사용자 친화적인 시각 비밀 분산 방법
(User Friendly Visual Secret Sharing Scheme)

윤 은 준 † 이 길 제 ††
(EunJun Yoon) (GilJe Lee)
유 기 영 †††
(KeeYoung Yoo)

요 약 본 논문에서는 이진 이미지 기반의 간단하고 사용자 친화적인 (n,n) 시각 비밀 분산 방법을 제안한다. 제안한 방법은 간단한 XOR 연산과 NOT 연산만을 이용하여 사용자 친화적인 이미지들 내에 숨기고자 하는 비밀 이미지 정보를 분산해서 숨기는 기법으로, 효율적인 숨김(embedding)과 복원(reconstruction) 알고리즘 제공, 비밀 이미지의 손실없는 완벽한 복원 기능 제공, 사용자 친화적인 의미있는 이미지들을 공유함으로써 자신이 속해있는 그룹을 쉽게 구분할 수 있는 기능 제공, 그리고 기존의 방법과 달리 원본 커버 이미지와 같은 크기의 비밀 이미지를 공유할 수 있는 등의 시각 비밀 분산 방법이 갖추어야하는 많은 장점들을 가진다.

키워드 : 시각 비밀 분산 방법, 정보은닉, 멀티미디어 보안, 스테가노그라피, 정보보호

Abstract In this paper, we propose a simple and user friendly visual secret sharing scheme based on binary image. The proposed scheme is a new information hiding method which uses only bit-wise exclusive-or (XOR) operation and NOT operation to share a secret binary image information in the user friendly binary images. The proposed scheme has the following merits: (1) It provides efficient embedding and reconstruction algorithms. (2) It provides lossless and perfect reconstruction of the secret binary image. (3) It provides the detection method of its own group by sharing the user friendly image. (4) It can share same sized secret image such as original cover image unlike previous methods.

Key words : Visual secret sharing, Information hiding, Multimedia security, Steganography, Information security

· 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음(IITA-2008-C1090-0801-0026)
· 본 논문은 2007 한국정보과학회 학술심포지움에서 '이진 이미지 기반의 간단한 친화적인 (n,n) 시각 비밀 분산 방법'의 제목으로 발표된 논문을 확장한 것임

† 정 회 원 : 대구산업정보대학 컴퓨터정보계열
ejyoon@tpic.ac.kr
†† 학생회원 : 경북대학교 컴퓨터공학과
vilelkj@purple.knu.ac.kr
††† 종신회원 : 경북대학교 컴퓨터공학과 교수
yook@knu.ac.kr

논문접수 : 2008년 2월 4일
심사완료 : 2008년 3월 26일

정보과학회논문지: 컴퓨팅의 실제 및 레터 제14권 제5호(2008.7)

1. 서 론

최근 디지털 멀티미디어와 인터넷 기술의 급속한 발달로 인하여 인터넷 또는 웹상으로의 중요한 기밀문서 및 개인의 프라이버시(privacy)를 손상시킬 수 있는 개인정보의 유출이 심각한 문제로 대두되고 있다. 이러한 문제점을 해결하기 위해 정보보호(information security) 기술은 최근 중요한 사회적 이슈가 되고 있으며, 이를 계기로 새로운 보안 및 암호 기술 개발에 많은 연구자들이 역점을 두고 있다. 특히, 다양한 멀티미디어 저작물에 관한 디지털 저작권 관리와 도래하는 유비쿼터스 환경에서의 개인의 프라이버시 보호 및 안전한 통신을 보장하기 위해 최근 스테가노그라피(steganography)가 중요한 연구 분야로 대두되고 있다[1-10].

메시지를 은밀하게 전송하기 위한 방법으로 사용되는 스테가노그라피 기법은 회사비밀정보, 군사기밀정보, 외교정책기밀정보 등을 은밀하게 교환하고자 할 때 유용하게 사용되어질 수 있다[1]. 스테가노그라피 기법들 중 최근에 이미지 공유(image sharing)에 관한 연구가 많은 연구자들에 의해 다양하게 제안되었다. 지금까지 알려진 이미지 공유에 관한 대표적인 기법으로 시각 암호화(VC: visual cryptography)[1-3,8-10]기법들과 다항식(polynomial)[4-7] 연산을 사용하는 기법들이 제안되어져 오고 있다. 특히, VC는 1994년에 Naor와 Shamir에 의해 최초로 제안되었다. VC의 장점은 빠른 복원(decoding) 기능과 완벽한 암호문 생성을 제공하는 것이다. 이에 VC는 다중 비밀 분산 방법(multi secret sharing scheme) 등으로 현재 광범위하게 연구되어지고 있다.

