed Steganography System

Fig. 4. Simple Example of Proposed Steganography System.

평문이 존재할 경우 동일한 길이의 킷값을 XOR(배타적 논리합)연산 하여 암호문을 얻는다. 이 암호문은 다시 킷값과 XOR 연산을 함으로서 원래의 평문을 다시 복구하는 것이 가능하다.

즉, 이 개념을 스테가노그래피에 적용하여 픽셀의 MSBs의 연산 값(패리티비트)은 암호화 킷값으로, 그리고 비밀메시지 1비트는 평문으로 가정하고 XOR 연산을 수행한다. 그 결과 값은 해당 픽셀의 LSB로 대체되고 픽셀은 영상에 저장되어 Stego픽셀이 되며 이 과정은 모든 픽셀에 대해서 적용된다. 수신자는 픽셀의 암호화 킷값인 MSBs의 연산 값(Parity bit)를 구하고 Stego픽셀의 LSB(암호문)과 XOR 연산을 수행한다. 결과 값은 원래의 평문이었던 비밀메시지 비트가 된다.

그림 4는 한 픽셀(픽셀 값: 215)에 대한 예를 설명한 것이며 픽셀에서 연산된 킷 값은 1이며 비밀 메시지 '1' 삽입 시 해당 픽셀의 LSB는 0이 되어 픽셀 값은 214가 되며 비밀 메시지 '0'삽입 시 해당 픽셀의 LSB는 1이 되어 픽셀 값은 215가 된다. 비밀 메시지를 검출하는

그림 5. 제안된 스테가노그래피 시스템
Fig. 5. Proposed Steganography System.

방법은 역순으로 수행이 된다.

그림 5는 대칭키 암호화를 모델로 구성된 제안된 스테가노그래피 시스템이다. 이러한 정보은닉 과정은 영상에서 간략하게 수행될 수 있다.

조건: Parity bit는 Even Parity를 기준으로 한다.

- Step I: 이미지(Cover Image)를 읽는다.
Step II: 좌측 상단부터 우측으로 한 픽셀을 읽는다.
Step III: 선택된 픽셀의 LSB를 Secret Message의 1 bit로 대체한다.
Step IV: 픽셀의 MSBs에 대해 XOR 연산을 수행한다.

IV-1: Parity bit가 0이면 Secret Message의 다음 1 bit를 읽은 다음 Step II로 이동한다.

IV-2: Parity bit가 1이면 해당 픽셀의 LSB의 보수를 취한다.

Step V: Secret Message의 다음 1 bit를 읽은 다음 Step II로 이동한다.

위의 2~5까지 과정을 모든 비밀 메시지열을 다 숨길 때 까지 반복 수행한다. 단 비밀메시지의 길이는 최대 영상의 픽셀 수 만큼이다. 정보검출 과정은 다음과 같

이 진행 된다.

Step I: 이미지(Steganogram)를 읽는다.

Step II: 좌측 상단부터 우측으로 한 픽셀을 읽는다.

Step III: 선택된 픽셀의 MSBs에 대해 XOR 연산을 수행한다.

III-1: Parity bit가 0이면 픽셀의 LSB를 읽어 복원 메시지열에 저장한 다음 Step II로 이동한다.

III-2: Parity bit가 1이면 LSB의 보수를 취하여 Recover Message에 저장하고 StepII로 이동한다.

IV. 정보은닉 실험 및 결과

제안된 알고리즘을 검증하고 평가하기 위해 프로그래밍은 MATLAB Ver 7.2에서 구현되었으며 기존의 방법들과 비교를 통해 제안된 방법의 우수성을 평가하였다. 그림 6은 실험에 쓰인 원본영상으로써 512×512

그림 6. $TI_1 \sim TI_6$ (실험영상)

Fig. 6. $TI_1 \sim TI_6$ (Test Images).

크기의 Lena, F-16, Tank, Neck_MRI, Baboon 그리고 Boat영상을 $TI_1 \sim TI_6$ (Test Image)으로 각각 명명하였다. 기존의 방법들에서는 Lena, Pepper, F-16영상에 대한 실험만 하였으나 본 실험에서는 군사 및 의료분야 등에서의 응용확대를 고려하여 실험영상의 종류를 확대하였다.

