http://dx.doi.org/10.7236/JIIBC.2013.13.4.75
JIIBC 2013-4-11

데이터 은닉과 멀티플렉서 기법을 이용한 (2, 2) 비밀 공유방법

(2, 2) Secret Sharing Using Data Hiding and Multiplexer Technique

김천식*

Cheonshik Kim

요 약 본 논문은 회색(Gray-scale) 이미지를 기반으로 (2, 2) 비밀 공유(Secret Sharing) 계획을 제안한다. 일반적으로 비밀 공유 방법은 비밀 이미지를 두개이상의 이미지 (그림자 이미지: Shadow Image)로 분배한 후, 그림자 이미지를 참가자(비밀 공유하는 사람)에게 나누어준다. 이 후 참가자들이 비밀을 보기위해 $k(k<n)$명이 모여서 이미지를 투명 용지에 프린트 한 후 이미지를 순서대로 쌓으면 비밀이 잡음이미지 (Noise Image)로 드러난다. 본 논문에서 제안하는 비밀 공유 계획은 데이터 은익과 멀티플렉서 (Multiplexer)를 활용하여 비밀을 두 개의 자연 친화적인 이미지(256 회색영상)에 분배한다. 비밀을 은닉한 이미지는 두 명의 참가자에게 분배한다. 제안한 비밀 공유방법(Scheme)은 스테가노그래피(Steganographic)의 장점을 갖고 있기 때문에 공격자의 공격에 쉽게 노출되지 않는다. 실험결과는 제안한 방법이 확실하며 성능 면에서 높은 성능을 보임을 입증하였다.

Abstract We presents a novel (2, 2) secret sharing (SS) scheme for all grayscale images. Generally, a secret image is distribute more than two shadow images, which are dealt out among participants. In order to find out secret image, participants print shadow images to transparent papers. Then, a secret image will appear as stacking transparent papers. The secret sharing scheme in this paper distribute secret image into natural grayscale images using multiplexer and data hiding scheme. After then, two participant have two shadow images respectively. The merit of the proposed scheme is that shadow images have small loss in aspect of the quality with steganographic features. Therefore, the proposed secret sharing scheme in this paper is not easily detected by attackers. The experiment result verified that the proposed scheme, obviously outperforms previous SS schemes.

Key words : Secret Sharing, Cryptography, LSB, Multiplexer, Steganographic

Ⅰ. 서 론

Liu 등은 "7명의 과학자가 하나의 비밀 프로젝트를 수행할 경우에서 비밀 유지 및 프로젝트"에 관련한 정보 유출과 관련해서 비밀을 유지할 수 있는 방법에 관한 문제를 제기하였다. 즉, 과학자들은 비밀문서를 비밀 보관함에 보관하며, 문서를 함께 열람하지 않을 경우에 보관함에 열쇠를 이용하여 봉인하기로 했고, 문서를 열람하고자 하는 경우 6명 이상이 참석하는 경우로 한정하였다. 이 경우 필요로 하는 잠금 장치와 열쇠의 수는 몇 개나

*종신회원, 안양대학교 디지털미디어공학과
접수일자: 2013년 7월 8일, 수정완료: 2013년 8월 8일
게재확정일자: 2013년 8월 16일

Received : 8 July, 2013 / Revised : 8 August, 2013 / Accepted : 16 August, 2013
*Corresponding Author: mipsan@paran.com
Dept. of Digital Media Eng., Anyang University, Korea

필요할까?[1]

이와 같은 문제에 대해서 처음으로 일반화를 시도한 사람은 Adi Shamir였다. Shamir는 (k,n) 계획을 제안하여 Liu 등이 제시한 문제의 해결 방안을 제안하였다[2]. 이와 같은 비밀이 필요한 문서나 이미지는 군사, 의료, 공공기관, 산업기밀 등 거의 모든 곳에 존재한다. 이러한 기밀정보가 하나의 문서로 존재할 경우 이 문서가 도난 되거나 복사되는 등의 부작용이 존재한다. 이와 같은 문제점을 해결하기 위해서 비밀문서를 n명의 참가자에게 분배해서 보관하도록 하고, $k < n$명이 참가 하면 비밀을 열람할 수 있도록 하자는 방법이 Shamir의 방법이다. 이 방법은 많은 계산 시간이 요구된다[2]. Thien[3]등은 이 문제를 해결하기 위해서 잡음(noise) 이미지를 만들어서 참가자들에게 비밀정보를 공유할 수 있는 방법을 제안하였다[4,5,6,7,8,9].

