情報保護學會論文誌
第11券 第6號, 2001. 12

누적행렬을 이용한 (k, n) 시각암호의 새로운 구성

김 문 수*, 박 지 환**

New Construction for Visual Cryptography Using the Cumulative Matrix

Moon-soo Kim*, Ji-hwan Park**

요 약

복잡한 암호학적 연산 없이 인간의 시각만으로 비밀정보를 직접 복원할 수 있는 시각암호는 영상형태의 비밀 정보를 n개의 랜덤한 영상(슬라이드)으로 분산시킬 때, 화소가 확장되면서 영상의 크기가 커지고 휘도가 떨어지는 문제점이 있다. 따라서 확장 화소의 수를 줄이고 휘도를 개선시키는 연구가 요구되고 있다. 본 논문에서는 n개의 슬라이드 중 k개를 겹치면 비밀정보를 복원할 수 있는 (k, n) 시각암호를 위하여 누적행렬에 따라 기저행렬을 생성하는 새로운 구성법을 제안한다. k가 홀수일 때 그 구성이 완전하며, k가 짝수일 때는 복수의 휘도를 허용함으로서 특별한 쌍의 최대 휘도를 높일 수 있는 방식이다. 제안 방식은 기존방식 중에서 최량의 휘도를 달성하는 Droste방식에 비하여 간단한 구성이면서 평균 휘도가 개선됨을 보인다. 또한, 일반 접근구조를 위한 기저행렬의 구성이 가능함을 보인다.

ABSTRACT

Visual cryptography is a simple method in which secret information can be directly decoded in human visual system without any cryptographic computations. When the secret image is scattered to n random shares(slides), this scheme has some week point such as pixel expansion and contrast degradation. Therefore, it is necessary to reduce the pixel expansion and improve the contrast in recovered image. In this paper, we propose a new construction method for (k, n) visual cryptography using the cumulative matrix. In case k is odd, we can construct the cumulative matrix perfectly. For even k, the contrast of special pair in decoded image can be achieved best by permitting multiple contrast. The proposed method is more simple than that of S. Droste's in construction and the average contrast of decoded image is improved for the most part. Also, we show that the basis matrices depending on the cumulative matrix are able to be applied for the general access structure.

keyword : *visual cryptography, cumulative matrix, (k, n) threshold scheme, multiple contrast*

Ⅰ. 서 론

A. Shamir에 의해 고안된 (k, n)-임계치 비밀 분산법은 비밀정보 S를 n개로 분산시킨 후, 임의의 k($k \leq n$)개 이상으로는 비밀정보 S를 복원할 수 있지만, k개 미만으로는 비밀정보 S에 관한 어떠한 정보도 얻을 수 없는 안전성을 갖는다.[1]

다항식 보간을 이용한 (k, n)-임계치 비밀 분산법의 새로운 형태로서 비밀정보를 영상의 형태로 취급할 수 있는 시각 복호형 비밀 분산법이 제안되었다.[2] 비밀영상은 흑과 백의 화소(pixel)로 구성되며, 슬라이드와 같이 물리적으로 중첩이 가능한 곳

* 본 연구는 부경대학교 2000년도 중등교원 연구비 지원에 의해 수행되었음.
** 부산여자고등학교, 교사(kms5812@mail1.pknu.ac.kr)
*** 부경대학교 전자컴퓨터정보통신공학부, 교수(jpark@pknu.ac.kr)

에 분산 인쇄되는 것을 가정한다. 원 비밀영상은 특별한 암호학적 연산 없이 임의의 슬라이드를 k장 이상 겹쳐 인간의 시각만으로 복원가능하며, k장 미만의 슬라이드를 겹치는 경우에는 비밀정보를 복원할 수 없기 때문에 안전성이 보장된다. (k, n)-임계치 비밀 분산법에 기반한 시각 복호형 비밀 분산법이 고안된 이후,

(1) 복원 시의 휘도 개선[3,4]
(2) gray scale 및 칼라 영상에의 적용[5~7]
(3) 일반 접근구조에 기반한 시각암호[8,9]

등의 다양한 연구가 진행되어 왔다. 복원 비밀영상의 휘도를 개선하기 위한 결과 중에는 S. Droste 방식[10]이 현재 가장 좋은 휘도를 달성하고 있다. 그러나, 이 방법은 기저행렬 구성에서 빈 행렬에 ADD (p, S_i) 알고리즘을 호출하여 열을 추가하고, 제한 행렬의 rest를 조사한 후 다시 ADD(p, S_i)에 의한 열 추가 과정을 반복해야하는 복잡성을 갖는다.

따라서, 본 논문에서는 (k, n)-VCS(Visual Cryptography Scheme)를 위하여 기존의 기법 중 가장 좋은 휘도를 달성하는 Droste 방식보다 간결한 기법을 제안한다. 2장에서 시각암호의 기본모델과 Droste에 의한 구성법을 고찰한다. 3장에서는 (k, n)-VCS의 기저행렬을 위하여 누적행렬을 이용한 구성 알고리즘을 제안하고, k가 홀수일 때와 짝수일 때 각각의 구성에 대한 실예를 보이며, 나아가 일반 접근구조를 위한 기저행렬의 구성이 가능함을 보인다. 4장에서 k가 홀수일 때 제안 기법이 (k, n) 비밀 분산 기법 중에서 최소의 확장 화소의 수와 기존의 가장 좋은 휘도 값을 나타내는 Droste의 결과와 동등한 성능을 지니는 간단한 구성법 임을 보인다. 또한, k가 짝수일 때 복수의 휘도를 허용하여 평균 휘도를 개선할 수 있음을 보이며, 필요에 따라 특수한 짝의 휘도를 조절할 수 있음을 보인다.

II. 시각암호

2.1 기본모델

시각암호에 의한 비밀분산의 가장 간단한 형태는 흑(1)과 백(0)의 화소로 구성된 이진 영상(binary image)을 대상으로 하는 것이다. 비밀영상의 각 화소는 m개의 부화소로 확장되어 n장의 슬라이드에 각각 분산되며, 이것을 share라 부른다.

이 구조는 비밀영상의 각 화소를 $n\times m$ 부울 행렬 $S=[s_{ij}]$로 표현할 수 있으며, 이때 s_{ij}의 값은 i번째 share 중 j번째 부 화소가 흑일 때 1이 되고, 백인 경우는 0으로 된다. Share들을 정확하게 겹쳤을 때, 행렬 S에서 행에 대한 부울리언 "or"로 표현되는 결합 share를 볼 수 있다. 결합 share의 grey 레벨은 "or" 연산을 한 m차 벡터 V에서 1의 개수인 해밍 가중치 $H(V)$에 비례한다. 이 grey 레벨은 어떤 고정된 임계치 $t(1\le t\le m$인 자연수)와 상대적 차 $\alpha>0$에 대해서 $H(V)\ge t$이면 흑으로, $H(V)\le t-\alpha\cdot m$이면 백으로 인식된다.

[시각암호의 정의]

$2\le k\le n$에 대하여 (k, n)-VCS는 $n\times m$부울 행렬들의 두 집합 C_0, C_1으로 구성된다. 백의 화소를 분산하기 위해서 C_0의 행렬 중 하나를 임의로 선택하고, 흑의 화소를 분산하기 위해서 C_1의 행렬 중 하나를 임의로 선택한다. 선택된 행렬의 각 행은 한 개의 share에 대응하고 행의 각 요소가 1이면 흑을, 0이면 백을 나타낸다. 아래의 3가지 조건을 만족하면 (k, n)-VCS의 해가 된다.