원본영상의 MSBs로부터 만들어진 킷값인 PBP (Parity Bit Plane)는 아래 그림 7과 같이 나타나게 된다. 대부분의 PBP들은 원본 영상의 형태와 무관하게 생성되어지며 Neck_MRI, Tank영상은 일부 과도한 저주파 영역들로 인해 PBP에서도 그 윤곽을 보임을 알 수 있다. PBP는 영상의 MSBs들로부터 얻어지므로 이러한 특성은 개연성이 있으며 제안된 알고리즘에서 PBP의 픽셀 값들은 단지 킷값으로만 이용되므로 성능에는 아무런 문제가 없다.

원본 영상들의 LSB Plane들도 PBP영상과 비슷한 형

그림 7. TI_1, TI_2, TI_5, TI_6 (Top-Left), TI_3 (Top-Right), TI_4 (Bottom-Left)의 Parity Bit Plane

Fig. 7. PBP of TI_1, TI_2, TI_5, TI_6 (Top-Left), TI_3 (Top-Right), TI_4 (Bottom-Left).

그림 8. 비밀메시지

Fig. 8. Secret Image.

태로 나타나며 실제 실험에서 LSB가 연산에 포함되지 않으므로 논문에서는 도시하지 않았다.

그림 8의 지도영상은 위성에서 비행장 지역을 촬영한 영상으로 군사목적의 전송이미지로 사용됨을 가정하여 사용하였다. 이 지도 영상은 비밀메시지로 간주되며 그레이영상으로 만들어졌고 크기는 155×155 이다. 기존의 방법들에 쓰인 비밀메시지의 크기를 따랐으며 그 이유는 동일한 환경에서 알고리즘 성능을 비교하기 위함이다.

제안된 알고리즘에 의해 비밀메시지를 삽입한 후 기존의 방법들과 성능비교를 하였다. 비교되는 방법들은 동일한 크기의 비밀메시지를 사용하였으며 모두 은닉된 비밀 메시지를 100%복구한다.

비밀메시지의 크기는 192,200bit이며 은닉 후 LSB의 반전(변형)이 이루어진 픽셀의 수는 TI_1 (Lena)을 사용하였을 때 [5],[6]방법에서 각각 64,254와 63,982회였으며 원본영상의 전체 LSB에 대한 반전율은 24.51%와 24.40%이다. 해당영상에서 제안된 방법은 18.17%의 LSB 반전율을 보임을 알 수 있다. LSB 반전율은 MSE(Mean Square Error)의 크기에 비례하게 된다. 즉, 낮은 LSB 반전율은 높은 영상화질(PSNR)을 제공함을 알 수 있다. 나머지 영상들에 대해서도 근소한 차이를 있지만 Lena영상에서 얻어진 결과와 크게 다르지 않음을 알 수 있다. 표에서 특이하게 Neck_MRI 영상만 낮은 LSB 반전율을 보이나 이것은 원본영상의 저주파영역이 완벽하게 동일한 값들로 이루어져 발생하는 현상으로 이해할 수 있다.

표 1. 알고리즘별 반전 LSB의 수 비교

Table 1. Comparison of The number of Flipping LSB per Each Algorithm.

	Chan's	Chan & Chang's	Proposed		
	반전 LSB수	반전 LSB수	반전 LSB수	반전 LSB %	PSNR
TI_1	64,254	63,982	47,632	18.17	55.54
TI_2	64,372	64,058	47,897	18.27	55.51
TI_3	None	None	48,176	18.37	55.48
TI_4	None	None	38,342	14.62	56.47
TI_5	None	None	50,082	19.1	55.31
TI_6	None	None	45,583	17.38	55.72

그림 9. String 이진 데이터가 삽입된 $TI_1' \sim TI_6'$ 영상
Fig. 9. String Binary Message Embedded $TI_1' \sim TI_6'$ Images.