반면에 다른 연구자들은 비밀을 재구성하기 전에 참가자가 믿을만한 참가자인지 확인하기위해서 이미지에 인증 코드를 추가하였다[10,11,12,20,21].

비밀공유 계획은 다음의 방법으로 성능을 평가할 수 있다:

(1) 비밀성, (2) 정확한 비밀정보 복원, (3) 계산속도, (4) 공간요구 유무(픽셀 확장).

모든 계획은 비밀 보호되어야 하며 정확하게 비밀 이미지를 복원할 수 있어야만 한다. 전통적인 방법인 비시각 비밀공유[7,13,14,15,16,17]방법은 많은 계산시간이 요구된다. 시각 비밀 공유방법은 비밀 이미지의 복원에 사람의 시각 시스템을 이용하며, 계산시간은 전혀 필요 없다. Chang 등[4,5,10]과 Yang 등[12]은 공격자들로 부터의 탐지를 피하기 위해서 이미지에 비밀정보와 인증코드를 함께 은닉하였다. 2009년에 Chang 등이 제안한 (2,2) 계획은 인증 가능한 공유 기법을 제안 하였다[18]. 이 방법은 공격자들로부터 비밀을 지키고 정직한 참가자들을 확인할 수 있는 방법이다.

본 논문에서는 (2,2) 비밀 공유 계획을 제안하였다. 제안한 계획은 정직한 참가자가 비밀 이미지 복원을 입증할 수 있다. 또한, 전통적인 비밀공유 방법보다 계산시간이 적게 요구된다. 실험결과 제안한 계획은 4가지의 기본적인 요구 조건인 비밀성, 정확성, 계산시간 등에서 만족스러운 결과를 보였다. 비밀 공유에 사용된 이미지는 일반적으로 잡음 이미지를 사용하나, 이는 공격자(Attacker)에게 공격 목표가 될 수 있다. 그러므로 본 논문에서는 회색(gray) 이미지를 사용하였다.

본 논문은 구성은 Ⅱ장에서 기본적인 비밀공유의 방법을 설명하며, Ⅲ장에서는 비밀 이미지를 두 개의 이미지에 분배하는 방법과 복호화 알고리즘을 제안한다. Ⅳ장에서는 제안한 방법에 대해서 실험결과를 보인다. Ⅴ장에서 결론과 함께 앞으로의 연구 방향을 제시한다.

Ⅱ. 관련 연구

1. 비밀 공유

1979년 Shamir[1]는 다항식 보간법에 기초해서 (t,n) 임계 계획을 제안하였다. Shamir의 계획은 데이터 SD가 n개의 조각인 SD_1, SD_2, ..., SD_n으로 나누어지고, SD의 $t\,(t \le n)$ 개의조각으로 원래의 비밀 데이터 SD를 복원하는 것이 가능하다.

$t-1$개의 조각으로는 비밀 정보를 복원할 수 없는 특성이 있다.

이 경우 SD는 정수로 가정한다. Shamir의 계획에서, 소수(prime number) P는 난수로 선택되며, 다항식 보간 공유 함수는 수식 (1)의 정의와 같고 SD를 n개로 나눈다.

$$f(x) = a_0 + a_1 x^1 + a_2 x^2 + \ldots + a_{t-1} x^{t-1} (\mathrm{mod}\, P) \quad (1)$$

수식 (1)에서, 각각 $a_1, a_2, \ldots, a_{t-1}$은 무작위 수(random number), $a_0 = SD$, 이고 $a_0 < P$이다. 각 이미지 SD_i^n는 수식 (2)에 의해서 유도할 수 있다.

$$SD_i = f(i) \quad (2)$$

수식 (2)에서, $i = 1$에서 n까지 이고, 각 SD_1, SD_2,..., SD_n은 이미지로서 간주한다. SD를 복원하기 위해서, t또는 그 이상의 SD_i들이 이용된다. 다항식 보간법 함수 $f(x)$는 라그랑지 보간법 수식으로부터 유도될 수 있고, 비밀 데이터 $SD = a_0 = f(0)$가 최종적으로 유도 될 수 있다.

