시각암호의 확장과 디지털 워터마크에 응용

이혜주† · 박지환†

요 약

본 논문에서는 인간의 시각에 의해 비밀 정보를 간단히 복호할 수 있는 시각암호를 이용하여 하드 카피 화상에 기밀정보를 분산시키는 기법에 대하여 고찰한다. 농도 패턴법에 의해 구성된 슬라이드를 시각암호의 관점에서 보면 해밍 가중치가 다르기 때문에 각 슬라이드는 원 화상의 형태를 유지하게 된다. 따라서, 슬라이드의 중첩에 의하여 분산된 기밀정보를 복원할 수 있을 뿐만이 아니라 원 화상의 정보를 유지할 수 있는 이점을 갖게된다. 본 논문에서는 하드 카피 화상에 기밀정보를 합성하기 위해 고안된 ONM(Oka-Nakamura-Matsui) 방식을 확장하여 복수의 원 화상에 기밀정보를 분산시키는 방식을 제안한다. 그 결과, 저작자의 검증용 화상과 배포된 복수의 화상의 중첩만으로 저작권을 식별할 수 있는 디지털 워터마크에 응용할 수 있음을 보인다.

An Extension of Visual Cryptography and Its Application into Digital Watermark

Hye-Joo Lee†, Ji-Hwan Park†

ABSTRACT

In this paper, we consider the method which a secret information is distributed in hard-copied image using visual cryptography that the secret can be identifying simply by human eyes. If slides constructed by patterning, which is one of dithering method, are considered from the viewpoint of visual cryptography, each slides will maintain the shape of original image because these slides have different Hamming weights. Therefore, this method has the advantage that information distributed into slides by stacking them can decode and the shape about the original image can be keeping as well. In this paper, we propose the method which shares the secret information into multiple original images by extension of ONM (Oka-Nakamura-Matsui) method which is devised to embed a secret information on hard-copied image. As a result, this proposed method is applicable to digital watermark because the copyright of image can be identified by stacking an image of owner for verification and the distributed multiple images.

1. 서 론

컴퓨터 네트워크의 발달로 인하여 신속한 정보의 교환과 더불어 정보 보안의 필요성이 증대되고 있다. 이를 위하여 평문(plaintext)을 암호문(ciphertext)으로 변형하는 암호화에 의해 중요한 정보를 보호하게 된다. 여러 가지 형태의 암호가 연구되고 있는 가운데 중요한 정보를 안전하게 관리하기 위한 비밀 분산법(secret sharing scheme)이 A.Shamir에 의해 제안되었으며[1], 이것을 기초로 하여 인간의 시각으로 비밀을 복원하는 시각암호[2]가 M.Naor와 A.Shamir에 의해 제안된 후, 많은 연구가 진행되고 있다[3-5]. 시각암호는 비밀 정보를 슬라이드와 같이 물리적으로 중첩이 가능한 곳에 인쇄하여 겹쳤을 때 비밀 정보를 확인할 수 있는 방법으로 복호시 복잡한 연산이 필요 없는 장점이 있다. M.Naor와 A.Shamir가 제안한 시각암호는 비밀을 n장의 슬라이드에 분산시켜

본 연구는 한국과학재단 핵심전문 연구과제(과제번호 : 981-0928-493-2) 연구비에 의해 연구되었음

† 부경대학교 전자계산학과

k장 이상 겹쳐야만 비밀을 확인할 수 있음을 제시하고 있으나, 비밀정보로서 간단하게 두 레벨의 화상만을 고려하고 있다.

한편, 인터넷과 같은 네트워크를 통한 디지털 데이터의 복사는 원본과 전혀 차이가 없기 때문에 저작권 보호의 측면에서 심각한 문제점이 생기게 되었다. 따라서, 멀티미디어 데이터의 저작권 보호를 위한 방법 중에서 디지털 컨텐츠(contents) 내에 저작권에 대한 서명정보를 집어넣는 디지털 워터마크 기법[6]에 대한 연구가 활발히 진행되고 있다. 서명정보인 워터마크는 화상, 음성과 같은 비정형화 데이터의 특성을 이용하여 몰래 집어넣게 된다. 이때, 데이터의 값은 인간의 시각 또는 청각에 의해 인식될 수 없는 범위 내에서 약간 변경되어 진다. 그리고, 불법복사로부터 저작자의 서명정보를 확인하기 위해서는 저작자만이 소유한 비밀키에 의해 화상으로부터 워터마크를 추출하게 된다. 워터마킹된 화상에 대해 화상의 변경 등과 같은 불법적인 조작이 이루어졌을 경우에도 저작권을 주장하는 워터마크를 확인할 수 있어야 한다. 이와 같은 관점에서 워터마크의 제거를 위한 공격에 대한 견고성을 가지면서 원 화상에 대한 워터마크의 삽입이 인지될 수 없도록 처리하는 다양한 방법들이 제안되어지고 있다[7-8]. 그러나, 기존의 디지털 워터마크 기법들은 단지 소프트웨어적으로 워터마크의 추출을 수행하기 때문에 하드 카피된 화상에 대한 저작권 보호는 불가능하다. 이 점에 주목하여 하드 카피된 화상에 대한 저작권 보호를 위한 방법이 Oka들에 의해 제안되었지만[9] 명확한 서명정보를 생성할 수 없다는 단점이 있다.

따라서, 본 논문에서는 두 레벨 이상의 화상을 대상으로 시각암호의 슬라이드를 구성하여 디지털 워터마크에 응용할 수 있음을 보인다. 먼저, 2장에서는 시각암호에 대하여 간단히 기술하고, 시각암호의 개념을 이용하여 하드 카피된 화상의 저작권 보호를 위한 ONM(Oka-Nakamura-Matsui) 방식을 기술한다. 그리고, 3장에서는 시각암호와 ONM 방식의 관계를 시각암호의 측면에서 고찰하고, ONM방식을 확장하여 원래의 화상을 유지한 채로 하나 이상의 서로 다른 화상으로 비밀 정보를 분산하는 방법을 제안한다. 4장에서는 시뮬레이션을 통하여 그 유효성을 확인하고, 마지막으로 5장에서는 결론과 향후 연구 과제를 제시한다.