1. C_0의 임의의 행렬 S_0에 대해 n행 중 임의의 k행에 대한 "or" 연산 시 m차 벡터 V의 해밍 가중치는 $H(V)\le t-\alpha\cdot m$을 만족한다.
2. C_1의 임의의 행렬 S_1에 대해 n행 중 임의의 k행에 대한 "or" 연산 시 m차 벡터 V의 해밍 가중치는 $H(V)\ge t$를 만족한다.
3. $q<k$인 $\{1,2,\cdots,n\}$의 임의의 부분집합 $\{i_1, i_2, \cdots, i_q\}$에 대해 $C_j(j\in\{0,1\})$의 각 $n\times m$ 행렬을 $i_1, i_2, \cdots, i_q$행으로 제한하여 얻은 $q\times m$ 행렬 $D_j(j\in\{0,1\})$는 열 치환하면 서로 동일한 행렬이 된다.(단, $\alpha=\frac{d}{m}$, d는 S_0와 S_1의 임의의 k행에 대한 "or"연산 시 발생하는 m차 벡터 V에 대한 해밍 가중치)

두 집합 C_0, C_1의 행렬 중 각각 하나를 임의로 선택한 행렬 쌍 S_0, S_1을 (k, n)-VCS를 위한 기저행렬이라고 한다. 기저행렬이 갖추어야 할 조건인 1과 2는 share를 겹쳤을 때 복원된 영상에서의 명료한 정도인 휘도(contrast)를 나타내고, 조건3은 k장미만의 share를 겹쳤을 때 분산된 화소가 흑인지

백인지를 구분할 수 없는 안전성(security)을 나타낸다.

2.2 Naor & Shamir의 시각암호

M. Naor와 A. Shamir는 (k, n)-VCS를 위한 기저행렬을 (k, k)-VCS로부터 구성함을 제시하였으며[2], 그림1은 시각암호에 대한 기본 개념을 보여준 일예이다.

[(k, k)-VCS 구성법]

k개의 원소를 갖는 임의의 기본집합 $\{e_1, e_2, \cdots, e_k\}$에 대하여, 짝수 개의 원소로 구성되는 부분집합의 리스트 $\pi_1, \pi_2, \cdots, \pi_{2^{k-1}}$과 홀수 개의 원소로 구성되는 부분집합의 리스트 $\sigma_1, \sigma_2, \cdots, \sigma_{2^{k-1}}$을 고려한다. $1 \le i \le k$와 $1 \le j \le 2^{k-1}$인 i, j에 대하여 S_0와 S_1은 $e_i \in \pi_j$일 때 $S_0[i, j]=1$, $e_i \in \sigma_j$일 때 $S_1[i, j]=1$로 정의되는 $k \times 2^{k-1}$ 기저행렬(basis matrix)이라 하자. S_0와 S_1의 모든 열들을 교환해서 만든 행렬의 집합을 C_0와 C_1으로 각각 나타낸다. C_0와 C_1의 각각에서 택한 임의의 행렬 쌍은 (k, k)-VCS를 위한 기저행렬의 해가 되며 확장 화소의 수는 $m=2^{k-1}$이고 상대휘도는 $\alpha = 1/2^{k-1}$인 기법이 된다. 기저행렬의 행은 사용자에게 각각 분산되는 확장된 화소를 나타낸다. 그림 1에 (3,3)-VCS의 일 예를 나타낸다. 이 때, 부 화소의 크기 m과 상대적 차 α는 각각 4와 1/4이 된다.($t=4$, $d=1$)

$$S_0 = \begin{pmatrix} 0110 \\ 0101 \\ 0011 \end{pmatrix}, \quad S_1 = \begin{pmatrix} 1001 \\ 0101 \\ 0011 \end{pmatrix}$$

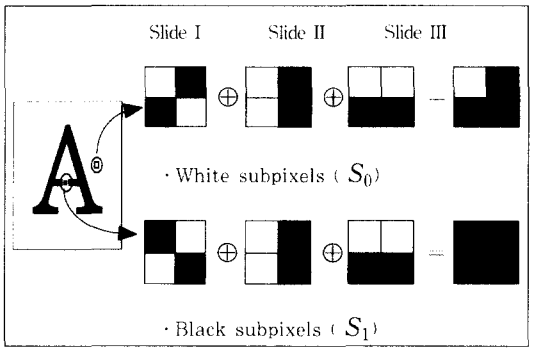


그림 1 화소의 분산

2.3 Droste 방식

S. Droste는 기저행렬의 구성을 위하여 열 추가 subroutine인 ADD(p, S_i)를 사용하고 있으며, 확장 화소의 수 m은 열 추가 알고리즘이 종료될 때 결정된다.[10] Droste 알고리즘은 다음과 같이 정의되는, rest 처리에 많은 계산량이 요구되는 기법이다.

[rest의 정의]

(k, n)-VCS의 구성 과정에서 백(흑)의 화소를 위한 기저행렬 S_0(S_1)의 k행을 취하여 제한행렬이라 하자. 제한행렬의 열에 대한 해밍 가중치를 조사하여 모든 종류의 짝(홀)수 열을 한번씩 제거하고 남은 열들에서 해밍 가중치가 같은 열들을 종류별로 모아 한 쌍을 만들었을 때, 그 쌍에 대한 해밍 가중치를 rest라 한다.

[(k, n)-VCS의 기저행렬을 위한 열 추가 알고리즘 ADD(p, S_i)]

기저행렬의 구성을 위하여 행의 수가 n이고 열의 수가 결정되지 않은 행렬을 S_i($i \in \{0,1\}$)라 둔다.

1. $p \le k-p$이면 $q=p$개의 1을 갖는 모든 열을 기저행렬 S_i의 마지막 열에 추가한다.
2. $p > k-p$이면 $q=p+n-k$개의 1을 갖는 모든 열을 기저행렬 S_i의 마지막 열에 추가한다.
   (단, p는 기저행렬 S_i에 추가되는 열에 대한 해밍 가중치)

[(k, n)-VCS의 기저행렬을 위한 Droste의 알고리즘]

1) 백/흑의 화소 분산을 위하여 행의 수가 n이고 열의 수가 결정되지 않은 빈 행렬 S_0/ S_1을 준비한다.
2) S_0의 구성을 위해 k 이하의 짝수를 택하여 ADD (p, S_0)를 호출하고, q개의 해밍가중치를 갖는 모든 열을 빈 행렬에 한번씩 추가한다.
3) S_1의 구성을 위해 k 이하의 홀수를 택하여 ADD (p, S_1)을 호출하고, q개의 해밍가중치를 갖는 모든 열을 빈 행렬에 한번씩 추가한다.
4) 2)와 3)에서 구성된 S_0, S_1에서 각 행의 수를 k로 제한하여 얻어지는 행렬의 rest를 조사한다.
5) S_1의 rest를 참조하여 ADD(p, S_0)를 호출하

고, q개의 해밍가중치를 갖는 모든 열을 S_0 행렬에 한번씩 추가한다.

S_0의 rest를 참조하여 ADD(p, S_1)을 호출하고, q개의 해밍가중치를 갖는 모든 열을 S_1 행렬에 한번씩 추가한다.