다양한 VC 기법 중에서도 n개의 이미지에 비밀 정보를 숨기고 n개 중 k개의 이미지만 있어도 비밀 정보가 확인이 되는 시각 비밀 분산 방법(visual secret sharing scheme)[1-3]이 최근 많이 연구되고 있다. 하지만 현재까지 알려진 대부분의 비밀 분산 방법들은 공유 이미지 크기의 확장 문제, 사용자 친화적이지 못한 의미없는 분산 이미지 공유 문제, 다항식 등과 같은 복잡한 연산을 수행해야 하는 문제 등을 가지고 있다[4-7].

본 논문에서는 위와 같은 단점을 해결한 이진 이미지 기반의 간단하고 사용자 친화적인 (n,n) 시각 비밀 분산

방법을 제안한다. 제안한 방법에서는 간단한 배타적논리합(XOR) 연산과 NOT 연산만을 이용하여 사용자 친화적인 이진 이미지들에 숨기고자 하는 비밀 이진 이미지 정보를 분산해서 숨기는 기법이다. 이 방법은 시각 비밀 분산 방법이 갖추어야하는 많은 장점들을 가진다. 특히 제안한 방법은 공유 되는 사용자의 수가 증가하면 할수록 공유 이미지의 사용자 친화성은 더욱 높아지는 장점을 가지므로 그룹 키 생성(group key agreement)과 같은 많은 사용자들이 필요로 하는 환경 등에 실용적으로 사용될 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 시각 암호화 기법과 Naor와 Shamir의 (k,n) 시각 비밀 분산 방법을 소개하며, 3장에서이진 이미지 기반의 간단한 사용자 친화적인 (n,n) 시각 비밀 분산 방법을 제안하며, 4장에서 그 실험 결과를 분석한다. 마지막으로 5장에서 결론을 도출한다.

2. 관련 연구

본 장에서는 관련연구로 제안한 방법에 적용되는 시각 암호화(VC) 기법[1-3,8-10]과 Naor와 Shamir가 제안한 (k,n) 시각 비밀 분산 방법[5]에 관해 간단히 설명한다.

2.1 시각 암호화(Visual Cryptography)

시각 암호화는 비밀 공유 기법으로 가장 중요한 특징은 완벽한 암호화와 인간 시각에 의해 바로 메시지를 복호화 할 수 있는 장점에 있다. 1979년에 Shamir의 Sharing 방법은 $q \geq n+1$인 GF(q)상의 라그란쥐 보간법(Lagrange interpolation)에 기반한 (k,n) 비밀 분산 방법을 제안하여 비밀 분산 방법의 기틀을 마련하였다[4].

1994년에 Naor와 Shamir[5]에 의해 최초로 시각 분산 방법이 제안되었으며, 그들이 제안한 (k,n) 비밀 분산 방법은 n명에게 공유 데이타를 나누었을 때 k명 이상이 모여야만 숨겨진 비밀 정보를 복원 할 수 있다[5-7]. VC의 가장 큰 장점은 인간의 시각체계(human visual system)를 이용하여 복잡한 연산 없이 분산한 이미지를 쉽게 복원할 수 있다[8,9,10]. 최근까지 Naor와 Shamir의 (k,n) 비밀 분산 방법을 기반으로 한 다양한 시각 암호화 기법들이 [1-3,8-10] 논문 등을 통해 제안되어져 오고 있다.

2.2 Naor와 Shamir의 (k,n) 시각 비밀 분산 방법

Naor와 Shamir가 제안한 (k,n) 시각 비밀 분산 방법은 n명에게 공유 이미지 데이타를 나누었을 때 k명 이상이 모여서 그들의 공유 이미지 데이타를 서로 겹침(stacking)하여서 숨겨진 비밀 이미지 정보를 복원하는 방법이다.

그림 1은 Naor와 Shamir가 제안한 몇가지 아주 간단한 패턴(pattern)들을 가진 블록(block)들을 사용한 흑백 비밀 이미지(black-and-white secret image) 조각으로 구성된 (k,n) 시각 비밀 분산 방법의 간단한 디자인 예를 보여준다. 그림 1에서 보여주는 것과 같이, 비밀 이미지의 각 픽셀(pixel)은 투명무늬(transparency)의 비밀분산-1에서의 2×2 블록과 투명무늬의 비밀분산-2에서의 또 다른 2×2 블록으로 생성되어진다. 흑(black) 또는 백(white)을 의미하는 픽셀의 밝기(brightness)와 관련된 2×2 블록들의 쌍(pair)은 비밀분산-1과 비밀분산-2내의 대응되는 위치를 그려주기 위해, 해당 픽셀이 흑 또는 백인지 여부에 따라 비밀 이미지의 모든 픽셀에 대하여 무작위(random)로 선택되어진다. 한 예로, 그림 1에서 만약 주어진 비밀 픽셀이 백이면 2열의 비밀분산-1의 2×2 블록들 가운데 하나와 이에 대응되는 3열의 비밀분산-2의 2×2 블록이 선택되어 져서 겹침(stacking)을 수행하여 4행의 백 픽셀을 복원하게 된다. 만약 주어진 픽셀이 흑이면 3열의 비밀분산-1의 2×2 블록들 가운데 하나와 이에 대응되는 3열의 비밀분산-2의 2×2 블록이 선택되어 져서 겹침을 수행하여 4행의 흑 픽셀을 복원하게 된다.