2. 시각암호에 의한 디지털 워터마크

2.1 시각암호

시각암호의 가장 간단한 형태는 흑과 백으로 구성된 이진 화상을 비밀 정보로 하여 슬라이드를 구성하는 방식이다. 비밀 화상을 구성하는 각 화소는 슬라이드에 $s\times s$의 패턴으로 표현되고 이 패턴들을 share라 한다. 슬라이드를 이루는 share는 $n\times m$의 부울 행렬 $S=[\ b_{ij}]$ 로부터 구성되는데, 이 행렬은 n장의 슬라이드에 크기 $m(=s\times s)$인 share들이 모두 중첩되었을때의 결합 share가 흑백 레벨을 나타낼 수 있도록 구성되어야 한다. 이때 결합 share의 흑백 레벨은 비밀 화상의 흑·백 값에 대응되어야 한다. 결합 share의 흑백 레벨은 행렬 S의 행들을 "or" 연산을 한 m차 벡터 V의 해밍 가중치(Hamming weight) $H(V)$에 비례한다. 즉, 고정된 임계값 $1\le d\le m$와 흑과 백의 상대적인 차이 $\alpha>0$ 에 대하여 식(1)과 같이 해밍 가중치 $H(V)$에 따라서 인간 시각 체계(human visual system)는 결합 share를 흑(black)과 백(white)으로 인식하게 된다.

$$HVS(H(V))=\begin{cases} black, & \text{if } H(V)\ge d \\ white, & \text{if } H(V)\le d-\alpha m \end{cases} \tag{1}$$

n명의 사용자에게 슬라이드를 나누어 준 후, k장 이상의 슬라이드를 중첩시켰을 때 비밀 정보가 나타나는 (k, n) 시각암호의 가장 간단한 형태인 (2, 2) 시각암호를 예로 들어 설명한다. 임계값 $d=4$, $\alpha=\frac{1}{4}$ 그리고 share의 크기 $m=4$인 경우, 2×4인 부울 행렬 S는 각각 백화소를 위한 부울 행렬 S_0, 흑화소를 위한 부울 행렬 S_1을 식(2)와 같이 정의할 수 있다.

$$S_0=\begin{bmatrix} 0&1&1&1 \\ 0&1&1&1 \end{bmatrix},\quad S_1=\begin{bmatrix} 0&1&1&1 \\ 1&0&1&1 \end{bmatrix} \tag{2}$$

여기서 각 행렬의 제1행은 첫 번째 슬라이드를 위한 share가 되고, 제2행은 두 번째 슬라이드를 위한 share가 된다. 앞에서 기술하였듯이 결합 share의 해밍 가중치를 계산하면 S_0에서는 $H(V=(0,1,1,1))=3$이 되고, S_1에서는 $H(V=(1,1,1,1))=4$로 흑과 백을 구분할 수 있게 된다. 이때, 식(2)의 S_0, S_1의 각 열들을 치환하여 만들어진 부울 행렬들의 집합을

C_0, C_1이라 하자.

$C_0=\left\{S_0=\begin{bmatrix}0111\\0111\end{bmatrix}\right.$ 의 열을 교환하여 얻어진 행렬$\left.\right\}$

$C_1=\left\{S_1=\begin{bmatrix}0111\\1011\end{bmatrix}\right.$ 의 열을 교환하여 얻어진 행렬$\left.\right\}$

이 집합으로부터 비밀 정보의 화소가 백인 경우에는 C_0의 한 원소인 임의의 부울 행렬의 행들을 각각의 슬라이드에 표시하고, 흑인 경우에는 C_1에서 임의의 부울 행렬을 선택하여 행들을 슬라이드에 표시하여 구성하게 된다. (k, n) 시각암호의 유효한 해가 존재하기 위해서는 문헌 [2]에 정의되어 있는 아래의 세 가지 조건을 만족해야 한다.

〔조건1〕 행렬들의 집합 C_0에서 임의의 행렬 S에 대해서, n행 중 임의의 k행을 "or" 연산하였을 때 m차 벡터 V의 해밍 가중치는 $H(V)\leq d-am$을 만족한다.

〔조건2〕 행렬들의 집합 C_1에서 임의의 행렬 S에 대해서, n행 중 임의의 k행을 "or" 연산하였을 때 m차 벡터 V의 해밍 가중치는 $H(V)\geq d$를 만족한다.

〔조건3〕 $q<k$인 $\{1,2,\cdots,n\}$의 임의의 부분집합 $\{i_1, i_2, \cdots, i_q\}$에 대해서, C_t내의 각 $n\times m$ 행렬을 $i_1, i_2, \cdots, i_q$ 행으로 한정하여 얻어진 동일한 빈도의 동일한 행렬들을 포함한 2개의 $q\times m$ 행렬의 집합 D_t는 서로 구분할 수 없다. 단, $t\in\{0,1\}$

여기서, [조건1]과 [조건2]는 슬라이드를 겹쳤을 때 흑과 백을 구별하기 위한 상대적인 휘도(contrast)를 나타내고, [조건3]은 k장 미만의 슬라이드를 중첩하였을 때 share에 대응되는 비밀 화소의 값이 흑인지 백인지를 구분할 수 없는 안전성(security)을 의미한다. 위에서 예로 든 (2, 2) 시각암호는 이 세 가지 조건을 만족하고 있다.

2.2. 디지털 워터마크를 위한 ONM방식

시각암호의 기본원리는 흑과 백을 구분하는데 있어서 흑·백의 적분 효과를 이용하는 것이다. 흑·백의 적분 효과란 인간의 시각이 흑 화소가 많은 영역은 흑으로 인식하고, 상대적으로 흑이 적은 영역은 백으로 인식한다는 것이다. 이러한 적분 효과를 이용하는 또 다른 분야의 예로 화상 디더링(dithering)을 들 수 있다. 화상의 디더링은 프린터 등에 이용되는 기술로 높은 레벨을 가진 화상을 프린터, 디스플레이와 같이 한정된 레벨만을 출력할 수 있는 장치에 표시하기 위해 레벨을 낮추어서 의사적으로 나타내는 것이다[10].