6) 두 행렬 각각에 대한 k행으로의 제한행렬에서 rest가 서로 같아질 때까지 4)와 5)의 단계를 반복하여 기저행렬을 완성한다.

[예1] (2,4)-VCS의 구성

1. 백/흑의 화소 분산을 위하여 행의 수가 4이고 열의 수가 결정되지 않은 빈 행렬을 S_0/S_1이라 둔다.
2. S_0 구성에 필요한 2 이하의 짝수 p는 0, 2이므로 ADD(p, S_0)를 호출한다.
   1) $p=0$일 때 : $p\le k-p \Rightarrow q=p=0$
      - 빈 기저행렬 S_0에 해밍가중치가 0인 열을 추가한다.
   2) $p=2$일 때 : $p>k-p \Rightarrow q=p+n-k=4$
      - 1)에서 구성된 S_0행렬에 해밍가중치가 4인 열을 추가한다.
3. S_1 구성에 필요한 2이하의 홀수 p는 1이므로 ADD (p, S_1)을 호출한다.
   1) $p=1$일 때 : $p\le k-p \Rightarrow q=p=1$
      - 빈 기저행렬 S_1에 해밍가중치가 1인 모든 열을 한번씩 추가한다.

   그 결과 얻어진 행렬 S_0, S_1은 다음과 같다.

$$S_0=\begin{pmatrix}01\\01\\01\\01\end{pmatrix},\quad S_1=\begin{pmatrix}1000\\0100\\0010\\0001\end{pmatrix}$$

4. 위에서 구성된 행렬에서 각각에 대한 제한행렬의 rest를 조사한다.

$$S_0=\begin{pmatrix}01\\01\\-\\01\\01\end{pmatrix},\quad S_1=\begin{pmatrix}1000\\0100\\--\\0010\\0001\end{pmatrix}$$

   1) S_0에서 2행으로 제한한 행렬에 대하여, $p=0$, $p=2$인 모든 종류의 열을 한번씩 제외한 나머지 열에서 rest는 존재하지 않는다.
   2) S_1에서 2행으로 제한한 행렬에 대하여, $p=1$인 모든 종류의 열을 한번씩 제외한 나머지 열에서 rest는 $p=0$, $p=0$인 열들이 된다.
5. 각 행렬의 rest를 참조하여 ADD(p, S)를 호출하고 열을 추가한다.
   1) S_1행렬의 rest 값인 $p=0$, $p=0$ 각각에 대하여 ADD(p, S_0)를 호출하고 S_0에 열을 추가한다.
      (1) $p=0$일 때 $p\le k-p$이므로 $q=p=0$의 해밍가중치를 갖는 열을 두 번 추가한다.
   2) S_0행렬의 rest가 없으므로 S_1에 추가되는 열은 없다.
6. 양쪽 행렬의 rest가 모두 같으므로 구성된 기저행렬은 다음과 같다. 추가 알고리즘에 의해 생성된 열들을 bold체로 구분하였다.

$$S_0=\begin{pmatrix}01\ \mathbf{0}\ \mathbf{0}\\01\ \mathbf{0}\ \mathbf{0}\\01\ \mathbf{0}\ \mathbf{0}\\01\ \mathbf{0}\ \mathbf{0}\end{pmatrix},\quad S_1=\begin{pmatrix}1000\\0100\\0010\\0001\end{pmatrix}$$

따라서, 확장 화소의 수 $m=4$, 상대 휘도는 $\alpha=1/4$이 된다. 이 알고리즘은 현재 휘도와 확장 화소의 측면에서 가장 좋은 결과를 보이고 있으나,[10] 빈 행렬에 열 추가 알고리즘인 ADD(p, S_i)를 호출하여 열을 추가하고, rest를 조사한 후 다시 ADD (p, S_i)를 호출하여 열을 추가하는 과정을 rest가 같아질 때까지 반복해야하는 복잡성을 갖는다.

Ⅲ. 누적행렬에 의한 (k, n)-VCS의 새로운 구성

(k, k)-VCS의 기저행렬 S_0, S_1에서 모든 행을 겹쳤을 때, 결합 share에 대한 해밍 가중치의 차가 1이 됨을 이용하여 (k, n)-VCS를 구성하게 된다. 먼저, S_0, S_1의 각 행에 $r_1, r_2, \cdots, r_k$의 인덱스를 차례로 부여하고, $r_i(S_j)$($i\in\{1,2,\cdots,k\}$, $j\in\{0,1\}$)는 행렬 S_j에서 i번째 행이라 하자. $r_1, r_2, \cdots, r_k$에서 중복을 허락하여 n개 선택한 조합을 열로 하는 행렬 M을 고려한다. 행렬 C는 최대 열의 수가 ${}_kH_n$ 크기인 M에서 임의의 k행을 선택할 때, $r_1, r_2, \cdots, r_k$의 조합이 모든 열에 대하여 오직 한번만 포함되도록 M의 열을 줄인 것이다. 행렬 C의 원소에 대응하는 행 $r_i(S_j)$를 치환하여 얻어지는 두 행렬 $\tilde{S}_0, \tilde{S}_1$는 임의의 k행을 "or" 연산한 결합 share에서 해밍 가중치의 차가 반드시 1만큼 발생하게 된다. 그러나, k미만의 행을 선택하면 행렬 C에서 $r_1, r_2, \cdots, r_k$의 조합이 포함될 수 없으므로 해밍 가중치의 차가 발생하지 않는다. 따라서, 행렬 $\tilde{S}_0, \tilde{S}_1$는 (k, n)-VCS를 위한 기저행렬의 요구조건을 만족하게 된다.

이후, 행렬 C의 열의 수가 최소로 되는 누적행렬을 정의하고, 누적행렬로부터 (k, n)-VCS를 위한 기저

행렬을 구성하는 방법을 제안한다.

[누적행렬 $C(k, n)$의 정의]

n개의 행을 갖는 행렬에서 행 번호를 위로부터 $1,2,\cdots,n$으로 인덱싱 한다. $k(1\le k\le n)$개의 행 번호로 이루어지는 ${}_nC_k$종류 조합의 순서쌍을 오름차순으로 나열한다. 이 순서쌍을 이루는 요소가 행 번호에 대응되도록 각 조합을 삽입한다. 모든 열에 대하여 오직 한번만 존재하도록 각 조합을 겹쳤을 때, 열의 수가 최소가 되는 행렬을 누적행렬 $C(k, n)$이라 한다.

3.1 k가 홀수일 때

k가 홀수일 때, $C(k, n)$의 각 요소가 (k, k)-VCS 기저행렬의 행 번호에 의해 완전하게 채워지는 구성이 됨을 아래에 보인다.

[누적행렬 $C(k, n)$의 구성]

1. $k(1\le k\le n)$개의 행 번호로 이루어지는 ${}_nC_k$종류 조합의 순서쌍을 오름차순으로 나열한다.(이 때, 각 조합의 요소는 1행부터 k행까지의 행 번호를 의미한다)
2. 행의 개수가 n이고 열의 수가 결정되지 않은 빈 누적행렬 $C(k, n)$을 준비한다.
3. $C(k, n)$의 첫 번째 열부터 시작하여 순서쌍을 이루는 요소가 행 번호에 대응되도록 각 조합을 삽입한다. 조합 내의 일부 행 번호가 이미 채워진 행 번호와 겹쳐질 수 있으며, 열이 다 차거나 채울 수 없을 때 다음 열에서 같은 방법을 계속하여 $C(k, n)$을 완성한다.
4. ${}_nC_k$종류의 모든 조합이 모든 열에 대하여 오직 한 번씩만 존재하는 $C(k, n)$의 각 원소를 i번째 행의 인덱스인 $r_i(i=1,\cdots,k)$로 표기한다.

