The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 4, pp.13-19, Aug. 31, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.4.13
JIIBC 2014-4-3

배타적 논리합을 사용한 DCT 기반의 비밀공유

Secret Sharing based on DCT using XOR

김천식*

Cheonshik Kim*

요 약 일반적으로 회사의 중요한 비밀을 한명이 소유하고 있다면 해킹과 같은 방법에 매우 취약할 수밖에 없다. 이와같은 문제를 해결할 수 있는 방안으로 탄생한 것이 비밀공유이다. 비밀을 중요한 한사람이 아닌 여러 명이 나누어 보관함으로써 한명이 누군가에 의해서 비밀을 도난당하더라도 복구할 수 있다는 개념에서 출발하였다. 즉, 비밀 정보를 도난으로부터 지킬 수 있는 강한 방법으로 비밀공유 방법이 제안되었다. 지금까지의 대부분의 방법은 공간영역에 기반을 둔 방법이었다. 이 방법은 간단한 포맷 변환만으로 쉽게 영상의 변형이 일어나므로 원래 은닉된 데이터가 제거된다. 본 논문에서는 JPG의 DCT 기반에 의해서 비밀을 배타적 논리합에 의해서 분배함으로써 이미지에 대한 공격에 보다 강한 면을 보완하고자 제안 하였다. 실험결과 원본 비밀을 정확해 복구할 수 있음을 실험을 통해서 입증하였다.

Abstract In general, if a secret of company is owned by a person, the secret is the most vulnerable to attack of hacking. Secret sharing is a solution to solve such a problem. To share the secret to many people not one, it is possible to restore secret when the secret is being stolen by someone. That is, secret sharing, a strong method, was proposed to keep secret information from the robbery. Until now, most secret sharing schemes were based on spatial domain. The hidden data based on spatial domain is easily deleted since a transformation of digital formats (i.e., jpeg to bmp or vise versa). In this paper, we proposed our scheme for complement to resist various attack of cover image as distributing secrets based on DCT of JPEG using exclusive-or operation. The result of experiments proved that the proposed scheme restore original secret.

Key Words : Secret Sharing, Cryptographic, DCT, JPEG, XOR

Ⅰ. 서 론

정보 보안 분야를 크기 분류하면 정보 보안과 암호화 프로토콜이다. 암호화 프로토콜은 키 교환이 필수 이며 이를 위한 다양한 연구가 있었고, 비밀 공유는 키 교환을 연구하던 중 발견한 분야로 볼 수 있다[1-3]. 비밀공유는 조직의 정보를 특정 인물이 독점하는 것의 문제점을 어느 정도 해결할 수 있다. 예를 들어 한 사람이 비밀금고(또는 회사의 중요한 기밀)의 키를 갖고 있다고 가정하면, 금고의 안전은 여러 사람이 키를 나누어 가질 경우보다 안전하지 않게 된다. 비밀공유는 이러한 목적으로 활용된다.

1979년 Sharmir[2]는 이와 같은 의문에 적합한 해결방안을 제안했다. 하지만 이 방법이 암호화로서 높은 수준의 안전성과 신뢰성을 제공할 수 없음이 증명되었다. Sharmir가 제안한 비밀 공유 방법은 비밀 공유를 위해서

*종신회원, 안양대학교 디지털미디어공학과
접수일자 : 2014년 6월 18일, 수정완료 : 2014년 7월 18일
게재확정일자 : 2014년 8월 8일

Received: 18 June, 2014 / Revised: 18 July, 2014
Accepted: 8 August, 2014
*Corresponding Author: mipsan@paran.com
Dept. of Digital Medial Engineering, Anyang University, Korea

참가한 참가자가 1명이 없더라도 비밀을 복구할 수 있는 특성을 갖고 있다. 즉, 중요한 정보를 열람해야 하는데 1명이 키를 분실하거나 도둑질을 당해서 키의 일부가 없더라도 복구를 가능하게 하는 특징을 갖고 있다. 만일 해커가 정보 전달에 사용되는 이미지를 탐지한다면 이미지를 훼손해서 비밀 이미지의 기능을 무력화 시킬 것이다. 비밀이미지 공유는 이와 같은 문제를 해결하기 위한 것이다. 이를 위해서 비밀 이미지를 n개의 의미 없는 그림자 이미지로 분리하고 비밀을 저장하여 전달한다.