디더링의 가장 간단한 방법인 농도 패턴법은 레벨을 1과 0의 흑백의 패턴으로 표현하게 된다. 예를 들어, 그림 1에 4×4 크기의 농도 패턴법에 의한 셀 패턴들을 나타낸다. 실제 이와 같은 패턴들은 출력시에 artifact 왜곡이 나타나지 않도록 세심하게 구성되어야 한다.

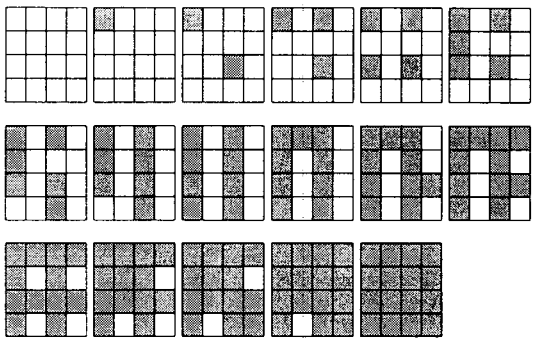


그림 1. 농도 패턴법 : Rylander's recursive patterning matrices

ONM방식은 저작권을 보호하기 위하여 셀 패턴을 이용하여 서명정보를 합성하는 디지털 워터마크의 한 기법이다. 즉, 서명 정보가 되는 비밀 S를 분산시키기 위해 q레벨을 가지는 원 화상 G의 각 화소 $g(i,j)\in\{0,1,\cdots,q-1\}$를 M레벨로 양자화한 후, S의 각 비트 $s(i,j)$의 값에 의해 출력화상 R과 검증화상 V를 생성하기 위한 셀 패턴을 결정한다. ONM 방식에서 이용하는 셀 패턴은 그림 2와 같이 간단한 것으로 표 1과 같이 0과 1로 표현할 수 있다. 양자화된 각 화소의 레벨을 l이라 할 때, $H_l\ (k_p, k_q)$는 레벨이 l인 번호 k_p, k_q인 셀 패턴간의 해밍 거리(Hamming distance)라 정의한다. R과 V의 출력패턴은 아래와 같이 서명정보 S와 셀 패턴의 해밍 거리에 의해 결정된다.

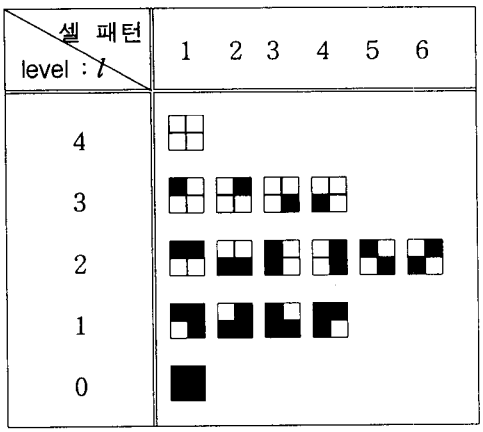


그림 2. 각 레벨에서의 셀 패턴

- $s(i,j)=1$(흑)인 경우,
  R과 V에 $H_l(k_p,k_q)$가 최대가 되는 셀 패턴 k_p, k_q를 각각 출력한다.
- $s(i,j)=0$(백)인 경우,
  $H_l(k_p,k_q)$가 최소가 되는 셀 패턴 k_p또는 k_q를 R과 V에 동시에 출력한다.

표 1에서 $l=2$인 경우, 6개의 셀 패턴 사이의 해밍 가중치는 표 2와 같이 계산된다. 이때, $s(i,j)$에 대하여 6개의 셀 패턴 중에서 2개를 선택하여 R과 V에 각각 출력하게 되는데, $s(i,j)=1$인 경우는 $H_2(k_p,k_q)$가 최대가 되는 셀 패턴인 (1,2), (3,4), (5,6) 중에서 임의로 선택하여 각각 R과 V에 출력한다. 반대로 $s(i,j)=0$인 경우는 $H_2(k_p,k_q)$가 최소가 되는 셀 패턴을 출력한다. 이와 같이 모든 레벨에 대하여 표2와 같은 해밍 거리를 계산할 수 있으며, 서명정보의 비트 $s(i,j)$에 따라 셀 패턴들을 출력화상 R과 검증화상 V에 각각 분산하게 된다.

표 1. 1과 0으로 표현된 셀 패턴

l (해밍가중치 h)	1 2 3 4 5 6
4 (0)	0000
3 (1)	1000 0100 0001 0010
2 (2)	1100 0011 1010 0101 1001 0110
1 (3)	1101 0111 1011 1110
0 (4)	1111

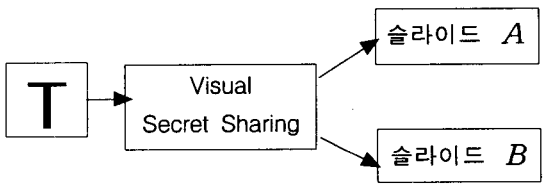
표 2. $l=2$에서 k_p와 k_q간 해밍 거리

k_q \ k_p	1	2	3	4	5	6
1	0	4	2	2	2	2
2	4	0	2	2	2	2
3	2	2	0	4	2	2
4	2	2	4	0	2	2
5	2	2	2	2	0	4
6	2	2	2	2	4	0

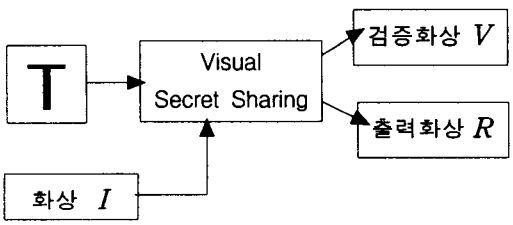
3. 시각암호에 의한 디지털 워터마크

3.1 ONM방식의 고찰

ONM방식을 시각암호의 측면에서 고찰하면 가장 간단한 형태인 (2,2) 시각암호가 된다. 시각암호 관점에서 ONM방식과 일반적인 시각암호와의 차이점을 그림 3에 나타낸다.