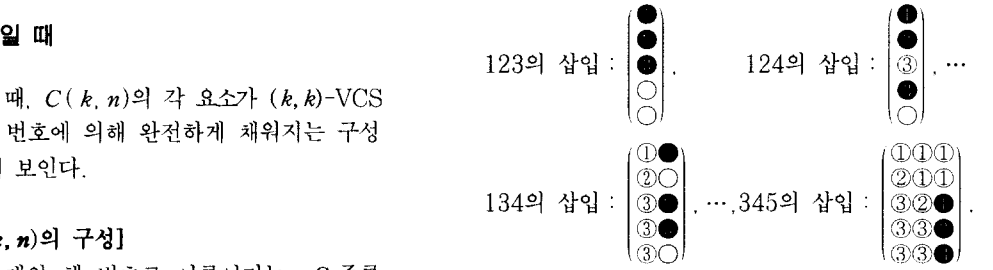
[기저행렬의 구성]

1. (k, k)-VCS를 위한 기저행렬 S_0와 S_1의 각 행을 1행부터 차례대로 $r_1, r_2, \cdots, r_k$로 인덱싱 한다.
2. $C(k, n)$의 각 원소에 대응하는 숫자를 S_0의 각 행 번호와 대응되도록 행을 치환함으로써 백의 화소를 위한 (k, n)-VCS의 기저행렬 S_0'를 구한다.
3. $C(k, n)$의 각 원소에 대응하는 숫자를 S_1의 각 행 번호와 대응되도록 행을 치환함으로써 흑의 화소를 위한 (k, n)-VCS의 기저행렬 S_1'을 구한다.
4. 구성된 기저행렬 S_0'와 S_1'의 양쪽에 같은 열(E)이 있으면 모두 제거하여 기저행렬 $\tilde{S}_0$와 $\tilde{S}_1$을 완성한다.

[예2] (3,5)-VCS의 구성

[누적행렬 $C(3,5)$의 구성]

1. 복호 가능한 모든 경우의 조합:(${}_5C_3=10$종류 : 123,124,125,134,135,145,234,235,245,345)
2. 각 경우가 꼭 한 번씩만 포함하도록 다음과 같이 누적시킨다. ●안의 숫자는 조합을 이루는 행 번호가 누적행렬에 차례로 할당됨을 나타낸다.



3. 구성된 $C(3,5)$는 다음과 같은 5×3의 행렬이 된다.

$$C(3,5)=\begin{pmatrix} r_1r_1r_1 \\ r_2r_1r_1 \\ r_3r_2r_1 \\ r_3r_3r_2 \\ r_3r_3r_3 \end{pmatrix}$$

[기저행렬의 구성]

1. $(3,3)$-VCS를 위한 기저행렬 S_0, S_1의 각 행을 다음과 같이 인덱싱한다.

$$S_0=\begin{pmatrix} 0110 \\ 0101 \\ 0011 \end{pmatrix}\begin{matrix} \leftarrow r_1(S_0) \\ \leftarrow r_2(S_0) \\ \leftarrow r_3(S_0) \end{matrix},\quad S_1=\begin{pmatrix} 1001 \\ 0101 \\ 0011 \end{pmatrix}\begin{matrix} \leftarrow r_1(S_1) \\ \leftarrow r_2(S_1) \\ \leftarrow r_3(S_1) \end{matrix}$$

2. $C(3,5)$의 각 원소 $r_i(i=1,2,3)$를 S_0/S_1의 각 행 번호 $r_i(S_j)(j=0,1)$와 대응되도록 치환함으로써 백/흑의 화소를 위한 $(3,5)$-VCS의 기저행렬 S_0'/S_1'를 구성한다.

$$S_0'=\begin{pmatrix} 0110\ 0110\ 0110 \\ 0101\ 0110\ 0110 \\ 0011\ 0101\ 0110 \\ 0011\ 0011\ 0101 \\ 0011\ 0011\ 0011 \end{pmatrix},\quad S_1'=\begin{pmatrix} 1001\ 1001\ 1001 \\ 0101\ 1001\ 1001 \\ 0011\ 0101\ 1001 \\ 0011\ 0011\ 0101 \\ 0011\ 0011\ 0011 \end{pmatrix}$$

3. S_0'와 S_1'의 양쪽에 존재하는 같은 열(E)을 제거하여 기저행렬 $\tilde{S}_0$와 $\tilde{S}_1$를 얻는다. 여기서, 두 행렬에 존재하는 같은 열들에 대한 순서쌍의 집합 $E(S_0', S_1')$은 다음과 같다.

$$E(S_0', S_1') = \{(S_0', S_1') \mid (2,5),(6,9),(8,3),(12,7)\},\ |E| = 4$$

$$\widetilde{S}_0 = \begin{pmatrix} 0\ 10\ 0\ 1\ \ 011 \\ 0\ 01\ 0\ 1\ \ 011 \\ 0\ 11\ 0\ 0\ \ 011 \\ 0\ 11\ 0\ 1\ \ 010 \\ 0\ 11\ 0\ 1\ \ 001 \end{pmatrix},\ \widetilde{S}_1 = \begin{pmatrix} 10\ 1\ \ 0\ 1\ \ 001 \\ 01\ 1\ \ 0\ 1\ \ 001 \\ 00\ 1\ \ 1\ 1\ \ 001 \\ 00\ 1\ \ 0\ 1\ \ 101 \\ 00\ 1\ \ 0\ 1\ \ 011 \end{pmatrix}$$

따라서, 기저행렬의 확장 화소의 수는 $m = 4\times 3 - E = 8$이고, $H_3(\widetilde{S}_0) = 5$, $H_3(\widetilde{S}_1) = 6$이므로 상대 휘도 α는 $(6-5)/m = 1/8$이 된다. 단, $H_i(\widetilde{S}_j)$는 기저행렬 $\widetilde{S}_j$의 임의의 i개 행을 "or"연산한 후의 해밍 가중치이다.

3.2 k가 짝수일 때

누적행렬 $C(k,n)$과 $C(k+1,n+1)$의 열의 수는 같으며, 홀수인 $k+1$의 경우는 3.1절의 구성에 의해 ${}_{n+1}C_{k+1}$조합이 $C(k+1,n+1)$에 완전하게 채워지는 형태가 된다. 그러나, 짝수인 k의 경우, ${}_nC_k$조합이 $C(k+1,n+1)$보다 한 행이 작은 $C(k,n)$의 누적행렬 내에 채워지게 된다. 이 때, ${}_{n+1}C_{k+1} = {}_nC_k + {}_{n-1}C_k + \cdots + {}_kC_k$의 성질을 고려하면, ${}_{n-1}C_k + \cdots + {}_kC_k$ 만큼의 조합이 $C(k,n)$에 더 추가될 수 있으므로 우측 상단에 행 번호가 할당되지 않은 곳이 발생하게 된다. 이곳에 원하는 행 번호를 할당하면 복수의 휘도를 가진 (k, n)-VCS를 구성할 수 있으며, 특별한 복원 쌍에 대한 휘도를 최대가 되도록 조절할 수 있게 된다.