이 경우 $r(1 \le r \le n)$ 개의 이미지로 원래 이미지를 완성하는 것이 가능하다. r미만의 이미지로는 비밀을 복구할 수 없다. 비밀공유의 개념은 Shamir와 Blakely에 의해서 각각 소개되었다. 이들이 제안한 (r,n)임계 스킴은 중요한 데이터 D를 n개의 데이터로 분할하고 r개 이상의 이미지가 있으면 복구가 가능한 것이다[1]. Noar와 Shamir(1995)[3]는 사람의 시각 시스템에 기반을 둔 비밀 이미지 공유를 위한 시각 암호화라 부르는 암호화 기술을 제안했다. 시각 암호화에서, 메시지를 암호화 하는 방법은 비밀 메시지를 검정색의 2진 픽셀들을 이용하여 투명 용지들에 분산 배치함으로써 가능하다. 반대로 디코딩 할 때는 투명용지를 겹치면 비밀 메시지가 노이즈 이미지 형태로 나타나게 된다[3-5].

시각암호화 방법의 장점은 빠른 디코딩이다. 이미지 용지를 간단히 겹침으로써 간단히 해결되지만 투명용지에는 많은 잡음이미지로 구성되므로 사용자에게 친숙한 면에서 단점이 될 수 있다. 이러한 문제점 때문에 최근에는 비밀 이미지의 공유 방법에 보통의 회색이미지나 컬러 이미지를 기반으로 한 스테가노그라픽 스킴[6-7]을 적용한 방법들이 제안되었다.

본 논문에서는 이미지에 대한 공격에 강한 면을 증가시키기 위해서 JPEG[8]의 DCT 기반에 의한 비밀 공유 방법을 제안 하고자 한다.

II. 관련 연구

1. Shamir의 비밀공유 방법

이 절에서 우리는 비밀 공유[9-17]를 위한 Shamir 스킴을 사용하는 방법을 설명하고자 한다. 이 방법에 따르면 비밀 정수 값 y로부터 비밀 공유 그룹의 참자가 n명에게 n개의 비밀 값을 나누어 준다(수식 1).

$$F(x) = y + m_1 \times x + m_2 \times x^2 + \ldots + m_{k-1} \times x^{k-1} \quad (1)$$

이 방법은 다음과 같은 과정을 따른다.

(a) 선택에 사용되는 k개의 값들은 n보다 작거나 같은 값이다.

(b) $k-1$개의 정수 값 $m_1, m_2, \ldots, m_{k-1}$을 임의로 선택한다.

(c) i번째 비밀공유 참가자의 값 x_i를 선택한다. (x_i의 모든 값은 서로 달라야 한다.)

(d) 선택된 x_i에 대해 수식 (1)을 이용하여 $F(x_i)$를 계산한다.

(e) $(x_i, F(x_i))$의 각 쌍을 비밀 공유로 획득하고 이를 참가자에게 전달한다.

위의 비밀 공유 처리에서 m_i은 보존할 필요가 없다. 다음 비밀 복구과정을 통해서 n개의 비밀공유의 값으로부터 비밀이 복구 되는 과정을 단계적으로 설명한다.

(a) n개로부터 적어도 k 비밀 공유를 수집한다.

$$\begin{aligned} F(x_1) &= y + m_1 \times x_1 + m_2 \times x_1^2 + \ldots + m_{k-1} \times x_1^{k-1}, \quad (2)\\ F(x_2) &= y + m_1 \times x_2 + m_2 \times x_2^2 + \ldots + m_{k-1} \times x_2^{k-1},\\ &\vdots\\ F(x_k) &= y + m_1 \times x_k + m_2 \times x_k^2 + \ldots + m_{k-1} \times x_k^{k-1}. \end{aligned}$$

(b) 랑그랑지 메소드와 같은 다항식 보간법 기술을 사용함으로써 k의 알려지지 않은 $m_1, m_2, \ldots, m_{k-1}$와 y를 계산할 수 있고 $(k-1)$의 다항식 $F(x)$가 다음의 수식과 같이 복구될 수 있다.