다시 말해, 비밀분산-1과 비밀분산-2의 두 블록들을 겹치면 그림 1의 4행에서 보여지는 것과 같이 대응되는 2×2 블록을 산출하게 된다. 명확한 것은, 만약 2×2 겹침된 블록내의 모든 4개의 요소들이 흑이면, 비밀 이미지의 입력 픽셀은 흑 픽셀(black pixel)임을 쉽게 알 수 있게 된다. 반대로 만약 겹침된 블록 결과내의 모든 4개의 요소들 중 2개의 요소만 흑이면, 비밀 이미지의 입력 픽셀은 백 픽셀(white pixel)임을 쉽게 알 수 있게 된다. 즉, 복원된 이미지 결과는 원본 비밀 이미지를 쉽게 역추적(trace back)하는데 이용되어 질 수 있다.

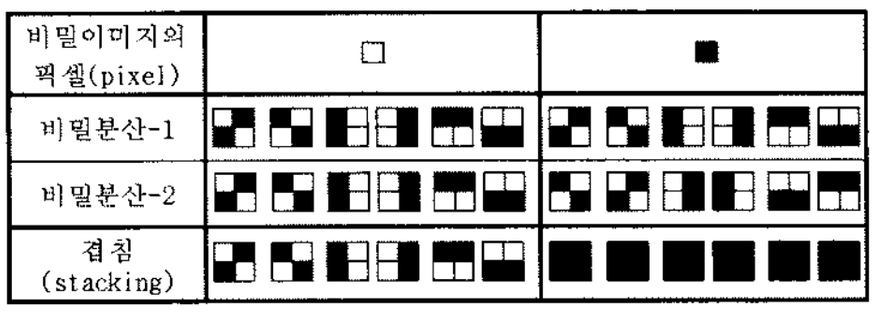

그림 1 Naor와 Shamir의 시각 비밀 분산 방법

3. 사용자 친화적인 시각 비밀 분산 방법

본 장에서는 이진 이미지 기반의 배타적논리합(XOR) 연산과 NOT 연산을 이용한 사용자 친화적인 (n,n) 시각 비밀 분산 방법을 제안한다. 제안한 방법은 숨김 단계와 복원 단계의 두 단계로 구성되어 진다.

3.1 숨김(embedding) 단계

그림 2는 제안한 숨김 단계의 흐름도를 보여준다. 제안한 숨김 단계에서는 (n,n) 시각 비밀 분산 방법을 위해 n명의 사용자들에게 각각 나누어 줄 사용자 친화적