[누적행렬 $C(k, n)$의 구성]

1. k가 홀수일 때 $C(k, n)$ 구성법의 1, 2, 3과 동일하게 구성한다.
2. ${}_nC_k$종류의 모든 조합이 모든 열에 대하여 오직 한 번씩만 존재하는 $C(k, n)$의 각 원소를 i번째 행의 인덱스인 r_i로 표기한다. 이 때, $C(k, n)$는 k가 홀수일 때와 달리 우측상단에 행 번호가 할당되지 않기 때문에 $C^e(k, n)$로 표기한다.
3. $C^e(k, n)$에서 행 번호가 할당되지 않은 우측 상단에 특별한 조합에 대한 휘도를 높일 수 있는 행 번호를 부여하여 누적행렬 $C(k, n)$로 정의한다.

[기저행렬의 구성]

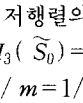
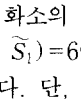
k가 홀수일 때의 기저행렬 구성법과 동일하다.

[예3] (2,4)-VCS의 구성

[누적행렬 $C(2,4)$의 구성]

1. 복호 가능한 모든 경우의 조합 : (${}_4C_2 = 6$ 종류 : 12,13,14,23,24,34)
2. $C^e(2,4)$를 얻기 위해서 각 경우가 꼭 한 번씩만 포함하도록 다음과 같이 누적시킨다.

12,13,14의 삽입 :  ,

23,24의 삽입 :  , 34의 삽입 : 

3. 구성된 $C^e(2,4)$은 우측 상단에 3개의 원소가 채워지지 않은 4×3의 행렬이 된다.

$$C^e(2,4) = \begin{pmatrix} r_1\ 0\ 0 \\ r_2 r_1\ 0 \\ r_2 r_2 r_1 \\ r_2 r_2 r_2 \end{pmatrix}$$

4. 가령 "12"의 조합이 최대 휘도를 갖도록 적당히 행 번호를 할당하여

$$C(2,4) = \begin{pmatrix} r_1 r_1 r_1 \\ r_2 r_2 r_2 \\ r_2 r_2 r_1 \\ r_2 r_1 r_2 \end{pmatrix}$$

로 조절한다.(즉, 두 행을 서로 교환하여도 결과가 같으므로 2행과 4행을 교환하고, 0대신 적절한 행 번호를 삽입하여 "12" 조합이 최대 휘도를 갖도록 조절한다)

[기저행렬의 구성]

k가 홀수일 때의 구성과 동일하며, 얻어진 (2,4)-VCS를 위한 기저행렬 $\widetilde{S}_0$, $\widetilde{S}_1$은 다음과 같다.

$$\widetilde{S}_0 = \begin{pmatrix} 010101 \\ 010101 \\ 010101 \\ 010101 \end{pmatrix},\ \widetilde{S}_1 = \begin{pmatrix} 101010 \\ 010101 \\ 010110 \\ 011001 \end{pmatrix}$$

얻어진 기저행렬의 확장 화소의 수는 $m = 2\times 3 - E = 6$이다. 평균 상대 휘도를 구하기 위하여 $C(2,4)$내의 복원 가능한 모든 조합의 수가 필요하고, 각 열에 대하여 복원 가능한 조합의 수를 구하면 각각 3, 4, 4개씩 존재하므로 평균 상대 휘도 $\bar{\alpha} = \frac{1}{6}(3+4+4) \times \frac{1}{6} = \frac{11}{36}$ (최대 3/6, 최소 1/6)을 얻을 수 있다. 이 결과는 2.3절의 Droste방식의 $\alpha = 1/4$보다 평균 휘도가 개선된 것이다.

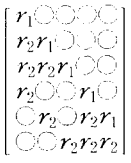
3.3 누적행렬의 일반 접근구조에 적용

(k, n)-VCS에서 n명 중 특정한 일부 참가자의 결합만으로 복원이 가능한 구조를 일반 접근구조라 한다.[8] 일반 접근구조를 위한 기저행렬도 제안기법의 누적행렬을 구성한 후, (k, k)-VCS를 위한 기저행렬의 행을 치환하는 방법으로 얻을 수 있다.

[일반 접근구조를 위한 기저행렬의 구성]

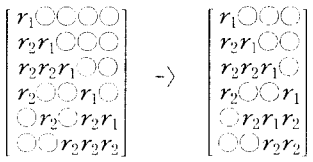
[예4] {12, 13, 14, 23, 25, 36, 45, 46, 56}을 위한 기저행렬

(1) (2,2)-VCS의 기저행렬을 이용하여 누적행렬을 다음과 같이 구성한다.

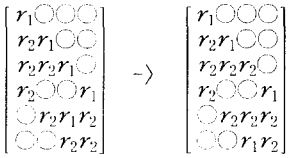


(2) 구성되는 누적행렬의 특성상 열에 대한 행 번호를 서로 교환하여도 결과가 같으므로 필요에 따라 행 번호를 교환할 수 있고, 어떤 열이 다른 열과 비교하여 행 번호의 위치가 모두 같고 오직 한 쌍만 서로 교차할 때, 한 열을 다른 열에 포함시켜 열의 수를 줄일 수 있다.

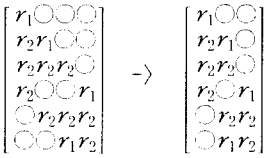
① 5열을 3열에 포함 :



② 3열의 r_1과 r_2를 교환:



③ 3열을 2열에 포함:



(3) 구성된 누적행렬의 각 원소 $r_i(i=1,2)$에 (2,2)-VCS를 위한 기저행렬

$$S_0=\begin{pmatrix}01\\01\end{pmatrix}\begin{matrix}\leftarrow r_1(S_0)\\\leftarrow r_2(S_0)\end{matrix},\quad S_1=\begin{pmatrix}10\\01\end{pmatrix}\begin{matrix}\leftarrow r_1(S_1)\\\leftarrow r_2(S_1)\end{matrix}$$

의 각 행 번호 $r_i(S_j)(j=0,1)$를 치환하고, 행 번호가 할당되지 않은 곳은 0의 행으로 채워서 기저행렬을 얻는다.

$$S_0=\begin{pmatrix}010000\\011000\\011000\\010010\\001010\\001010\end{pmatrix},\quad S_1=\begin{pmatrix}100000\\011000\\010100\\010010\\000101\\001001\end{pmatrix}$$

이 때, 확장화소의 수는 $m=6$이고, 상대 휘도는 $\alpha=1/6$이 된다. 이 구성의 결과는 최적은 아니지만 그래프 분할법[12]보다 개선된다. 예제4의 일반 접근구조에 대하여 그래프 분할법에 의한 기저행렬과 최적으로 알려진 기저행렬들을 아래에 나타낸다.

1. 그래프 분할법에 의한 기저행렬.[12]

$$S_0=\begin{pmatrix}10\ 00\ 00\ 00\\10\ 10\ 00\ 10\\10\ 00\ 00\ 10\\00\ 10\ 10\ 00\\00\ 10\ 00\ 00\\00\ 00\ 10\ 00\end{pmatrix},\quad S_1=\begin{pmatrix}10\ 00\ 00\ 00\\01\ 01\ 00\ 10\\01\ 00\ 00\ 01\\00\ 01\ 01\ 00\\00\ 10\ 00\ 00\\00\ 00\ 10\ 00\end{pmatrix}$$

이 때, 확장 화소의 수는 $m=8$, 상대 휘도는 $\alpha=1/8$이다.