$$\begin{aligned} F(x) = {} & F(x_1)\frac{(x-x_2)(x-x_3)\ldots(x-x_k)}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_k)} \\ & + F(x_2)\frac{(x-x_1)(x-x_3)\ldots(x-x_k)}{(x_2-x_1)(x_2-x_3)\ldots(x_2-x_k)} \\ & + \ldots + F(x_k)\frac{(x-x_1)(x-x_2)\ldots(x-x_{k-1})}{(x_k-x_1)(x_k-x_3)\ldots(x_k-x_{k-1})} \end{aligned} \quad (3)$$

(c) 비밀 공유 값 y를 다음과 같이 계산한다.

$$y = (-1)^{k-1}\left[\begin{aligned} & f(x_1)\frac{x_2 x_3 \ldots x_k}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_k)} \\ & + F(x_2)\frac{x_1 x_3 \ldots x_k}{(x_2-x_1)(x_2-x_3)\ldots(x_2-x_k)} + \ldots \\ & + F(x_k)\frac{x_1 x_2 \ldots x_{k-1}}{(x_k-x_1)(x_k-x_2)\ldots(x_k-x_{k-1})} \end{aligned}\right] \quad (4)$$

[예제 1] $(2,3)$임계 시스템에서 비밀공유를 알아본다.

$(2,3)$임계 시스템이므로 공유이미지가 3개의 이미지로 만들어지며 2개 이상의 이미지가 모이면 공유 비밀정보를 복원할 수 있다. 그림 1과 같이 픽셀 값 2와 3을 그

림과 같이 다항식 공식을 만들어서 이미지를 생성한다. 즉, $f(x)=2x+3 \bmod 251$이 된다. 따라서 3개의 노이즈 이미지 $(1,5),(2,7),(3,9)$가 생성된다.

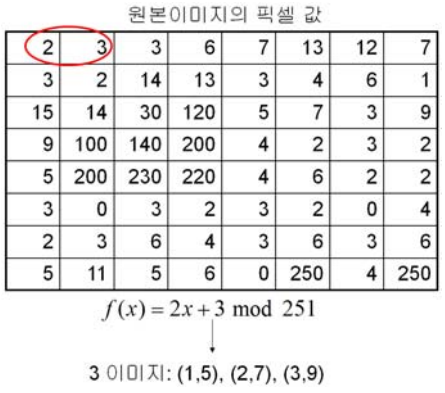

그림 1. (2,3)임계 시스템 계산과정
Fig. 1. computing procedure of (2,3) critical system

다항식에 의한 $(2,3)$임계 시스템으로 생성된 픽셀 값을 그림 2와 같이 분배하여 새로운 이미지를 생성하여 비밀공유에 참가하는 참가자에게 분배한다.

2. DCT (Direct Cosine Transformation) 변환

하나의 화소 입장에서 확률적으로 비슷한 색을 가진 픽셀이 근처에 있을 확률이 높다. 이런 확률적 특성을 이용해서 화면을 분할해서 DCT변환을 하여 데이터를 압축한 것이 JPEG이다. 이제 영상을 8×8의 사각형 행렬로 분할한다. 이 8×8행렬을 블록(block)이라고 부르며 영상 압축의 기본 단위가 된다. JPEG의 압축은 8×8의 블록 행렬을 수학적인 변환 (수식 1)에 의해 가능하다.

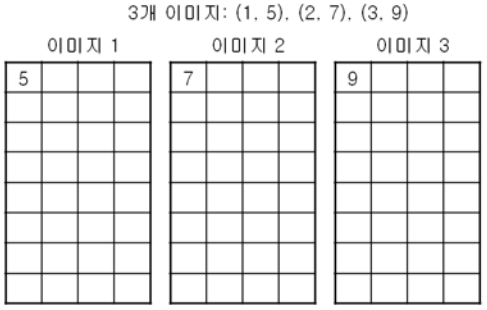

그림 2. (2,3) 임계 시스템에서 이미지 생성과정
Fig. 2. procedure of generating images on (2,3) critical system