2. 시각 비밀공유

Naor와 Shamir가 제안한 해결방안은 단순하지만, 계

산 없이 비밀공유를 허용하는 보안방법이다. 이와 같은 계획을 시각 암호화 계획 (Visual Cryptography Scheme: VCS) 이라고 한다. 시각 암호화 계획은 다음의 과정으로 만들어진다. 즉, 비밀 이미지는 흑과 백의 비트맵 픽셀들로 구성된다. 비밀을 암호화하는데, 원본 이미지는 n개의 잡음 이미지로 나누어지며, 각 픽셀은 m개의 흑과 백의 부분 픽셀로 나누어진다. 비밀을 복호화 하는데, n개의 잡음 이미지 중 부분 이미지들 S를 선택하고 이를 투명용지에 출력한다. 이후, 투명용지를 순서 없이 정확하게 맞추어 쌓으면 비밀이 복호화 된다.

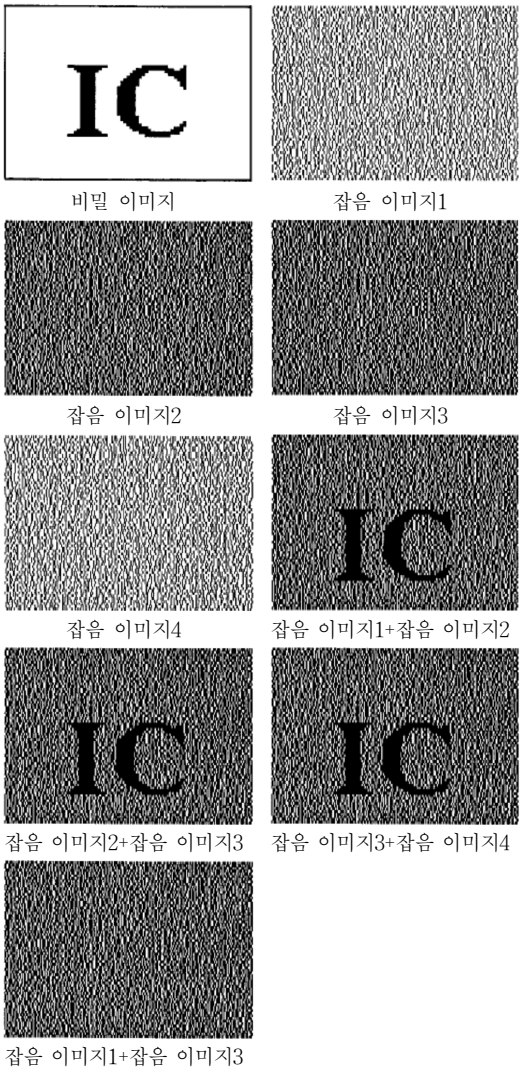


그림 1. 시각 비밀공유[19]
Fig. 1. Visual secret sharing

그림 1은 비밀공유의 예를 보인 것이다. 비밀 이미지 문자를 "IC"로 가정하고, 4개의 잡음 이미지로 분배한다. 잡음 이미지의 집합은 $S=\{1,2,3,4\}$로 가정한다. S의 다음과 같은 조합으로 복호화가 가능하다.

R = {{1,2}, {2,3}, {3,4}, {1,2,3}, {1,2,4}, {1,3,4}, {2,3,4}, {1,2,3,4}}

원본 비밀이미지는 단순히 k개의 잡음 이미지를 쌓는 것으로 비밀을 복호화 할 수 있다.

Ⅲ. 제안 방법

1. 멀티플렉서 (Multiplexer, mux)

멀티플렉서는 데이터입력과 선택입력(제어입력)을 가지고 있다. 제어입력(select)은 들어오는 n개의 입력 중 하나를 선택하는 기능을 한다.