(a) 일반적인 시각암호의 개념



(b) 시각암호 관점의 ONM방식

그림 3. 시각암호와 ONM방식의 차이

일반적인 시각암호의 개념을 나타내는 그림3(a)에서 비밀이 분산된 슬라이드 A,B는 그 내용을 전혀 볼 수 없는 랜덤 화상으로 나타난다. 이것은 시각암호의 [조건3]을 만족하는 결과로 한 장의 슬라이드로는 비밀정보를 인지할 수 없도록 share의 해밍 가중치를 동일하게 하였기 때문이다. 그러나, 그림3(b)는 화상 I를 이용하여 비밀정보 T를 분산함과 동시

에 화상 I의 형태가 그대로 슬라이드에 나타나도록 하는 방법이다. 따라서, 분산 화상 R과 V는 비밀정보를 숨기고자 하는 l레벨로 양자화한 화상 I로 유지되면서 비밀정보의 비트에 따라 구성되는 슬라이드 화상 R와 V는 비밀정보가 분산된 슬라이드 A, B에 대응한다.

기존의 시각암호와의 차이점은 분산 화상 R와 V의 각 share 해밍 가중치가 동일하지 않다는 것이다. 따라서, 원 화상 I의 레벨을 유지하면서 share를 표시하여야 하기 때문으로 흑과 백을 나타내는 S_0, S_1만이 아니라 각 레벨마다 서로 다른 부울 행렬을 구성하여야 한다. 슬라이드 화상이 표1과 같이 5 레벨로 이루어지고, share 크기 $m=4$, 흑과 백의 상대적 차이 $\alpha=\frac{1}{4}$ 로 하는 경우, 레벨 l에 따른 부울 행렬 S_t^l, $t\in\{0,1\}$은 표3과 같이 구성된다.

표 3. 레벨 l에 대응하는 부울 행렬

레벨 l	백과 흑의 화소를 위한 부울 행렬
0	$S_0^0=\begin{bmatrix}1111\\1111\end{bmatrix}$, $S_1^0=\begin{bmatrix}1111\\1111\end{bmatrix}$
1	$S_0^1=\begin{bmatrix}1101\\1101\end{bmatrix}$, $S_1^1=\begin{bmatrix}1101\\1110\end{bmatrix}$
2	$S_0^2=\begin{bmatrix}1100\\1100\end{bmatrix}$, $S_1^2=\begin{bmatrix}1100\\0011\end{bmatrix}$
3	$S_0^3=\begin{bmatrix}1000\\1000\end{bmatrix}$, $S_1^3=\begin{bmatrix}1000\\0100\end{bmatrix}$
4	$S_0^4=\begin{bmatrix}0000\\0000\end{bmatrix}$, $S_1^4=\begin{bmatrix}0000\\0000\end{bmatrix}$

그러나, 표3에서 레벨 0과 4를 위한 부울 행렬은 앞에서 기술한 [조건1]과 [조건2]를 만족하지 않는다. 즉, [조건1,2]의 중첩 share들의 m차 벡터 V의 해밍 가중치가 동일하여 흑과 백의 차이가 나지 않는다. 또한, 레벨 3은 임계값 $d=2$, $\alpha=\frac{1}{4}$ 으로 [조건1,2]를 만족하지만, 중첩시에 주변 화소간의 상관성을 고려하면 레벨 1, 2에 비하여 비밀정보의 명확성이 떨어진다. 따라서, 비밀정보가 흑화소인 경우 중첩 share들이 모두 동일한 최대 해밍 가중치 m을 가지도록 구성함이 바람직하다. 이 점을 고려하여 모든 레벨의 흑화소를 위한 부울 행렬 S_1의 각 행을 "or" 연산한 m차 벡터 V의 해밍 가중치 $H(V)=m$이 되도록 하기 위해서는 모든 레벨의 해밍 가중치를 식(3)에 의해 계산된 B이상이 되도록 설정한다.

$$H=m,\ B=(\lfloor H/2\rfloor+k)$$
$$\text{단, } k=H \bmod 2 \tag{3}$$

결국 최대 해밍 가중치가 되지 않는 레벨을 제거시킴에 따라 레벨의 수는 감소되어 새로운 레벨의 수 $M'=H-B$로 조정된다. 따라서, share의 크기 $m=4$인 경우에는 가능한 레벨의 수는 2가 되고 각 레벨을 위한 셀 패턴들이 표4와 같이 구성된다.

표 4. 수정된 셀 패턴

셀 크기	l (h)	셀 패턴 (흑:1, 백:0)
$m=4$	1(2) 0(3)	1100 0011 1010 0101 1001 0110 1101 0111 1011 1110
$m=9$	3(5) 2(6) 1(7) 0(8)	"000011111"의 모든 조합 "000111111"의 모든 조합 "001111111"의 모든 조합 "011111111"의 모든 조합

레벨의 수를 증가시키기 위하여 share 크기를 $m=9$로 하면 식(3)에 의해 4레벨을 표현할 수 있어 보다 자연스러운 화상의 레벨을 나타낼 수 있으나, 슬라이드의 크기가 늘어 나고 화상이 전반적으로 어두워지는 상호보완 관계가 발행한다.

3.2 복수화상에 의한 비밀화상의 분산법

지금까지 기술한 시각암호의 관점에서 본 ONM 방식은 하나의 화상을 이용하여 비밀정보를 분산하는 슬라이드를 구성하였다. 이것을 확장하여 서로 다른 화상에 대해 비밀 정보를 분산하도록 슬라이드를 구성하는 방식을 제안한다. 이 방식은 그림3(b)를 확장 하는 것으로 그 개략도를 그림4에 나타낸다.