이 연산을 하면 왼쪽 위쪽으로 큰 숫자들이 집중된다. 제일 좌측 상단에 있는 큰 숫자를 DC(저주파)값, 나머지 63개의 숫자들은 AC(고주파)값이라고 부른다. 특히 DC 값 및 이 근처에 있는 숫자들은 블록전체의 명도를 결정하는 정보를 담고 있다.

$$F(u,v)=\left(\frac{1}{4}\right)C(u)C(v)\sum_{i=0}^{7}\sum_{j=0}^{7}f(i,j)\cos\left(\frac{(2i+1)u\pi}{16}\right)\cos\left(\frac{(2j+1)v\pi}{16}\right) \quad (5)$$

여기서, $C(x)=\begin{cases}1/\sqrt{2}, & x=0\\ 1, & otherwise\end{cases}$

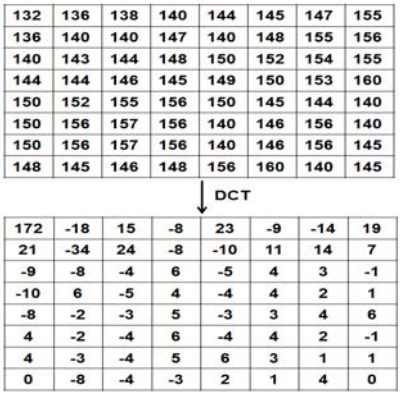

그림 3. DCT 변환 예
Fig. 3. The example of DCT transformation

전체적인 데이터 량을 줄이기 위해 DCT 변환 후 생성된 행렬을 양자화 행렬로 나눈다. 그러면 작은 값 들은 0으로 바꾼다. 이렇게 0이 되어 사라진 숫자들 때문에, 정보손실(loss)이 발생하며 또한 이미지 압축이 된다.

Ⅲ. 제안한 방법

본 장에서는 비밀 공유를 위한 인코딩과 디코딩 알고리즘을 소개하고자 한다.

1. 비밀공유 인코딩

본 절에서 우리는 비밀공유를 위한 스킴을 소개하고자 한다. 우리는 Shamir가 제안한 방법과는 달리 노이즈 이미지를 생성해서 참가자에게 나누어주지 않는다.

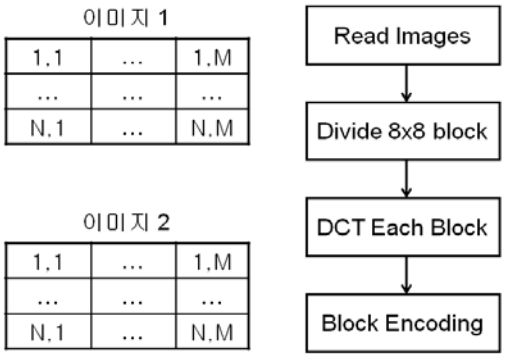

그림 4. 인코딩 과정
Fig. 4. Encoding procedure

그 이유는 노이즈 영상이 결국 어떤 비밀을 포함하는 것과 같은 의심을 심어주기 때문에 자연스러운 회색영상을 사용하고자 한다. 그러므로 우선 참가자에게 나누어 줄 자연스러운 영상 ($C_1, C_2, ..., C_n$)을 선택한다. 즉, N명의 참가자는 서로 다른 커버 영상을 갖는다. 인코딩 과정은 다음의 과정으로 가능하다(그림 4).

[단계 1] 영상 C_1, C_2를 읽은 후 8×8크기로 나누고 나누어진 블록을 Block 함수에 각각 메시지 비트와 함께 전달한다(그림 5).

[단계 2] Block 함수는 각 블록을 DCT 변환 한 후 각 블록이 0 혹은 1을 나타내는지에 대한 정보를 T1과 T2에 저장 한다. M은 T1과 T2에 대한 배타적 논리합이다: M=T1⊕T2.