2. 알려진 최적의 기저행렬.[8]

$$S_0=\begin{pmatrix}110\\110\\110\\100\\100\\100\end{pmatrix},\quad S_1=\begin{pmatrix}110\\101\\011\\001\\010\\100\end{pmatrix}$$

여기서 확장 화소의 수는 $m=3$, 상대 휘도는 $\alpha=1/3$이다.

Ⅳ. 제안기법의 성질과 비교분석

4.1. k가 홀수인 경우

k가 홀수일 때, 제안된 (k, n)-VCS를 위한 누적행렬은 아래의 두 가지 특징을 갖는다.

첫째, $C(k, n)$은 행렬 내에 복원 가능한 모든 조합이 빈틈없이 배열될 수 있으며, 그 열의 수 $\#(k, n)$는 다음과 같이 주어진다.

$$\#(k, n)=\#(k-2, n-2)+\#(k, n-1),$$

$$\#(3, n)=n-2.\ \text{단},\ k<n,\ k=5,7,9,\cdots$$

[예5] 누적행렬 $C(3,5)$의 열의 수

$C(3,5)$의 각 열에 포함된 경우의 수를 차례로 나열하면, ${}_5C_3=10=1\times3+2\times2+3\times1$과 같은 분포를 갖는 3개의 열로 구성되어 5×3의 행렬이 된다.

따라서, k가 홀수일 때 $C(k, n)$의 열의 수는 [표 1]과 같은 규칙성을 갖는다.

[표 1] $C(k, n)$의 열의 수(k : 홀수)

n \ (k, n)	(3, n)	(5, n)	(7, n)	(9, n)	(11, n)
$k+1$	2	3	4	5	6
$k+2$	3	6	10	15	21
$k+3$	4	10	20	35	56
$k+4$	5	15	35	70	126
$k+5$	6	21	56	126	252
$k+6$	7	28	84	210	462

둘째, 누적행렬 $C(k, n)$에 따라 구성된 S_0'와 S_1'에 동시에 존재하는 같은 열의 수 $|E|$는 두 행렬의 모든 열의 해밍 가중치를 구했을 때, 같은 가중치를 갖는 열의 수의 최소 값의 합만큼 존재한다.

S_0'와 S_1'에는 ${}_nC_k$종류의 모든 조합이 오직 한번씩 포함되어 있다. S_0'와 S_1'에 같은 열들이 존재하면 이들을 제거하여 확장 화소의 수 m이 작고, 휘도가 좋은 (k, n)-VCS를 위한 기저행렬을 얻을 수 있다. 만일, (k, n)-VCS를 위한 기저행렬이 최적의 확장 화소의 값 m으로 구성된 기법이라면 두 기저 행렬 각각에는 같은 열이 존재하지 않아야 한다. 한편, 같은 열의 수에 대한 최대 값은 S_0'와 S_1'의 가중치를 조사하였을 때, 같은 가중치에 대한 최소 값들의 합만큼 존재 할 수 있고, 이들을 제거하면, 최적의 확장 화소를 갖는 기저행렬을 얻을 수 있다. 따라서, k가 홀수일 때의 제안기법은 $C(k, n)$에 따라 처음부터 최적의 상태를 유지하였으므로 같은 열의 수 $|E|$의 값은 S_0'와 S_1'에 존재하는 같은 가중치를 갖는 열의 수에 대한 최소 값들의 합과 같다. 복수의 휘도를 허용하는 CYPK방법[11]의 기저 행렬 M도 본 제안 방법으로 구성이 가능하게 된다.

[예6] (3,5)-VCS를 위한 S_0'와 S_1'에서 열에 대한 해밍 가중치 H_i($i=0, \cdots, n$)에 의한 $|E|$의 값은 다음과 같다.

(3,5)-VCS	H_0	H_1	H_2	H_3	H_4	H_5	계
S_0'	3	0	2	2	5	0	12
S_1'	0	5	2	2	0	3	12
$\|E\|$	0	0	2	2	0	0	4

4.2 k가 짝수인 경우

k가 짝수일 때, 누적행렬 $C(k, n)$은 아래의 두 가지 특징을 갖는다.

첫째, $C(k, n)$의 열의 수는 $C(k+1, n+1)$의 열의 수와 같다..

복원 가능한 모든 조합의 수에 대하여 ${}_nC_k<{}_{n+1}C_{k+1}$의 부등식이 성립하므로, 누적행렬을 구성하는 규칙을 적용하면 $C(k, n)$의 열의 수는 $C(k+1, n+1)$의 열의 수와 같은 [표 2]의 결과를 얻는다.

따라서, k가 홀수일 때를 동시에 고려하면 모든 $k(2\le k\le n)$에 대하여 누적행렬의 열의 수 $\#(k, n)$은 다음의 식으로 구할 수 있다.

$$\#(k, n)={}_{n-\lfloor\frac{k+1}{2}\rfloor}C_{\frac{k}{2}}$$

둘째, $C(k, n)$에서 특별한 조합의 휘도를 최대가 되도록 조절할 수 있으며, 이때 최대 휘도와 최소 휘도는 각각

[표 2] $C(k, n)$의 열의 수

(k, n)	(2, n)	(3, n)	(4, n)	(5, n)	(6, n)	(7, n)	(8, n)	(9, n)	(10, n)	(11, n)
$n=k+1$	2	2	3	3	4	4	5	5	6	6
$n=k+2$	3	3	6	6	10	10	15	15	21	21
$n=k+3$	4	4	10	10	20	20	35	35	56	56
$n=k+4$	5	5	15	15	35	35	70	70	126	126
$n=k+5$	6	6	21	21	56	56	126	126	252	252
$n=k+6$	7	7	28	28	84	84	210	210	462	462

$$\frac{1+\text{추가되는 열의 수}}{\#(k,n)\times 2^{k-1}-E}, \quad \frac{1}{\#(k,n)\times 2^{k-1}-E}$$

로 된다. 단, $\#(k,n)$는 $C(k,n)$의 열의 수를 나타낸다.

k가 짝수일 때, 제안방법은 Droste 기법과 달리 기저행렬이 누적행렬에 의존하게 되므로 확장 화소의 수와 상대 휘도 값은 가변적으로 된다. 제안기법에서 기저행렬의 확장 화소 값은 다소 늘어나지만, 그 구성이 간단하고, 평균 휘도는 Droste의 결과보다 대부분 개선되었으며, 최대 휘도는 대폭적으로 개선되었다. 특히, 특별한 조합에 대한 휘도를 누적행렬에 의존하여 최대로 조절할 수 있는 장점이 있다. [표 3]에 제안기법과 S. Droste기법[10]에 대한 비교표를 나타내었으며, [그림 2, 3, 4]에서는 두 방식의 평균 휘도, 최대 휘도, 확장 화소의 수에 대한 비교를 그래프로 나타내었다. [표 3]과 [그림 2]에서는 k가 작을 때, 제안기법의 개선이 돋보임을 알 수 있다. [표 3]과 [그림 3]에서는 두 기법의 최대 휘도를 비교한 것으로 Droste방식에 비하여 뛰어남을 알 수 있다. 그리고 [그림 4]에서는 $(2,n)$-VCS에 대한 확장 화소의 수를 비교한 것으로 제안기법의 m이 다소 커진다. [표 4]는 확장 화소의 수를 줄일 수 있는 중복된 열의 수를 나타낸다.