그림 9에서는 비밀메시지인 지도영상이 은닉된 후의 영상(Steganogram)들을 도시하였다. 화질의 저하를 거의 보이지 않는다.

표 1에서 PSNR을 구하기 위한 연산은 아래와 같다.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \|I(i, j) - I'(i, j)\|^2$$

$$PSNR = 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right)$$

여기서 I 는 원본영상, I' 은 변형된 영상 그리고 m, n 은 각각 영상의 가로, 세로 픽셀 수이다. MAX_I 는 영상의 픽셀이 가질 수 있는 최대의 값이므로 255이다.

그림 10과 같이 변형된 영상(Steganogram)의 LSB는 임의의 패턴으로 나타나는 것을 알 수 있다. 일부 영상에서는 Steganogram MSBs의 형태를 보이기도 하지만 은닉된 비밀메시지에 대한 어떠한 정보도 노출하지 않

그림 10. 비밀영상이 삽입된 $TI_1 \sim TI_6$ Steganogram의 LSB영상

Fig. 10. Secret Message Embedded $TI_1 \sim TI_6$ Steganogram's LSB Images.

음을 확인할 수 있다.

위에서도 설명한 것과 같이 PBP상에서의 형태도출, Steganogram의 LSB에서의 영상형태 도출 등의 특이점이 나타나므로 향후 방법에서는 이러한 현상을 최소화시키는 알고리즘으로 개선되어질 것이다. 물론 알고리즘에 미치는 영향은 없지만 대부분 영상들의 Steganogram LSB에서는 잡음 형태를 보이는 것을 고려한다면 Steganalysis관점을 고려하여 비슷한 패턴을 보이도록 하는 것이 유리할 것으로 판단된다.

본 알고리즘에서는 MSBs의 조합에 의한 Parity Bit를 얻어내 PBP를 구성한다. 은닉정보 검출(Decoding) 단계에서 다른 조합을 통해 얻어진 PBP와 Steganogram의 XOR연산을 통해 얻어낸 결과는 그림 11과 같다. 정확한 PBP(대칭키)값을 가지지 못할 경우 비밀영상의 복원이 어려움을 확인하였다. 대체적으로는 그림 11의 왼쪽 그림과 같이 부정확한 대칭키에 의한 연산결과는 잡음의 형태로 나타남을 실험을 통해 확인

그림 11. 틀린 MSBs 조합을 통한 PBP와 Steganogram LSB(Left: TL_2 , Right: TL_4)의 연산 결과

Fig. 11. Output of Operation between Steganogram LSB(Left: TL_2 , Right: TL_4) and PBP by Incorrect MSBs's Combination.

하였으며 Neck_MRI와 같은 영상에서는 비밀메시지의 일부정보가 보이게 되나 이를 회피하는 방법을 향후 논문에서 제시하는 것이 가능할 것이다.

기밀성(Confidentiality)의 측면에서는 암호화에 사용한 정확한 대칭키를 이용하였을 때만 암호문의 복호화가 가능해야 하므로 제안된 알고리즘은 조건을 만족한다. 무결성(Integrity)의 관점에서 본다면 암호화된 데이터에 변경(제3자에 의한 훼손)이 가해지면 훼손여부를 확인 가능하여야 하며 제안된 방법에서는 Steganogram의 LSB가 변조되었을 때 조건을 만족하게 된다. 원본의 변조에 따른 Randomness를 고려할 때 Steganogram의 LSB는 대부분 잡음형태로 나타나므로 이점 또한 만족한다.

V. 결론 및 향후 연구방향

본 논문에서는 군사, 의료 및 일반영상들에 대해 제안한 알고리즘을 적용하여 정보은닉과 검출을 수행하였다. 제안한 방법은 기존의 방법들보다 LSB의 반전률이 약 6%정도 감소됨을 실험을 통해 보였으며 기존의 알고리즘에 비해 정보은닉 효율성이 높아짐을 알 수 있었다.

제안된 방법에서는 1 bpp(Bits per Pixel)의 정보를 숨겼음에도 불구하고 정보은닉 후 Steganogram의 영상 화질(PSNR)은 55.5dB을 보여 화질저하는 거의 없음을 확인하였다.