[단계 3] 비밀 공유 비트 B가 M과 같다면 Q1, Q2는 아무 변화가 없고, 그렇지 않은 경우 다음과 같이 교환한다 (그림 6): SWAP(Q2(3,2), Q2(4,1)).

```
Function Encoding (cover image C1, C2, ....;
                   messages M)
Begin
    Read (C1); Read(C2)
    for i=1:8:xdim,
        for j=1:8:ydim,
            CALL Block1(Bit Mi, C1(8×8), C2(8×8))
          // 함수 Block1 호출 (메시지, 블록1, 블록2)
End
```

그림 5 인코딩 알고리즘
Fig. 5. computing procedure of (2,3) critical system

```
Function Block1 (Bit B; C1, C2)
Begin
    Q1 = DCT(C1); // 블록 C1의 DCT 변환
    Q2 = DCT(C2); // 블록 C2의 DCT 변환
    T1 = Q1(3,2)<Q1(4,1); // Q1의 1/0을 T1에 배정
    T2 = Q2(3,2)<Q2(4,1); // Q2의 1/0을 T2에 배정
    M=T1⊕T2; // T1과 T2의 XOR 결과를 M에 배정
    IF (B = M)  No Change;
    ELSE        SWAP(Q2(3,2), Q2(4,1));
    C1 = IDCT(Q1); // Q1을 역 양자화
    C2 = IDCT(Q2);
    RETURN C1, C2
End
```

그림 6. 인코딩을 위한 블록단위 처리
Fig. 6. block-based encoding process

2. 디코딩 알고리즘

본 절에서 참가자에게 분배된 이미지를 이용하여 은닉된 비밀의 데이터를 복호화 하는 과정을 설명하고자 한다.

```
Function Decoding (cover image C1, C2, ....)
Begin
    Read (C1); Read(C2)
    for i=1:8:xdim,
        for j=1:8:ydim,
            CALL Block2(Bit Mi, C1(8×8), C2(8×8))
            // 함수 Block2 호출 (블록1, 블록2)
End
```

그림 7. 디코딩 알고리즘
Fig. 7. decoding algorithm

그림 7은 디코딩을 위한 메인 함수이고 그림 8은 디코딩을 위한 서브함수 이다. 인코딩과정에서 설명한 부분과 대부분 일치한다. 그림 8과 같이 첫 번째 이미지의 블록에 은닉된 값 T1과 두 번째 블록에 은닉된 값 T2에 대해서 배타적 논리합을 수행하면 간단히 두 블록에 은닉된 값을 복원할 수 있다. 나머지는 이러한 과정을 반복적용 하는 것으로 충분하다.

```
Function Block2 (Bit B; Block C1, C2, ...)
Begin
    Q1 = DCT(C1); // 블록 C1의 DCT 변환
    Q2 = DCT(C2); // 블록 C2의 DCT 변환
    T1 = Q1(3,2)<Q1(4,1); // Q1의 1/0을 T1에 배정
    T2 = Q2(3,2)<Q2(4,1); // Q2의 1/0을 T2에 배정
    M=T1⊕T2; // T1과 T2의 XOR 결과를 M에 배정
    RETURN M;
End
```

그림 8. 디코딩을 위한 블록단위 처리
Fig. 8. block-based decoding process

Ⅳ. 실험 및 결과

본 논문제서 제안한 비밀공유 방법을 평가하기 위해서 우리는 MATLAB 7.0을 사용하여 실험하였다. 실험에 사용한 이미지는 512×512 크기의 256색상의 회색이미지를 사용하였다 (그림 9).

(c) Boat (d) Barbara

(e) Jet(F16) (f) Lena

그림 9. 실험에 사용한 원본이미지
Fig. 9. original image for experiment

제안한 방법은 비밀공유에 참가한 참가자에게 자연스러운 회색이미지를 나누어주기 때문에 이미지의 질(해상도, PSNR)을 평가하는 것은 의미가 있다. 이러한 평가 기준은 데이터 은닉 시스템의 성능을 평가하는데 보편적으로 활용되고 있다. 본 논문에서는 이러한 평가를 보다 객관적으로 증명하기 위해서 PSNR (Peak Signal to Noise Ratio)[18]을 사용한다.