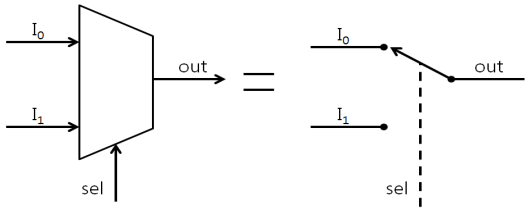


그림 2. 2-to-1 멀티플렉서
Fig. 2. 2-to-1 Multiplexer

그림 2에서 sel이 '0'이면 out에 I_0값이 출력되고, sel이 '1'이면 out으로 I_1값이 출력된다. 입력이 2개이고 출력이 1개이므로 멀티플렉서를 2-to-1 멀티플렉서라 한다. 수식(3)은 (그림 3)을 수식으로 나타낸 것이다.

$$out = (I_0 \bullet \overline{s}) + (I_1 \bullet s) \tag{3}$$

그림 3에서의 I와 s는 각각 수식(3)의 I와 s와 같다. 즉, $s=(s_0,s_1)$ 이다. 그림 3은 비밀 공유를 위해 사용되는 이미지의 픽셀 구조를 설명하기 위한 것이다. LSB는 I이고 두 번째 LSB는 s를 의미한다.

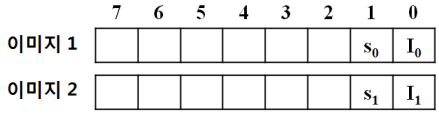


그림 3. 공유 이미지의 픽셀(pixel) 구조
Fig. 3. Pixel structure of sharing image

2. 비밀공유 부호화(Encoding) 알고리즘

이 절에서는 비밀 이미지를 두 개의 이미지에 분산 은닉하는 설계를 제안한다.

사용자 친화적인 2개의 공유 이미지(SI)를 생성하기 위해 $N \times M$ 픽셀(pixel)로 이루어진 2개의 이미지 (C_1, C_2)와 숨겨져야 할 비밀 이미지(SI)를 각각 선택한다. 선택된 2개의 이미지(C_1, C_2)에 이미지(SI)를 감추는 과정은 다음의 5단계로 수행된다.

단계 1: 이미지 $C=\{C_1, C_2\}$와 비밀 이미지 SI를 선택한다. cnt변수는 비밀이미지의 픽셀 개수만큼 반복하기 위한 제어변수로 초기 값은 1이다.

단계 2: C에서 각 (i,j)번째 픽셀 값을 수식(4)에 적용하여 수식 (3)의 s의 값을 구한다. s는 멀티플렉서 sel 그림 2에 해당한다.

$$s = (s_0 \in (C_{11}^{\,n}) \oplus s_1 \in (C_{21}^{\,n})) \qquad (4)$$

단계 3: s의 값을 이용하여 (I_0, I_1)값 중 하나를 선택한다. 수식 (5)는 s의 값이 '0'이면 I_0를 선택하고, s의 값이 '1'이면 I_1를 선택하도록 한다.

$$out = \begin{cases} I_0, & \text{if}(s=0) \\ I_1, & \text{if}(s=1) \end{cases} \qquad (5)$$

단계 4: SI는 비밀 이미지이고 ss는 비밀 이미지의 한 픽셀 (이진 이미지)이다. 이때, out과 비밀 이미지의 한 픽셀 값 ss가 같으면 픽셀은 그대로 둔다. 반면에, 만일 out과 비밀 이미지의 한 픽셀 값 ss가 일치하지 않는 경우, I에 $\bar{I}$를 배정하며, 규칙은 수식 (7)과 같다.

$$\begin{cases} no\ change, & \text{if}(out = ss \in (SI_1^n)) \\ \bar{I}, & else \end{cases} \qquad (6)$$

$cnt = cnt + 1$을 수행한다.

$$out = \begin{cases} \overline{I_0}, & \text{if}(s=0) \\ \overline{I_1}, & \text{if}(s=1) \end{cases} \qquad (7)$$

(a) Baboon (b) Barbara (c) Boat (d) Goldhill (e) Jet(F16) (f) Lena (g) Pepper (h) Tiffany (i) Zelda

그림 4. 실험 이미지들 (256 회색 이미지)
Fig. 4. Experimental images (256 gray-scale image)

단계 5: SI의 모든 비밀 이미지의 픽셀에 대해서 이미지 C에 분배를 완료할 때까지 단계2에서 단계4까지를 반복하여 처리 한다.