그림4에서 화상 I과 II는 서로 다른 화상으로 하나의 화상을 처리하는 ONM 방식과 달리 대응되는 위치의 레벨이 같지 않는 경우도 생기게 된다. 예를 들어, 화상 I과 II의 레벨의 쌍 $(l=0, l'=1)$인 경우, 레벨 l, l'의 셀 패턴들의 집합 P_l, $P_{l'}$로부터 표5와 같은 중첩 share들을 구할 수 있다.

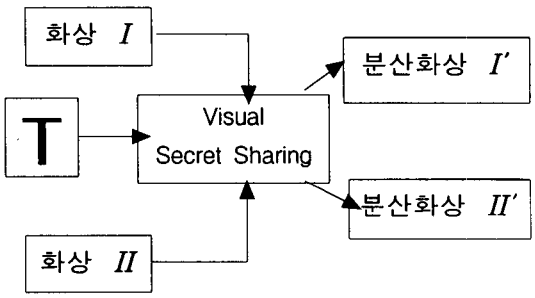


그림 4. 서로 다른 화상을 이용한 비밀화상 분산법

표 5. ($l=0, l'=1$) 일 때의 셀 패턴

P_l \ $P_{l'}$	0011	1100	0101	1010	0110	1001
0111	0111	1111	0111	1111	0111	1111
1011	1011	1111	1111	1011	1111	1011
1110	1111	1110	1111	1110	1110	1111
1101	1111	1101	1101	1111	1111	1101

$P(H(V)=h)$를 셀 패턴들을 중첩시 해밍 가중치가 h인 셀 패턴 쌍의 집합이라 할 때, 표5로부터 아래와 같은 집합을 얻을 수 있다.

$$P(H(V)=3)=$$

$$\left\{\begin{array}{l}(0011,0111),(0101,0111),(0110,0111),\\(0011,1011),(1010,1011),(1001,1011),\\(1100,1110),(1010,1110),(0110,1110),\\(1100,1101),(0101,1101),(1001,1101)\end{array}\right\}$$

$$P(H(V)=4)=$$

$$\left\{\begin{array}{l}(1100,0111),(1010,0111),(1001,0111),\\(1100,1011),(0101,1011),(0110,1011),\\(0011,1110),(0101,1110),(1001,1110),\\(0011,1101),(1010,1101),(0110,1101)\end{array}\right\}$$

이 결과로부터 각 행들이 서로 다른 해밍 가중치를 가지는 부울 행렬 $S_t^{l,l'}$, ($t\in\{0,1\}$, $(l,l')\in\{(0,0),(0,1),(1,0),(1,1)\}$)는 표6과 같이 구성된다.

표6의 첫 번째 행과 두 번째 행은 각각 화상 I 와 I''를 위한 share가 된다. 이때, 서로 다른 레벨 (0,1), (1,0)인 레벨 쌍에 대해서는 각 행의 해밍 가중치가 동일하지 않게 된다. 그러나, 모든 부울 행렬들은 시각암호의 [조건1,2]를 만족하고 있음을 확인할 수 있다. 이때, 주의해야 할 점은 부울 행렬의 해밍 가중치가 다르게 되기 때문에 [조건3]은 분산화상 I', II'에 대해서 만족하지 않게 된다. 또한, 화상의 수가 증가하게 되면 레벨 쌍의 조합 수 역시 증가하기 때문에 표6과 같은 간단한 부울 행렬 구성으로는 불가능하다. 즉, 레벨의 수 M과 화상의 수 n에 대해서 필요한 부울 행렬의 수는 $M^n\times 2$개가 필요하다. 따라서, 부울 행렬 구성을 위한 일반화된 방법에 대한 연구가 요구되어진다.

표 6. 서로 다른 레벨일 때의 부울 행렬

l \ l'	0	1
0	$S_0^{0,0}=\begin{bmatrix}0111\\0111\end{bmatrix}$ $S_1^{0,0}=\begin{bmatrix}1110\\1101\end{bmatrix}$	$S_0^{0,1}=\begin{bmatrix}0111\\0011\end{bmatrix}$ $S_1^{0,1}=\begin{bmatrix}1110\\0011\end{bmatrix}$
1	$S_0^{1,0}=\begin{bmatrix}0011\\0111\end{bmatrix}$ $S_1^{1,0}=\begin{bmatrix}0011\\1110\end{bmatrix}$	$S_0^{1,1}=\begin{bmatrix}1100\\0110\end{bmatrix}$ $S_1^{1,1}=\begin{bmatrix}1100\\0011\end{bmatrix}$

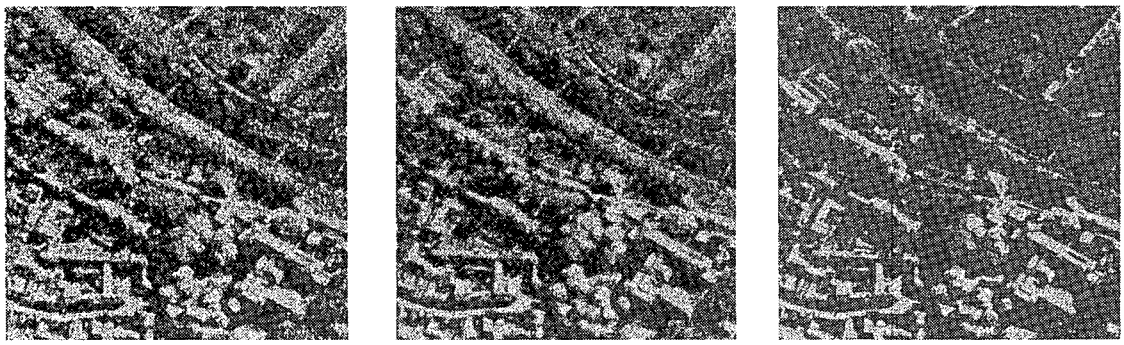
4. 시뮬레이션 및 결과

ONM방식과 제안방식에 의해 슬라이드를 구성하여 물리적으로 중첩시켜 비밀정보를 복원하는 시뮬레이션을 수행하였다. 원 화상으로 Lenna, Moon, Aerial, Boat(256×256, 8bits/pixel)를 각각 표1과 표4의 셀 패턴들을 이용하여 ONM방식과 제안방식을 구현하였으며, 양자화 처리는 테스트의 용이성을 위해 간단하게 선형 양자화 하였다.