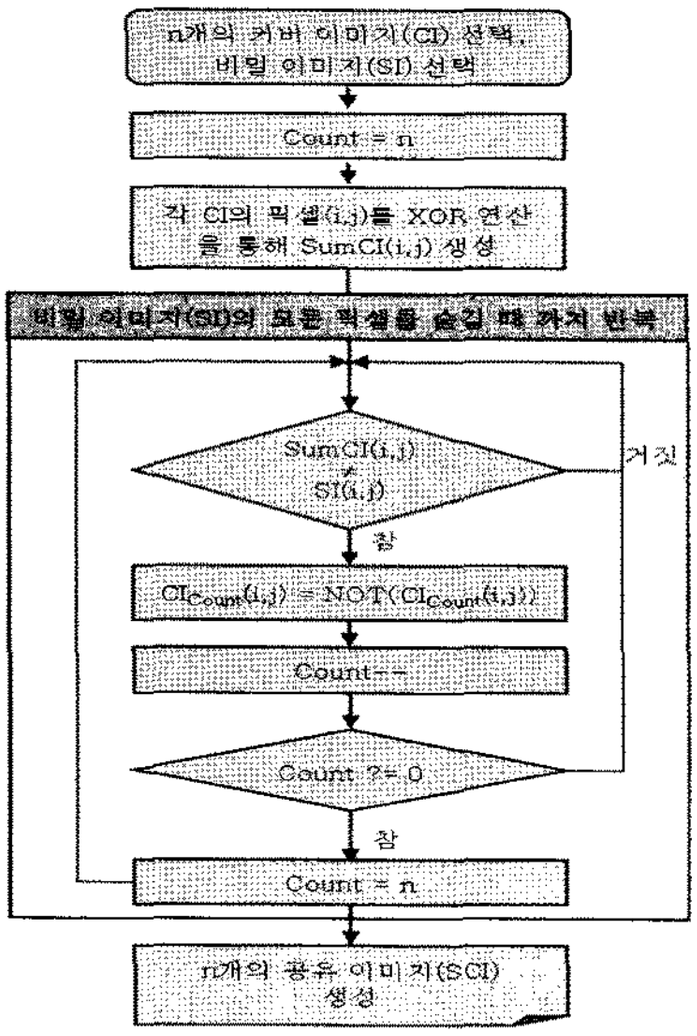

그림 2 숨김(Embedding) 단계

인 n개의 공유 이미지(SCI)를 생성하기 위해 $N\times M$ 픽셀(pixel)로 이루어진 n개의 이진 커버 이미지(CI_1, CI_2, …, CI_n)와 공유 및 분산 숨겨져야 할 비밀 이진 이미지(SI)를 각각 선택한다. 선택된 n개의 이진 커버 이미지(CI_1, CI_2, …, CI_n)에 비밀 이진 이미지(SI)를 숨기는 과정은 다음의 5단계로 수행된다.

숨김 알고리즘:

단계 1. $CI = \{CI_1, CI_2, \cdots, CI_n\}$와 SI를 선택한다.

단계 2. 전제 CI의 개수를 의미하는 n을 Count에 저장한다.

단계 3. n개의 CI에서 각 (i,j)번째 픽셀 값을 아래의 식 (1) XOR 연산을 수행하여 모든 SumCI (i,j)값을 구한다. $(0\leq i<N,\ 0\leq i<M)$

$$SumCI(i,j) = CI_1(i,j)\oplus CI_2(i,j)\oplus\cdots\oplus CI_n(i,j) \quad (1)$$

단계 4. 각 SumCI(i,j)번째 픽셀 값과 각 SI(i,j)번째 픽셀 값을 비교하여 두 픽셀 값이 같으면 숨기고자 하는 비밀 SI(i,j)번째 픽셀 값이 이미 숨겨진 효과를 가짐으로 SumCI$(i+1,j+1)$번째 픽셀 값과 SI$(i+1,j+1)$번째 픽셀 값을 이용하여 단계 4를 다시 수행한다. 만약 두 값이 같지 않으면 CI_{Count} (i,j)번째 픽셀 값의 NOT 연산(예:1이면 0, 0이면 1로)을 수행한 픽셀 값을 해당 $CI_{Count}(i,j)$ 위치에 대체하여 비밀 픽셀 값이 숨겨지게 하고 Count를 1씩 감소시킨다. 이때 만약 이진 커버 이미지(CI)의 개수를 의미하는 Count가 0이 되면 Count의 값을 다시 n으로 초기화하여, 모든 커버 이미지에 고르게 비밀 픽셀 값이 숨겨지게 조절 해준다.

단계 5. 비밀 이진 이미지(SI)의 $(N\times M)$ 픽셀 값까지 모두 숨길 수 있도록 단계 4를 반복 수행하여 n개의 사용자 친화적인 공유 이미지(share image) $SCI = \{SCI_1, SCI_2, \cdots, SCI_n\}$들을 생성한다.