$$PSNR = 10 \times \log_{10}\left(\frac{I_{\max}^2}{MSE}\right) dB \quad (6)$$

즉, 수식(6)에서 MSE는 원본 영상 I와 스테고 영상 I′의 차이 값에 다음 수식 (7)를 적용하였다.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(|I_{i,j} - I'_{i,j}|)^2 \quad (7)$$

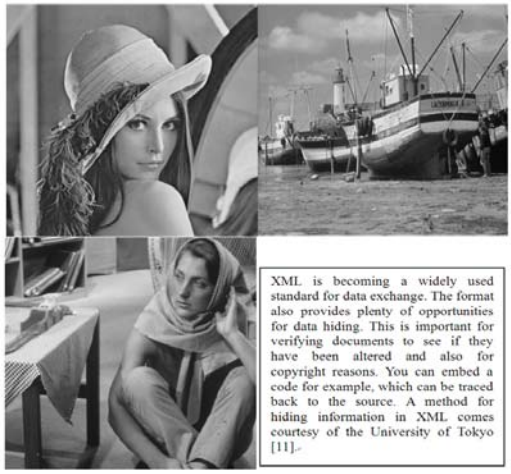

그림 10. 3개의 512x512 커버 이미지와 1개의 비밀 공유 이미지; (a)Lena, (b)Boat, (c)Barbara 그리고 (d)텍스트.
Fig. 10. 3 512x512 cover images and 1 secret sharing image; (a)Lena, (b)Boat, (c)Barbara and (d)text.

여기서 M은 이미지의 폭이고 N는 높이를 의미한다. 수식(6)은 평가에 따라 PSNR이 큰 값일 경우 스테고 이미지가 원본 이미지와 유사함을 나타내고, 반대의 경우 스테고 영상이 원본 영상과 차이가 있음을 나타낸다.

그림 11. 비밀 공유데이터가 커버에 이미지에 은닉된 상태
Fig. 11. shown cover images, embedding secret sharing data.

일반적으로 PSNR이 30dB 이상인 경우 스테고 이미지의 노이즈를 인간의 눈으로 탐지하기 어려움을 의미한다. 그림 10에서 (a)Lena, (b)Boat, 그리고 (c)Barbara는 비밀공유에 사용된 커버이미지들이다. (d)는 비밀 공유되는 메시지를 의미한다.

그림 11은 비밀메시지를 제안한 알고리즘에 따라서 내포한 이미지들이다. 원본 이미지와 비밀을 은닉한 이미지들이 시각적으로 구분하기 어려움을 알 수 있다. 그림 12은 디코딩 알고리즘에 의해서 스테고 이미지에 은닉된 비밀 메시지를 복원한 결과를 보인 것이다.

XML is becoming a widely used standard for data exchange. The format also provides plenty of opportunities for data hiding. This is important for verifying documents to see if they have been altered and also for copyright reasons. You can embed a code for example, which can be traced back to the source. A method for hiding information in XML comes courtesy of the University of Tokyo [11].

그림 12. 복원한 비밀공유 데이터
Fig. 12. restoring secret sharing data.

제안한 방법이 DCT를 기반으로 하고 8×8 블록당 1비트를 저장할 수 있는 방법이기 때문에 최대 4,096 비트를 비밀공유 할 수 있다. 표 1의 실험 결과와 같이 3개의 커버 이미지를 이용한 비밀 공유에서 은닉 데이터가 390 바이트일 경우에 Lena는 45dB, Boat는 43dB 그리고 Barbara는 54dB의 결과를 보였다.

표 1. 제안한 방법의 성능
Table 1. performance of the proposed scheme.

Images (512x512)	Size [byte]	은닉 데이터	PSNR[dB]
Lena	262,144	390 byte	45.5839
Boat	262,144		43.2971
Barbara	262,144		54.2331

V. 결 론

본 논문에 우리는 DCT 기반의 비밀공유 방법을 제안하였다. DCT를 기반으로 하기 때문에 비밀공유 데이터를 이미지로 한다면 다양한 공격에 대해서 강한 성질을 보일 것이다. 또한 전통적으로 비밀공유를 위한 커버이미지를 노이즈 이미지로 사용했었으나 본 논문에서는 친밀감과 공격자의 의심을 감소시킬 수 있는 장점을 갖고 있는 자연친화적인 회색 이미지를 사용하였다. 실험결과에서 보듯이 비밀공유가 성공적으로 복원됨을 알 수 있다. 따라서 향후 비밀공유가 필요한 다양한 응용에 활용될 수 있을 것으로 기대한다.