그림5와 그림6은 ONM방식으로 표1의 셀 패턴과 5레벨로 양자화한 Lenna, Aerial 화상을 비밀정보에 따라 각각 슬라이드 화상을 구성하고 중첩한 결과이다. 그림5의 화상 Lenna는 V와 R을 중첩하는 경우 비밀정보가 있는 부분에 최대 해밍 가중치를 달성할 수 있는 셀 패턴들이 구성되어 비밀정보를 어느 정도 확인할 수 있으나, 명확한 비밀 정보를 확인하기는 어렵다. 또한, 그림 6의 화상 Aerial은 Lenna보다 화상의 특징으로 인하여 많은 부분들이 해밍 가중

(a) 검증화상 V (b) 출력화상 R (c) V ∪ R

그림 5. ONM방식에서 비밀정보의 확인(Lenna, 512×512)



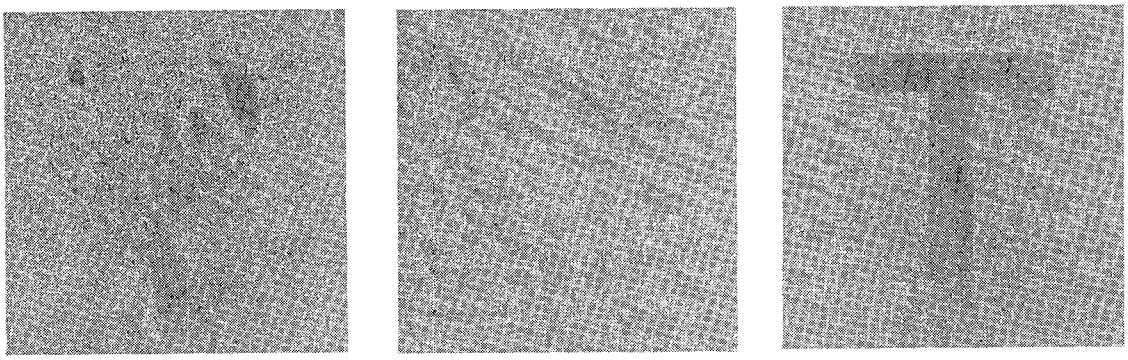
(a) 검증화상 V (b) 출력화상 R (c) V ∪ R

그림 6. ONM방식에서 비밀정보의 확인(Aerial, 512×512)

치가 낮은 상위 레벨로 결정되어 진다. 따라서, 최대 해밍 가중치를 달성하지 않는 셀 패턴들이 비밀정보가 있는 부분에 다수 분포되어서 Lenna보다 비밀정보는 더욱 명확하지 않게 된다. 이와 같이 ONM방식은 화상에 따라 비밀정보의 명확성이 다르다. 이러한 단점을 보완한 제안방식은 비밀정보가 있는 부분에 최대 해밍 가중치를 달성할 수 있도록 셀 패턴들을 선택하는 것으로써 제안방식의 결과를 아래에 나타낸다.

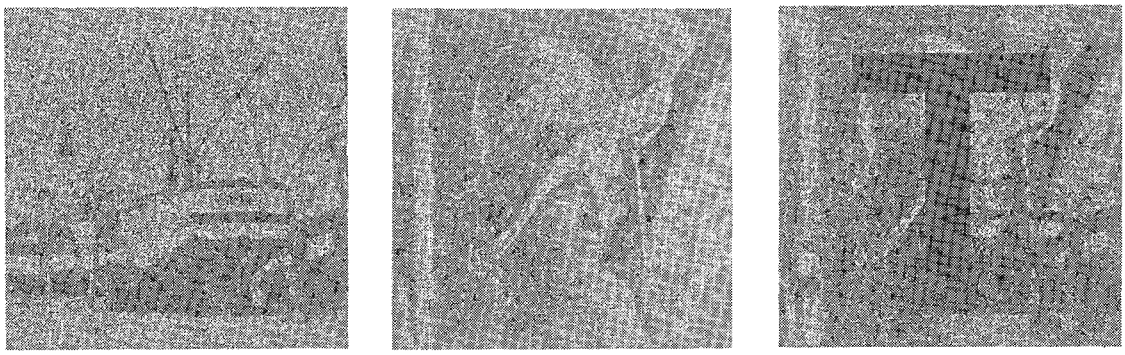
그림7과 그림8은 Moon과 Aerial, Boat와 Lenna를 각각 화상 I와 II로 하여 표4의 $m=9$인 셀 패턴을 이용하여 출력화상을 구성하고 중첩한 후, 비밀정보를 확인하는 제안방식의 결과이다. 식(3)으로부터 유도된 셀 패턴의 레벨은 5레벨에서 4레벨로 감소된다. 그리고, 셀 패턴의 구성은 시각암호의 관점으로 부울 행렬을 구성한 것이 아니라 단지 최대 해밍 가중치를 달성할 수 있는 셀 패턴들의 집합에서 패턴의 쌍을 임의로 선택하여 출력화상을 구성하였다. 이 경우에 서명 부분의 셀 패턴은 중첩 시에 모두 최대 해밍 가중치를 달성할 수 있도록 구성되었기 때문에 ONM 방식과 비교하여 화상에 관계없이 명확하게 비밀정보를 확인할 수 있음을 알 수 있다. 그러나, 그림5와 그림6에 비해 슬라이드의 크기가 큰 반면에 레벨의 수가 적음에 따라 전반적으로 출력화상들이 어두워 보이게 된다. 따라서, 제안방식은 화상의 성질을 기초로 한 보다 적절한 양자화 처리가 요구된다.