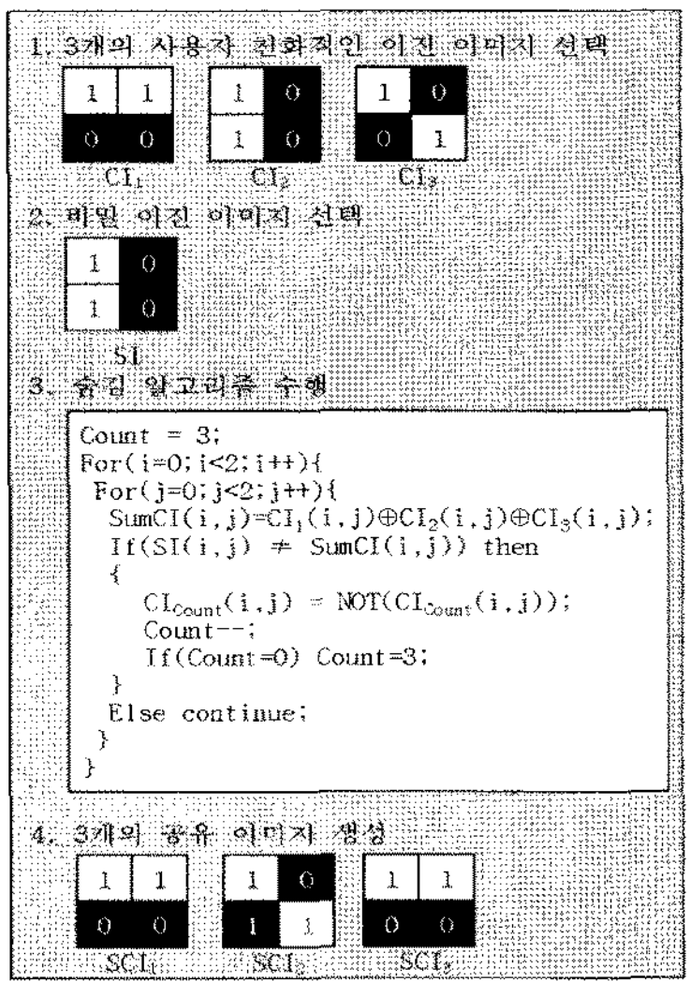

그림 3 (3,3) 시각 비밀 분산 방법에서의 숨김 알고리즘을 수행한 예

위 숨김 단계에서 생성된 $SCI = \{SCI_1, SCI_2, \cdots, SCI_n\}$는 최종적으로 n명의 공유자들에게 1개씩 배분된다. 그림 3은 위의 숨김 알고리즘 과정을 (3,3) 시각 비밀 분산 방법에 적용한 예를 보여준다.

3.2 복원(reconstructing) 단계

그림 4는 제안한 복원 단계의 흐름도를 보여준다. 제안한 복원 단계에서는 (n,n) 시각 비밀 분산 방법을 위해 n명에게 공유되어진 n개의 공유 이진 이미지 $SCI = \{SCI_1, SCI_2, \cdots, SCI_n\}$으로부터 숨겨진 비밀 이진 이미지 SI를 복원해 내는 방법은 다음의 2단계로 구성된 복원 알고리즘을 수행하여 간단하게 복원되어 진다.

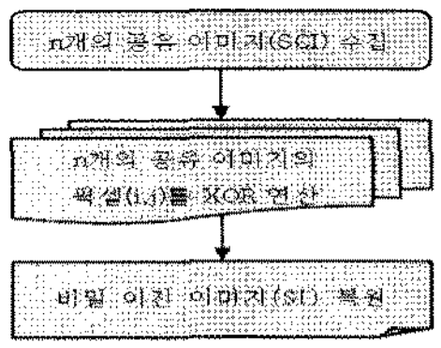

그림 4 복원(Reconstructing) 단계

복원 알고리즘:

단계 1. n명의 사용자들로부터 n개의 공유 이진 이미지 $SCI = \{SCI_1, SCI_2, \cdots, SCI_n\}$을 모두 수집한다.

단계 2. n개의 SCI에서 각 (i,j)번째 픽셀 값을 아래의 식 (2) XOR 연산을 수행하여 겹침 과정을 통하여 모든 숨겨진 비밀 이진 이미지 SI(i,j)번째 픽셀 값을 구한다. $(0\leq i<N,\ 0\leq i<M)$

$$SI(i,j) = SCI_1(i,j) \oplus SCI_2(i,j) \oplus \cdots \oplus SCI_n(i,j) \quad (2)$$

그림 5는 위의 복원 알고리즘 과정을 (3,3) 시각 비밀 분산 방법에 적용한 예를 보여준다. 그림 5에서 보여지는 것과 같이 숨김 단계에서 숨겨진 비밀 이미지 SI의 모든 픽셀 값들이 간단한 XOR 연산을 통해 완벽히 복원 추출됨을 알 수 있다.

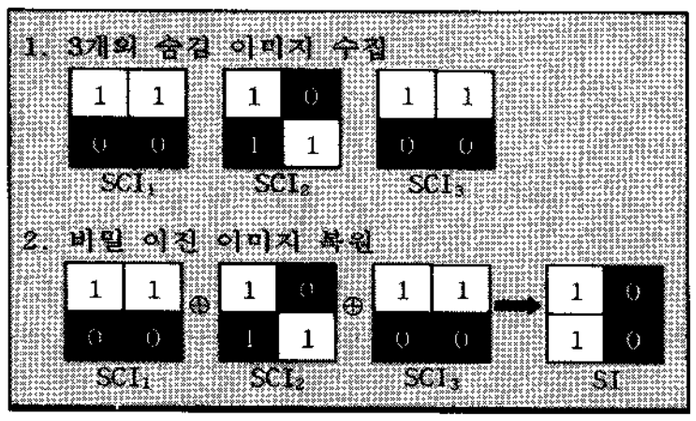

그림 5 (3,3) 시각 비밀 분산 방법에서의 복원 알고리즘을 수행한 예

4. 실험 결과 및 분석

본 장에서는 제안한 사용자 친화적인 (n,n) 시각 비밀 분산 방법의 실험 결과들을 살펴보며 이를 분석한다. 본 실험은 Pentium 4 CPU 2.80GHz 컴퓨터 환경에 개발 툴은 Visual C++ 6.0으로 구현하였다. 또한 (n,n) 시각 비밀 분산 방법 중 두 가지 실험 결과로 (3,3) 시각 비밀 분산 방법과 (7,7) 시각 비밀 분산 방법에 대한 실험 결과를 각각 보인다.