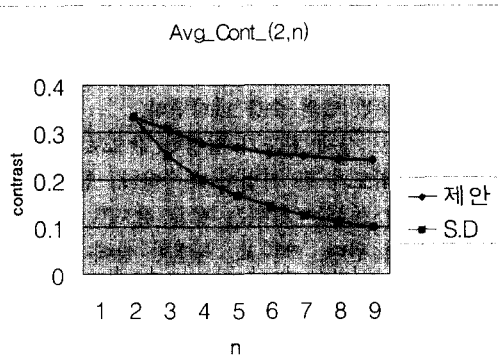
일반적으로 상대 휘도가 일정한 값으로 결정될 경우는 상대 휘도가 큰 기법이 우수하나, 일정한 값으로 결정되지 못하는 경우는 평균 휘도로 그 우수성을 평가하게 된다. 그리고, 특별한 쌍에 대한 최대

[표 3] 제안기법과 S. Droste기법에 의한 (k,n)-VCS의 결과 비교

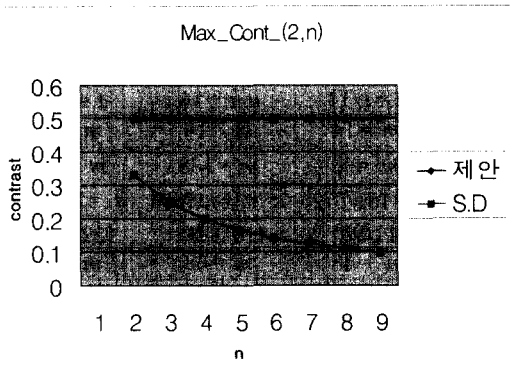
$n\backslash k$	기법	3	4	5	6	7	8	9	10
2	제안기법	$m=4$ $\tilde{\alpha}=1/3$ (2/4)	$m=6$ $\tilde{\alpha}=11/36$ (3/6)	$m=8$ $\tilde{\alpha}=11/40$ (4/8)	$m=10$ $\tilde{\alpha}=4/15$ (5/10)	$m=12$ $\tilde{\alpha}=16/63$ (6/12)	$m=14$ $\tilde{\alpha}=1/4$ (7/14)	$m=16$ $\tilde{\alpha}=35/144$ (8/16)	$m=18$ $\tilde{\alpha}=13/54$ (9/18)
	S.D	$m=3$	$m=4$	$m=5$	$m=6$	$m=7$	$m=8$	$m=9$	$m=10$
3	제안기법		$m=6$ $\alpha=1/6$	$m=8$ $\alpha=1/8$	$m=10$ $\alpha=1/10$	$m=20$ $\alpha=1/12$	$m=24$ $\alpha=1/14$	$m=28$ $\alpha=1/16$	$m=32$ $\alpha=1/18$
	S.D		$m=6$	$m=8$	$m=10$	$m=12$	$m=14$	$m=16$	$m=18$
4	제안기법			$m=18$ $\tilde{\alpha}=1/15$ (2/18)	$m=36$ $\tilde{\alpha}=11/270$ (4/36)	$m=62$ $\tilde{\alpha}=1/35$ (7/62)	$m=96$ $\tilde{\alpha}=151/6720$ (11/96)	$m=138$ $\tilde{\alpha}=161/8694$ (16/138)	$m=188$ $\tilde{\alpha}=26/1645$ (22/188)
	S.D			$m=15$	$m=24$	$m=35$	$m=48$	$m=63$	$m=80$
5	제안기법				$m=30$ $\alpha=1/30$	$m=48$ $\alpha=1/48$	$m=70$ $\alpha=1/70$	$m=96$ $\alpha=1/96$	$m=126$ $\alpha=1/126$
	S.D				$m=30$	$m=48$	$m=70$	$m=96$	$m=126$
6	제안기법					$m=80$ $\tilde{\alpha}=1/70$ (2/80)	$m=176$ $\tilde{\alpha}=37/4928$ (4/176)	$m=326$ $\tilde{\alpha}=16/3423$ (7/326)	$m=576$ $\tilde{\alpha}=187/58170$ (12/576)
	S.D					$m=70$	$m=128$	$m=210$	$m=320$
7	제안기법						$m=140$ $\alpha=1/140$	$m=256$ $\alpha=1/256$	$m=420$ $\alpha=1/420$
	S.D						$m=140$	$m=256$	$m=420$
8	제안기법							$m=316$ $\tilde{\alpha}=5/1422$ (2/316)	$m=763$ $\tilde{\alpha}=56/34335$ (4/763)
	S.D							$m=315$	$m=640$
9	제안기법								$m=630$ $\alpha=1/630$
	S.D								$m=630$

※ α : 상대 휘도, $\tilde{\alpha}$: 평균 휘도, ( ) : 특별한 조합에 대하여 가능한 최대 휘도.
※ S.D기법의 상대 휘도 : $\alpha=1/m$.

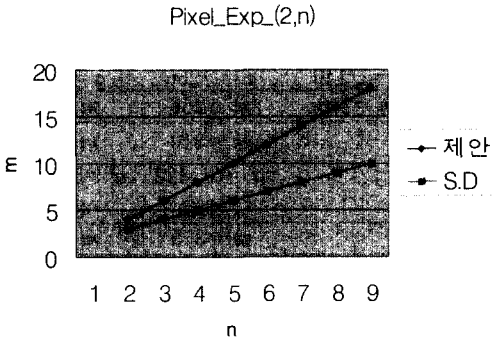
휘도가 높을수록 응용에 유리하게 된다. 또한 같은 조건에서 확장 화소의 수가 작을수록 상대적으로 휘도가 커지므로 확장 화소는 작을수록 우수한 것이나, 확장 화소의 수를 크게하여 상대휘도를 높일 수 있는 경우[13]도 있으므로 종합적으로 평가되어야 한다.



〔그림 2〕 제안기법과 Droste방식의 평균 휘도 비교



〔그림 3〕 제안기법과 Droste방식의 최대 휘도 비교



〔그림 4〕 제안기법과 Droste방식의 확장 화소 수에 대한 비교

〔표 4〕 $|E|$ 값의 분포

k/n	3	4	5	6	7	8	9	10
2	0	0	0	0	0	0	0	0
3		2	4	6	8	10	12	14
4			6	12	18	24	30	36
5				18	48	90	144	210
6					48	144	314	566
7						116	384	860
8							324	1157
9								650

4.3 구성의 간결성과 확장성

제안기법은 Droste방식보다 그 구성이 간결하며, 일반 접근구조를 위한 기저행렬의 구성도 가능한 확장성이 있다. 제안기법의 기저행렬은 아래와 같이 얻어진다.