디지털 워터마크에 응용하기 위한 ONM방식은 단지 하나의 화상에 대한 저작권 보호를 위한 것으로 1:1로 대응하는 출력화상과 검증화상이 필요하다. 따라서, 만일 한 명의 저작자가 n개의 화상에 대해 서명정보를 집어넣고자 한다면 저작자는 각 화상에 대해 n개의 검증화상을 보관하고 있어야 하는 단점이 있다. 제안방식은 복수의 화상에 대하여 서명정보를 숨길 수 있는 것으로 ONM방식과 달리 시각암호의 개념을 이용하면 디지털 워터마크에 보다 효율적으로 응용할 수 있다. 즉, 저작자 자신의 검증용 화상



(a) Moon 출력화상 (b) Aerial 출력화상 (c) Moon ∪ Aerial

그림 7. 제안방식에 의한 비밀정보의 확인(Moon과 Aerial, 768×768)



(a) boat 출력화상 (b) Lenna 출력화상 (c) boat ∪ Lenna

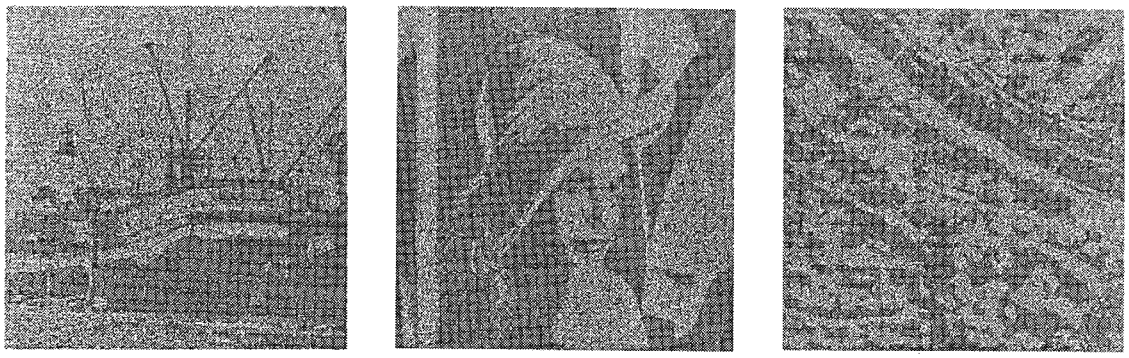
그림 8. 제안방식에 의한 비밀정보의 확인(Boat와 Lenna, 768×768)

과 서명화상(비밀화상)을 이용하여 저작자가 만든여러 개의 화상에 자신의 서명정보를 숨긴 후 화상을 배포하고, 저작자 자신은 단지 자신의 검증용 화상과 원 화상만을 보관한다. 또한, 명확한 서명정보의 확인이 가능하다는 점에서 ONM방식보다 불법 복사된 화상에 대해서 저작권의 보호에 더욱 효과적이다.

제안방식을 디지털 워터마크에 적용하기 위한 예로 표7과 같이 하나의 검증화상과 2개의 출력화상을 이용하여 서명정보를 숨기기 위해 구성된 부울 행렬을 이용하면 그림9와 같이 2레벨로 구성된 검증용 화상과 2개의 출력화상을 만들 수 있다. 특히 표7의 부울 행렬의 세 번째 행은 검증화상을 위한 것으로써 이 행으로 구성된 그림 9(a)의 검증용 화상을 저작자는 비밀리에 보관하고 그림 9(b)와 그림 9(c)는 각각 하드카피된 상태로 배포하게 된다.

이와 같이 배포된 출력화상에 대해 불법 복사된 화상을 발견하면 저작권을 확인하기 위해 검증용 출력화상을 발견된 불법 복사된 출력화상에 물리적으로 중첩하면 그림10(a), 그림10(b)와 같이 서명정보를 시각적으로 확인할 수 있게 된다

이와 같이 동시에 여러 개의 화상을 이용하는 경우에 ONM방식과 같이 단순한 셀 패턴이 아니라 시각암호의 관점에 셀 패턴을 구성하는 것이 적절하다는 것을 이 결과로부터 확인할 수 있다. 이때 서명정보는 저작자의 검증용 화상을 어떤 출력화상과 중첩하였을 때 확인할 수 있으며, 이것은 $(2, n)$ 시각암호와 다소 유사하게 된다. 일반적인 $(2, n)$ 시각암호는 2개의 임의의 화상을 중첩하여도 비밀정보를 확인할 수 있으나, 제안방식에서는 검증용 화상이 있어야 서명정보를 복원할 수 있다. 따라서, 검증용 화상은 하나의 키로 이용되어 검증용 화상이 유출되지 않는 한 그 안전성은 보장된다.

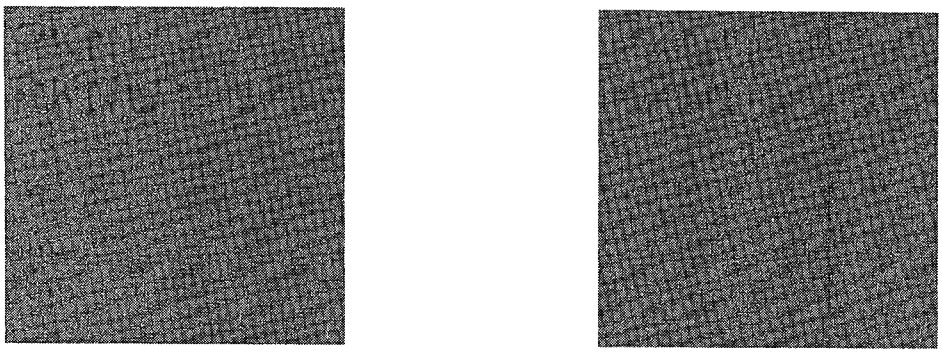


(a) 검증용 출력화상 (b) 출력화상 I (c) 출력화상 II

그림 9. 제안방식의 디지털 워터마크에 응용(512×512)