4.1 사용자 친화적인 (3,3) 시각 비밀 분산 방법의 예

그림 6은 (3,3) 시각 비밀 분산 방법을 위해 사용된 이진 이미지들을 보여준다. (a),(b),(c)는 비밀 이미지가 숨겨지게 될 3개의 이진 커버 이미지 CI를 의미하며, (d)는 비밀 이진 이미지 SI를 의미한다.

그림 7은 제안한 숨김 알고리즘을 수행하여 SI를 숨김 처리를 했을 때의 SI가 숨겨진 3개의 공유 이미지 SCI를 보여준다. 그림 7에서 알 수 있듯이 제안한 방법은 기존의 방법과는 달리 공유된 이미지들이 시각적으로 의미있는 형태를 보임으로 사용자 친화적인 성질을 보장할 수 있다.

그림 8은 그림 7의 공유 이미지 SCI를 이용하여 제안한 복원 알고리즘을 수행한 결과를 보여주며, 결과로서 알 수 있듯이 그림 6의 (d) 비밀 이진 이미지 SI가 완벽히 복원되었다.

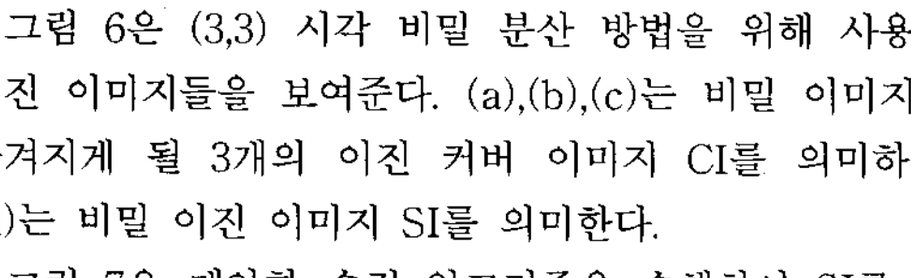

그림 6 256×256 크기의 3개의 CI인 (a),(b),(c)와 비밀 이미지 SI인 (d)

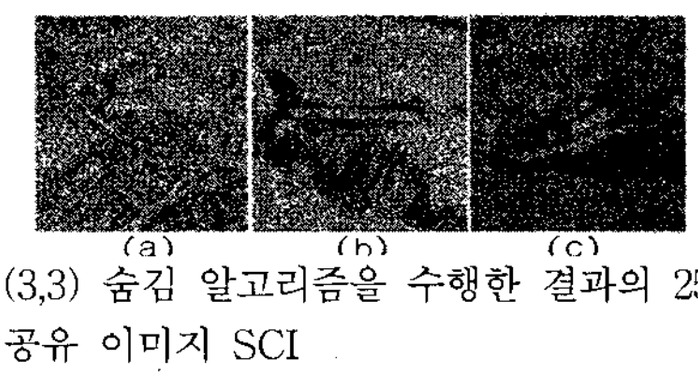

그림 7 (3,3) 숨김 알고리즘을 수행한 결과의 256×256의 공유 이미지 SCI

그림 8 (3,3) 복원 알고리즘 수행 후 얻은 256×256의 비밀 이미지

4.2 사용자 친화적인 (7,7) 시각 비밀 분산 방법의 예

그림 9는 (7,7) 시각 비밀 분산 방법을 위해 사용된 이미지들을 보여준다. (a)~(g)는 비밀 이미지가 숨겨지게 될 7개의 이진 이미지 CI를 의미하며, (h)는 비밀 이진 이미지 SI를 의미한다.

그림 10은 숨김 알고리즘을 수행하여 SI를 숨김 처리하였을 때의 SI가 숨겨진 7개의 공유 이미지 SCI를 보여준다. 그림 10에서 알 수 있듯이 위 (3,3) 시각 비밀 분산 방법에 비해 공유된 이미지들의 선명도 높아져 더욱 사용자 친화적인 속성을 가짐을 알 수 있다. 즉, 제안한 방법은 n값이 크면 클수록 사용자 친화적인 속성 즉 공유 이미지들이 시각적으로 더욱 의미있는 형태를 가지게 됨을 알 수 있다.