1) (k, n)-VCS에서 ${}_nC_k$종류 조합의 순서쌍을 오름차순으로 나열한다.
2) 행의 개수가 n이고 열의 수가 결정되지 않은 빈 누적행렬에서 시작하여 $C(k, n)$을 구성한다. 이때, k가 짝수이면 휘도 조절을 위한 과정을 거쳐서 완성한다.
3) (k, k)-VCS를 위한 기저행렬의 각 행을 $C(k, n)$의 원소로 할당된 행 번호의 위치에 치환하여 S_0'와 S_1'을 얻는다.
4) S_0'와 S_1'에서 같은 열을 찾아 제거하여 최종 기저행렬 $\widetilde{S_0}$와 $\widetilde{S_1}$을 얻는다.

따라서, 제안방식은 2.3절의 Droste 방식이 내부에 loop를 포함하는 것에 비해 간결하다고 할 수 있다. 즉, Droste방식은 ADD(p, S_i)를 호출하여 열을 추가해 가는 과정과 제한행렬에서 rest를 조사하는 두 과정을 최대 $\lfloor \frac{k}{2} \rfloor$회 만큼 반복하게 되며, 특히 ADD(p, S_i)의 호출이 적어도 k회 이상 반복되어야 하고, 모든 열을 하나씩 구성해야 하는 복잡성을 갖는다. 또한, 열 추가나 rest의 조사과정에서 q개의 1을 갖는 모든 종류의 열을 동시에 추가하거나 조사해야 하며, 특히 rest의 조사는 추가된 ${}_nC_q$개의 모든 열을 k행으로 제한하고 각 열의 해밍 가중치를 검사한 후, 비로소 다음 추가될 열에 대한 종류를 결정하게 되므로 다시 모든 열을 비교해야 하는 복

잡성을 갖는다. 반면, 제안기법의 $C(k, n)$은 휘도 조절 과정까지 고려하더라도 절차가 단순하고, 완성된 $C(k, n)$에 따라 (k, k)-VCS의 기저행렬에 대한 행으로 치환한 후, 같은 열을 제거하는 것만으로 가능하다.

또한, 제안기법은 누적행렬을 완성하고, 그것에 의존하여 (k, k)-VCS를 위한 기저행렬의 행을 치환하면 모든 일반 접근구조를 위한 기저행렬로 확장할 수 있다. 서로 다른 작은 규모의 접근 구조 두 개를 따로 구성한 후, 결합하여 큰 규모의 일반 접근구조의 기저행렬을 구성하는 Stinson기법[8]에 비해 하나의 누적행렬로 동일한 기저행렬을 얻을 수 있는 개선된 기법이다.

V. 결 론

(k, n)-VCS가 Naor & Shamir에 의해 제안된 이후, 휘도 개선과 확장 화소의 수를 줄이기 위한 연구가 끊임없이 계속되어 왔다. 시각 비밀분산기법은 접근구조에 의한 방법 등 다양한 방향으로 응용이 되고 있는 가운데 Droste방식이 확장 화소의 수와 휘도의 관점에서 현재 가장 좋은 결과를 보이고 있다. 본 논문에서는 (k, n)-VCS의 기저행렬을 누적행렬 $C(k, n)$를 이용하여 최적인 상태를 유지하면서 구성하고, 같은 열을 제거할 수 있는 간단한 방법을 제안하였다. 그 결과, k가 홀수일 때는 Droste 방식과 같은 휘도 값을 얻을 수 있었으며, k가 짝수일 때는 휘도를 조절하여 평균 휘도를 개선할 수 있고, 특별한 조합에 대한 휘도를 최대화할 수 있음을 보였다. 또한, 누적행렬을 이용하여 일반 접근구조를 위한 기저행렬을 구성할 수 있음을 보였다. 향후, 제안기법의 성질을 엄밀히 증명하는 과제가 남아 있다.

참 고 문 헌

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

[2] M. Naor & A. Shamir, "Visual Cryptography", Advances in Cryptology-EUROCRYPT'94, Perugia, Italy, pp. 1~12, May 1994.

[3] M. Kim, J. Park, S. Park, K. Kim, "A Study on Secret Sharing Scheme Using Visual Cryptography", Proc. of SCIS97, 25B, 1997.

[4] M. Kim, S. Shin, J. Park, "New Construction for Multiple Visual Secret Sharing", Proc. of SCIS2000, B44, 2000.

[5] M. Naor, A. Shamir, "Visual Cryptography II", Lecture Notes in Computer Science 1189, pp. 179~202, 1997.

[6] H. Koga, H. Yamamoto, "Proposal of Lattice-Based Visual Secret Sharing Scheme for Color and Gray-Scale Images", IEICE Trans. on Fundamentals, Vol. E81-A, No.6, pp. 1262~1269, 1998.

[7] Y. Hou, C. Chang, "Visual Cryptography for Color Images Without Pixel Expansion", Proc. of CISST'2001, Las Vegas, Nevada, USA, Vol.1 pp. 239~245, Jun. 2001.

[8] G. Ateniese, C. Blundo, A. De Santis & D. R. Stinson, "Visual Cryptography for General Access Structure", Information and Computation 129, pp. 86~106, 1996.

[9] C. K. Choi, J. H. Park, R. Kohno, "Contrast Analysis According to Hierarchical Access Structure of Visual Cryptography Scheme and Its Application into Authentication", Proc. of SITA, Vol. 20 No. 1 pp. 217~220 1997. 12.

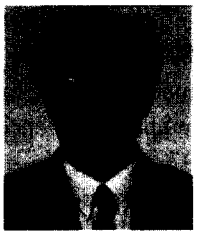
[10] S. Droste, "New Results on Visual Cryptography", Advanced in Cryptology-CRYPTO'96, pp. 401~415, Aug. 1996.

[11] C. K. Choi, S. S. Yang, J. H. Park and R. Kohno, "New construction for improving contrast in visual cryptography", Proc. of The 1998 International Symposium of Information Theory and Its Applications, Vol. 2, pp. 368~371, 1998.

[12] Y. Suga, K. Iwamura, K. Sakurai, H. Imai, "Visual Secret Sharing Scheme for Access Structures Based on Graphs", Proc. of Spring Conf. of IPSJ, S3, pp. 163~168, 2001.3 (in Japanese)

[13] 양신석, 김문수, 박지환, "시각암호의 휘도 개선을 위한 새로운 구성법", 한국 멀티미디어학회 논문지 제4권, 제2호, pp. 135~144, 2001.

〈著者紹介〉



김 문 수 (Moon-Soo Kim)
1982년 2월 : 부산대학교 수학교육과 졸업
1997년 8월 : 부산대학교 수학교육과 석사
1998년 8월 : 부경대학교 전자계산학과 박사과정 수료
2000년 3월~현재 : 부산여자고등학교 교사
2002년 2월 : 부경대학교 전자계산학과 박사졸업 예정
〈관심분야〉 정보보호 및 정보이론

박 지 환 (Ji-Hwan Park)
1990년 3월: 일본 요코하마국립대학 전자정보공학 졸업(공학박사)
1994년 9월~1995년 3월: 동경대학 생산기술연구소 방문연구
1996년 4월~현재: 동경대학 생산기술연구소 협력연구원
1999년 7월~1999년 8월: 호주 Monash University, Visiting Research
1990년 3월~현재 : 부경대학교 전자컴퓨터정보통신공학부 교수
2000년 1월~2000년 2월 : University of Electro-communications, Japan, Visiting
2001년 2월~2001년 3월 : Communication Research Lab., STA Fellow Ship
〈관심분야〉 정보이론 및 응용, 암호학 및 정보보안