References

[1] Blakley, G.R., 1979. Safeguarding cryptographic keys. In: Proc. AFIPS National Computer Conf., vol. 48, pp. 313 - 317.

[2] Shamir, A., 1979. How to share a secret. Comm. ACM 22 (11), 612 - 613.

[3] Naor, M., Shamir, A., 1995. Visual Cryptography. Advances in Cryptology: Eurocrypt'94. Spring-Verlag, Berlin. pp. 1 - 12.

[4] Chen, T.H., Tsao, K.H., 2009. Visual secret sharing by random grids revisited. Pattern Recognition 42 (9), 2203 - 2217.

[5] Shamir, A., Naor, M., 1996. Visual cryptography II: Improving the contrast via the cover base. Security Comm. Networks, 16 - 17.

[6] Lin, C.C., Tsai, W.H., 2004. Secret image sharing with steganography and authentication. J. Syst. Software 73 (3), 405 - 414.

[7] Yang, C.N., Chen, T.S., Yu, K.H., Wang, C.C., 2007. Improvements of image sharing with steganography and authentication. J. Syst. Software 80 (7), 1070 - 1076.

[8] Beimel, A., Chor, B., 1998. Secret sharing with public reconstruction. IEEE Trans. Inform. Theory 44 (5), 1887 - 1896.

[9] Park, Y. B., Park, J. I., 2002. A Study on the Cipher JPEG Img,Journal of the Korea Academia-Industrial cooperation Society, vol.3, no.4, pp.308-312, 2002.

[10] Chang, C.C., Lin, C.C., Lin, C.H., Chen, Y.H., 2008. A novel secret image sharing scheme in

color images using small shadow images. Inform. Sci. 178 (11), 2433 - 2447.

[11] Chang, C.C., Hsieh, Y.P., Lin, C.H., 2008. Sharing secrets in stego images with authentication. Pattern Recognition 41 (10), 3130 - 3137.

[12] Lin, P.Y., Lee, J.S., Chang, C.C., 2009. Distortion-free secret image sharing mechanism using modulus operator. Pattern Recognition 42 (5), 886 - 895.

[13] Thien, C.C., Lin, J.C., 2002. Secret image sharing. Comput. Graphics 26 (1), 765 - 770.

[14] Wang, R.Z., Su, C.H., 2006. Secret image sharing with smaller shadow images. Pattern Recognition Lett. 27 (6), 551 - 555.

[15] Wang, D., Zhang, L., Ma, N., Li, X., 2007. Two secret sharing schemes based on Boolean operations. Pattern Recognition 40 (10), 2776 - 2785.

[16] Kim, C., 2013. (2, 2) Secret Sharing Using Data Hiding and Multiplexer Technique, The Journal of The Institute of Internet, Broadcasting and Communication, vol.13, no.4, pp.75-81.

[17] Wu, Y.S., Thien, C.C., Lin, J.C., 2004. Sharing and hiding secret images with size constraint. Pattern Recognition 37 (7), 1377 - 1385.

[18] Kim, C., 2014. Data hiding by an improved exploiting modification direction, Multimedia Tools and Applications, vol.69, no.3, pp 569-584.

저자 소개

김 천 식 (종신회원)

- 1997년 : 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학석사)
- 2003년 : 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학박사)
- 2010년 ~ 2012년 : 세종대학교 교수
- 2013년 ~ 현재 : 안양대학교 교수
- 2007년 ~ 2009년 : 대한전자공학회 컴퓨터소사이어티 멀티미디어 분과위원장
- 2012년 : TACT 영문 저널 - 위원
- 2012년 : UMAS 워크샵 프로그램 의장
- 2013년 : GPC 2013 프로그램 의장
- 2014년 : FutureTech 2014 프로그램 의장

<주관심분야 : 데이터베이스, 데이터마이닝, Steganography, 영상처리, e-Learning>