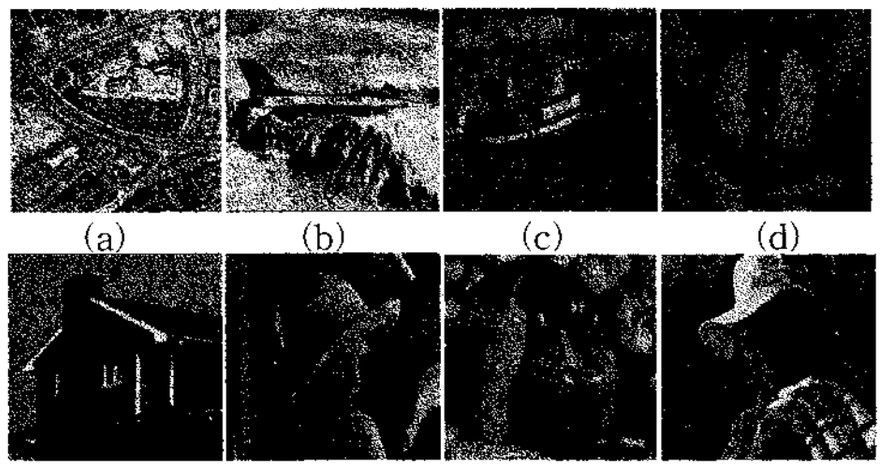

그림 9 256×256 크기의 7개의 CI인 (a)~(c)와 비밀 이미지 SI인 (h)

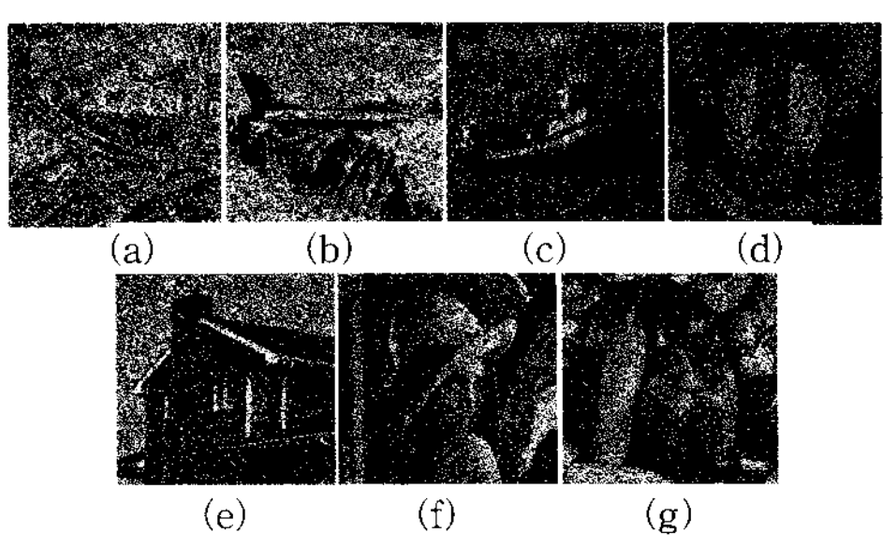

그림 10 (7,7) 숨김 알고리즘을 수행한 결과의 256×256의 공유 이미지 SCI

그림 11 (7,7) 복원 알고리즘 수행 후 얻은 256×256의 비밀 이미지

그림 11은 그림 10의 공유 이미지 'SCI를 이용하여 제안한 복원 알고리즘을 수행한 결과를 보여주며, 결과로서 알 수 있듯이 그림 9의 (h) 비밀 이미지 SI가 완벽히 복원되었다.

4.3 PSNR을 이용한 이미지 노이즈 측정

본 논문에서는 원본 이진 커버 이미지(CI)와 숨김 처리된 공유 이진 이미지(SCI)의 이미지의 픽셀 값 차이, 즉, 노이즈를 측정하기 위해 PSNR(Peek Signal To Noise Rate)을 사용하였다. PSNR은 두 이미지의 노이즈 차이를 사람이 알 수 있는 측정치로 표현한 것으로, PSNR을 구할 때, $M \times N$ 크기의 두 이미지 사이의 차이를 누적하는 MSE(Mean Squared Error)를 통하여 쉽게 계산할 수 있다. MSE와 PSNR은 수식 (3)과 (4)로 각각 표현되어 진다.