3. 비밀공유 복호화 알고리즘

단계 1: 비밀이 포함된 공유 이미지 $SC=\{SC_1, SC_2\}$를 선택한다.

단계 2: SC에서 각 (i,j)번째 픽셀 값을 수식 (8)에 적용하여 s의 값을 구한다.

$$s=(s_0 \in (SC_{11}^{\ n}) \oplus s_1 \in (SC_{21}^{\ n})) \qquad (8)$$

단계 3: s의 값을 수식 (5)에 적용하여 out의 값을 구한다. out을 수식 (9)에 반복 적용하여 SI를 복구할 수 있다.

$$SI_{i,j}= SI_{i,j}+out \qquad (9)$$

단계 4: $cnt=cnt-1$을 실행하고, cnt가 0이 될 때까지 단계2와 단계3을 반복 적용한다.

Ⅳ. 실험 및 결과

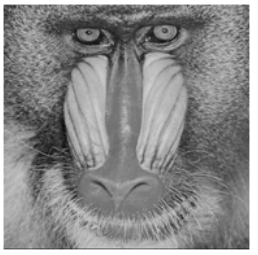
본 장에서는 제안한 사용자 친화적인 (2, 2) 비밀 분산 방법을 실험한다. 실험은 Windows 7 운용체제 환경이며 개발 툴은 매트랩 7.0으로 구현하였다. 그림 4는 비밀 분산 방법을 위해 사용된 이미지들이다. 대부분의 시각 비밀분산 방법은 잡음 이미지를 사용한다. 하지만, 본 논문에서 공격자들의 의심을 피하기 위해 사용자 친화적인 회색 이미지를 사용하였다.

예제 1. 그림 5는 제안한 (2, 2) 계획의 응용을 보인 것이다. 이때 사용된 이미지는 512×512의 Boat, Baboon, 그리고 Barbara 이미지이다. (a)는 비밀 공유이미지의 원본이고, (b)와 (c)는 커버(Cover) 이미지이고, (d)는 복원 이미지이다. 또한, (a)와 (d)는 이진 비트맵 이미지이고, (b)와 (c)는 256 회색 이미지이다.

그림 6에서 (a), (b), (f), 그리고 (g)는 이미지들이다. (d)와 (h)는 이진 비트맵 이미지이다. (e)와 (i)는 각각의 복원한 비밀 이미지이다.

비밀 정보가 탐지 되지 않으려면 기본적으로 이미지가 잡음이 없어야 공격자들로부터 의심을 받지 않는다. 이와 같이 잡음을 객관적으로 측정하기 위해서, PSNR (Peek Signal To Noise Rate)을 사용하여 공유 이미지 (CI)와 비밀 정보를 포함한 이미지(SCI)의 픽셀 값 차이를 계산하였다. PSNR을 구할 때, M×N 크기의 두 이미지 사이의 차이 값을 누적하는 MSE(Mean Squared Error)를 통하여 쉽게 계산할 수 있다. PSNR과 MSE은 수식 (10)과 (11)과 같다.

(a) Boat - SI (비밀 이미지) (원본)



(b) Baboon - C_1

(c) Barbara - C_2

(d) Boat - SI (복원된 이미지)

그림 5. (2, 2) 비밀 공유 예제
Fig. 5. (2, 2) secret sharing example

PSNR은 주관적인 평가요인(예, 사람의 시각에 의한 평가)의 문제점을 해결하기 위해서 객관적인 측정도구로 활용되고 있다. 그렇기 때문에, PSNR은 이미지의 질을 평가하는데 가장 보편적으로 사용되는 측정 방법이다.