LSB 대체 방법은 픽셀 당 1Bit를 숨기는 것이 가능하나 보안성이 매우 낮으며 본 논문에서 참조한 [6]의 방법은 LSB 4개에 3Bit를 숨기므로 픽셀 당 1Bit를 숨

기는 제안된 방법에 비해 은닉률이 25% 낮다.

또한 이전 비밀영상이 잡음의 형태로 삽입되므로 LSB대체 방법 등과는 확연히 다른 임의성을 제공해주므로 높은 보안성을 갖는다고 할 수 있다.

향후 연구에서는 정보은닉용량의 확대방안, 정보은닉 효율성, 화질저하 개선 등의 다각도 성능평가를 기존 방법들과 비교할 예정이다. 또한 일부 Steganogram의 LSB가 영상의 형태를 띠고 있는 점을 개선하는 것이 필요하다.

참 고 문 헌

- [1] M. Venkatesan, P. MeenakshiDevi, K. Duraiswamy, K. Thiagarajah, "A New Data Hiding Scheme with Quality Control for Binary Images Using Block Parity," Third Int'l. Symposium on Information Assurance and Security, 2007.
- [2] J. Y. Byun, K. H. Jung, K. Y. Yoo, "Improved Data Hiding Method by Block Parity for Binary Images", Int'l. Conf. on Computer Science and Software Engineering, 2008.
- [3] C. K. Chan and L. M. Cheng, "Hiding Data in Images by Simple LSB Substitution", Pattern Recognition, vol. 37, no. 3, pp. 469-474, 2004.
- [4] J. Mielikainen, "LSB Matching Revisited", IEEE Signal Processing Letters, vol. 13, no. 5, pp. 835-839, 2010.
- [5] C. S. Chan, "On Using LSB Matching Function for Data Hiding in Pixels", Fundamenta Informaticae, Vol. 96, pp 49-59, 2010.
- [6] C. S. Chan and C. Y. Chang, "Hiding Data in Parity Check Bit", Proc. of Int'l Conf. on Ubiquitous Information Management and Communication, pp 469-474, 2010.
- [7] C. S. Chan and C. Y. Chang, "Hiding Secret in Parity Check Bits by Applying XOR Function", Proc. 9th IEEE Int. Conf. on Cognitive Informatics, pp. 835-839, 2010.
- [8] Rajkumar, Rahul Rishi, Sudhir Barta, "A New Steganography Method for Gray Level Images Using Parity Checker", Int'l. Journal of Computer Applications, Vol. 11 No. 11, 2010.
- [9] 최장희, 윤은준, 유기영, "DC기반의 적응적인 가역 정보은닉기법", 대한전자공학회논문지-CI, 제49권 제2호, pp. 103-114, 2012.

저 자 소 개

최 용 수(정회원)-교신저자
1998년 강원대학교
제어계측공학과 공학사
2000년 강원대학교
제어계측공학과 공학석사
2006년 강원대학교
제어계측공학과 공학박사
2006년~2007년 연세대학교 첨단융합건설연구단
연구교수
2007년~현재 고려대학교 정보보호대학원
연구교수
<주관심분야 : Multimedia Hashing, Information
Hiding, Watermarking, Steganography>

김 형 중(평생회원)
1978년 서울대학교 제어계측공학과 공학사
1986년 서울대학교 제어계측공학과 공학석사
1989년 서울대학교 제어계측공학과 공학박사
1990년~2006 강원대학교 제어계측공학과 교수
2006년~현재 고려대학교 정보보호대학원 교수
<주관심분야 : Parallel Computing, Image
Hashing, Data Compression, Reversible Data
Hiding>

이 달 호(정회원)
1982년 서울대학교
제어계측공학과 공학사
1985년 서울대학교
제어계측공학과 공학석사
1992년 서울대학교
제어계측공학과 공학박사
1992년~현재 가천대학교 전자공학과 교수
<주관심분야 : 시스템 식별, 필터링 기법, INS 응용,
Data Hiding>