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(|CI(i,j) - SCI(i,j)|)^2 \qquad (3)$$

$$PSNR = 10 \times \log_{10}\left(\frac{MAX_C^2}{MSE}\right) \qquad (4)$$

원본 이진 커버 이미지(CI)와 제안한 숨김 알고리즘을 수행하여 숨김 처리된 공유 이진 이미지(SCI) 이미지의 PSNR 측정 결과 값은 표 1과 같으며, 그림 12의 그래프에서 알 수 있듯이 공유하는 이미지가 많을수록

표 1 PSNR 실험 결과 표

	(2,2) 시각비밀 분산스킴	(3,3) 시각비밀 분산스킴	(5,5) 시각비밀 분산스킴	(7,7) 시각비밀 분산스킴
PSNR	54.04	55.94	58.13	59.59

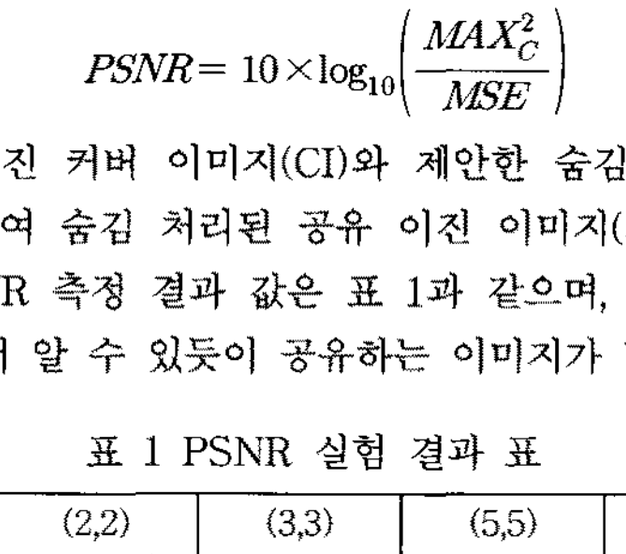

그림 12 n값의 증가에 따른 PSNR 측정 결과 그래프

즉 공유 사용자 수가 증가할수록 각 공유 이미지의 PSNR은 더욱 좋아짐을 확인할 수 있다.

5. 결론 및 향후연구

본 논문에서는 간단한 배타적논리합(XOR) 연산과 NOT 연산을 이용하여 사용자 친화적인 이미지들 내에 숨기고자 하는 비밀 이미지 정보를 분산해서 숨기는 이진 이미지 기반의 간단하고 사용자 친화적인 (n,n) 시각 비밀 분산 방법을 제안하였다. 제안한 방법은 다음과 같은 장점들을 가짐을 보였다. (1) 효율적인 숨김과 복원 알고리즘 제공. (2) 비밀 이미지의 손실없는 완벽한 복원 제공. (3) 사용자 친화적인 의미있는 이미지들을 공유함으로써 자신이 속해있는 그룹을 쉽게 구분 가능. (4) 원본 공유 이미지와 같은 크기의 비밀 이미지 공유 가능.

향후 연구로써는 이진 이미지 외에 그레이 이미지, 컬러 이미지, 동영상 등 다양한 멀티미디어 데이타에 응용 가능한 방법을 개발하는 데 목적을 둔다.

참 고 문 헌

[1] K. Curran, K. Bailey, "An evaluation of image based steganography method," International Journal of digital Evidence, Vol.2, pp. 1-40, 2003.

[2] D. Wang, L. Zhanga, N. Maa, X. Lib, "Two secret sharing schemes based on boolean operations," Pattern Recognition Society, Vol.40, No.10, pp. 2776-2785, Oct. 2007.

[3] W.P. Fang, "Friendly progressive visual secret sharing," Pattern Recognition Society, Vol.41, No.4, pp. 1410-1414, Apr. 2008.

[4] A. Shamir, "How to share a secret," Comm. of the ACM, Vol.22. No.1, pp. 612-613, Nov. 1979.

[5] M. Naor, A. Shamir, "Visual cryptography," Advances in Cryptology-EUROCRYPT'94, LNCS Springer Verlag, Vol.950, pp. 1-12, May. 1994.

[6] C.C. Thien, J.C. Lin, "Secret image sharing," Computers & Graphics, Vol.26. pp. 765-770, May. 2002.

[7] J.B. Feng, H.C. Wu, C.S. Tsai, Y.P. Chu, "A new multi-secret images sharing scheme using larg-range's interpolation," Journal of Systems & Software, Vol.76. No.3, pp. 327-339, Mar. 2005.

[8] T. Hofmeister, M. Krause, H.U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," Theoretical Computer Science, Vol.240, No.2, pp. 471-485, June 2000.

[9] C. Blundo, A. De Santis, D.R. Stinson, "On the contrast in visual cryptography schemes," Journal of Cryptology, Vol.12, pp. 261-289, Apr. 1999.

[10] C. Blundo, A. De Bonis, A. De Santis, "Improved schemes for visual cryptography," Design, Codes, and Cryptography, Vol.24, No.3, pp. 255-278, Mar. 2001.