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

수식 (10)에서 MSE는 원본 이미지 I와 SCI 이미지 I'의 차이 값이다. MSE의 정의는 수식 (11)과 같다.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(|I_{i,j} - I'_{i,j}|)^2 \qquad (11)$$

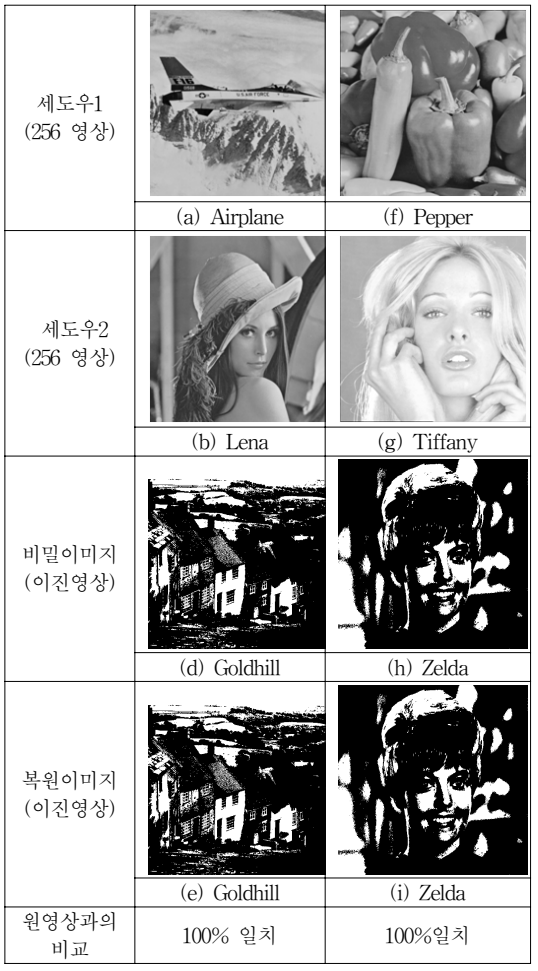


그림 6. (2, 2) 비밀 공유 비교
Fig. 6. (2, 2) comparison of secret sharing

수식 (10)과 (11)의 평가에 따라서, PSNR이 큰 경우 이미지가 원본 이미지와 가까운 것을 의미한다. 반대로, PSNR이 작을 경우, 원본과 유사하지 않음을 의미한다. 일반적으로 PSNR이 30dB를 넘을 때, 이미지의 왜곡은 시각으로는 탐지되기 어려움을 의미한다.

표 1은 제안한 방법의 실험 결과 이미지의 시각적인 질(Quality)을 보여준다. PSNR이 54dB 이상임을 알 수 있다. 그러므로 본 논문에서 제안한 방법은 공격자에게 쉽게 노출되지 않는 방법임을 알 수 있다.

V. 결 론

본 논문에서는 (2, 2) 비밀 공유 방법을 제안하였다. 제안한 방법에서 멀티플렉서를 활용하여 비밀 이미지를 2개의 이미지에 분배하는 처리를 하였다. 이 방법은 스테가노그래피 특성을 갖고 있어서 이미지의 질이 높은 편에 속한다. 기존의 이미지는 잡음 이미지들에 비밀정보(이미지)를 은닉했었다. 하지만, 잡음 이미지는 공격자의 공격 목표가 되기 쉬운 문제점이 있다. 그런 문제점을 해결하기 위해서 256 회색 이미지를 사용하였고, 실험결과 높은 이미지의 질을 확인할 수 있었다. 향후 (n,n)방법으로 확장할 수 있는 방법을 찾을 계획이다.

표 1. 실험결과의 이미지의 질 평가
Table 1. evaluation of image quality in experimental result

공유 이미지				비밀영상 (이진영상)
이미지1	PSNR	이미지2	PSNR	
Baboon	54.1544	Barbara	54.1460	Boat
Airplane	54.1454	Lena	54.1513	Goldhill
Pepper	54.1398	Tiffany	54.1848	Zelda
평균	54.1465	평균	54.1607	

References

[1] A. Shamir, "How to share a secret," Communications of the Association for Computing Machinery, pp.612 - 613, 1979.