표 7. 1장의 검증용 화상과 2장의 화상의 부울 행렬(레벨 : 2)

l_1, l_2, l_3 / 서명정보	0,0,0	0,0,1	0,1,0	0,1,1
백	$S_0^{0,0,0}=\begin{bmatrix}0111\\0111\\0111\end{bmatrix}$	$S_0^{0,0,1}=\begin{bmatrix}0111\\0111\\0110\end{bmatrix}$	$S_0^{0,1,0}=\begin{bmatrix}0111\\0101\\0111\end{bmatrix}$	$S_0^{0,1,1}=\begin{bmatrix}0111\\0101\\0110\end{bmatrix}$
흑	$S_1^{0,0,0}=\begin{bmatrix}0111\\0111\\1110\end{bmatrix}$	$S_1^{0,0,1}=\begin{bmatrix}0111\\0111\\1010\end{bmatrix}$	$S_1^{0,1,0}=\begin{bmatrix}0111\\0101\\1110\end{bmatrix}$	$S_1^{0,1,1}=\begin{bmatrix}0111\\0101\\1010\end{bmatrix}$
l_1, l_2, l_3 / 서명정보	1,0,0	1,0,1	1,1,0	1,1,1
백	$S_0^{1,0,0}=\begin{bmatrix}0101\\0111\\0111\end{bmatrix}$	$S_0^{1,0,1}=\begin{bmatrix}0101\\0111\\0110\end{bmatrix}$	$S_0^{1,1,0}=\begin{bmatrix}0101\\0101\\0111\end{bmatrix}$	$S_0^{1,1,1}=\begin{bmatrix}0101\\0101\\0110\end{bmatrix}$
흑	$S_1^{1,0,0}=\begin{bmatrix}0101\\0111\\1110\end{bmatrix}$	$S_1^{1,0,1}=\begin{bmatrix}0101\\0111\\1010\end{bmatrix}$	$S_1^{1,1,0}=\begin{bmatrix}0101\\0101\\1110\end{bmatrix}$	$S_1^{1,1,1}=\begin{bmatrix}0101\\0101\\1010\end{bmatrix}$



(a) 검증용 화상 ∪ 출력화상 Lenna (b) 검증용 화상 ∪ 출력화상 Aerial

그림 10. 서명정보의 확인

5. 결 론

본 논문에서는 디지털 워터마크의 한 기법으로 제안된 ONM방식을 시각암호의 관점에서 고찰하였다. ONM방식은 시각암호의 가장 간단한 방법인 (2, 2) 시각암호의 한 형태임을 보였다. 나아가, 서로 다른 2개의 화상을 이용하여 원 화상의 형태를 유지하면서 서명정보를 분산시키는 확장된 방식을 제시하였다. 3개 이상의 화상을 처리하는 경우에는 저작자의 검증용 화상과 저작자가 만든 다수의 화상으로 서명정보를 처리하여 저작권 보호를 위한 디지털 워터마크에 적용 가능함을 보였다. 그러나, 실제적인 디지털 워터마크에 응용하기 위하여 하드카피된 화상을 확대·축소 복사하는 경우와 리스캐닝 등의 위조에 대한 견고성이 고려되어야 하며, 시각암호를 적용할 경우에는 효율적인 부울 행렬 구성법에 대한 연구가 요구된다.

참 고 문 헌

[1] A.Shamir, "How to Share a Secret", Commun. of the ACM, Vol.22, No.1, pp.612-613, 1979

[2] M. Naor, A. Shamir, "Visual Cryptography", Advances in Cryptology-Eurocrypt'94 Proc., LNCS Vol.950, Springer-Verlag, pp.1-12, 1995

[3] T. Katoh and H.Imai, "An Extended Construction Method of Visual Secret Sharing Scheme", IEICE Trans. Vol.J79-A, No.8, pp. 1344-1351, 1996.8(in Japanese)

[4] 김미라, 박지환, 박상우, 김광조, "시각암호에 의한 비밀 분산법", 통신정보보호학회 논문지, 제7권 4호, pp.37-50, 1997.12

[5] 김미라, 박지환, "시각암호에 의한 개인 인증 방식", 통신학회 논문지, 제23권 제6호, 1998.6

[6] 한종옥, 박춘식, 김은수, "저작권 보호를 위한 디지털 워터마크", 통신정보보호학회지, 제7권 제4호, pp.59-72, 1997.12

[7] I. J. Cox, J. Kilian, T. Leighton, and T. Shammoon, "Secure Spread Spectrum Watermarking for Multimedia", NEC Research Institute, Technical Report 95-10, 1995

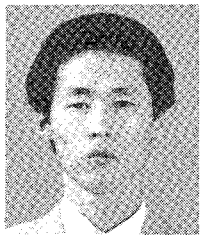
[8] J. Fridrich, A. C. Baldoza and R. J. Simard, "On Digital Watermarks", Second Workshop on Information Hiding Proc., 1998

[9] K. Oka, Y. Nakamura. K. Matsui, "Embedding Signature into a Hardcopy Image Using Micropatterns", IEICE Trans., Vol. J79-D-II, No.9, 1996.9(in Japanese)

[10] R. Crane, A Simplified Approach to Image Processing, Prentice Hall, pp.153-172, 1997

이 혜 주

1994년 부산수산대학교 전자계산학과 졸업(이학사)
1997년 부경대학교 전자계산학과(이학석사)
1997년~현재 부경대학교 전자계산학과 박사과정 재학 중
관심분야 : 멀티미디어 압축, 암호학 응용, 화상 처리 등



박 지 환

1984년 경희대학교 전자공학과 졸업(공학사)
1987년 일본국립전기통신대학 정보공학과(공학석사)
1990년 일본요코하마국립대학 전자정보공학과(공학박사)
1990년~1996년 부산수산대학교 전자계산학과 전강, 조교수, 부교수
1994년~1996년 일본동경대학 생산기술연구소 객원연구원
1996년~현재 일본동경대학 생산기술연구소 협력연구원
현재 부경대학교 전자계산학과 부교수
관심분야 : 멀티미디어 압축, 암호학 응용, 오류제어부호 등