[2] Moni Naor, Adi Shamir: "Visual Cryptography," EUROCRYPT, pp.1-12, 1994.

[3] C.C. Thien, J.C. Lin, "Secret image sharing," Computers and Graphics, vol. 26, no. 1, pp. 765 - 770, 2002.

[4] C.C. Chang, C.C. Lin, C.H. Lin, Y.H. Chen, "A novel secret image sharing scheme in color images using small shadow images," Information Sciences, vol. 178, no.11, pp.2433 - 2447, 2008.

[5] C.C. Chang, C.Y. Lin, C.S. Tseng, "Secret image

hiding and sharing based on the (t,n)-threshold," Fundamenta Informaticae, vol. 76, no. 4, pp.399 - 411, 2007.

[6] J.B. Feng, H.C. Wu, C.S. Tsai, Y.P. Chu, "A new multi-secret images sharing scheme using Lagrange's interpolation," Journal of Systems and Software, vol. 76, no. 3, pp. 327 - 339, 2005.

[7] S.J. Shyu, S.Y. Huang, Y.K. Lee, R.Z. Wang, K. Chen, "Sharing multiple secrets in visual cryptography," Pattern Recognition, vol. 40, no. 12, pp. 3633 - 3651, 2007.

[8] D.S. Tsai, G. Horng, Z.H. Chen, Y.T. Huang, "A novel secret image sharing scheme for true-color images with size constraint," Information Sciences, vol. 179, no. 19, pp.3247 - 3254, 2009.

[9] C.S. Tsai, C.C. Chang, T.S. Chen, "Sharing multiple secrets in digital images," Journal of Systems and Software, vol. 64, no. 2, pp.163 - 170, 2002.

[10] C.C. Chang, Y.P. Hsieh, C.H. Lin, "Sharing secrets in stego images with authentication," Pattern Recognition, vol.141, no.10, pp.3130 - 3137, 2008.

[11] C.C. Lin, W.H. Tsai, "Secret image sharing with steganography and authentication," Journal of Systems and Software, vol.73, no.3, pp. 405-414, 2004

[12] C.N. Yang, T.S. Chen, K.H. Yu, C.C. Wang, "Improvements of image sharing with steganography and authentication," Journal of Systems and Software, vol.80, no.7, pp.1070-1076, 2007.

[13] Y.F. Chen, Y.K. Chan, C.C. Huang, M.H. Tsai, Y.P. Chu, "A multiple-level visual secret-sharing scheme without image size expansion," Information Sciences, vol. 177, no. 21, pp.4696-4710, 2007.

[14] W.P. Fang, "Friendly progressive visual secret sharing," Pattern Recognition, vol. 41, no. 4, pp. 2008.

[15] D.C. Lou, H.K. Tso, J.L. Liu, "A copyright protection scheme for digital images using visual cryptography technique," Computer Standards and Interfaces, vol. 29, pp.125 - 131, 2007.

[16] R. Lukac, K.N. Plataniotis, "Bit-level based secret sharing for image encryption," Pattern Recognition, vol. 38, no. 5, pp.767 - 772, 2005.

[17] M. Naor, A. Shamir, "Visual cryptography," in: Advances in Cryptology-EuroCrypt'94, LNCS, Springer, Berlin, vol. 950, pp.1-2, 1995.

[18] Chin-Chen Chang, Chia-Chen Lin, T. Hoang Ngan Le, Hoai Bac Le: "Sharing a verifiable secret image using two shadows," Pattern Recognition, vol. 42, no.11, pp. 3097-3114, 2009.

[19] J. Cai, A Short Survey On Visual Cryptography Schemes, 2004, Available: http://www.cs.toronto.edu/~jcai/paper.pdf

[20] J.K. Moon, J.M. Kim, H.R. Kim, A Secure Authentication Protocol for Cloud Services, Journal of Advanced Information Technology and Convergence, vol.1, no.2, pp.33-36, 2011.

[21] J.K. Baek, J.P. Park, A Study on Personal Information Control and Security in Printed Matter, Journal of the Korea Academia Industrial, vol.14, no.5, pp.2415-2421, 2013.

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

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