시각암호에서 부화소를 줄이기 위한 새로운 구성법

양신석, 박지환
부경대학교 전산정보학과

New Construction for Reducing the Number of Subpixel in Visual Cryptography

Sin-Sok Yang, Ji-Hwan Park
Dept. of Computer and Information, PuKyong Nat'l University

요 약

시각암호는 n개로 분산된 비밀화상을 슬라이드와 같이 물리적으로 중첩 가능한 곳에 인쇄하여 그룹내 n명에게 슬라이드를 배포한 후, 임의의 k명 이상의 슬라이드를 겹치면 비밀화상을 복원할 수 있지만, $k-1$명 이하의 슬라이드를 겹치는 경우에는 비밀화상을 복원할 수 없는 방식이다. 이 논문에서는 (k, n) 시각암호의 휘도(contrast)를 개선하기 위한 구성법에서 모든 경우에 동일 휘도를 유지하면서 부화소의 수를 줄이기 위한 새로운 구성법을 제안한다.

1. 서론

중요한 비밀정보를 누출 또는 누설로부터 안전하게 관리하기 위해서 그 정보를 여러 개로 분산하여 임의의 문턱치(threshold)를 만족하면 비밀값을 결정하고, 만족하지 않으면 비밀값을 결정할 수 없도록 하는 비밀 분산법이 1979년 A. Shamir에 의하여 제안되었다[1]. 이 방식은 비밀의 분산과 복호에 있어서 연산량이 많고 구성이 복잡한 문제점이 있다. 따라서 인간의 시각이 복호기 역할을 하도록 하여 복잡한 암호학적 연산없이 간단히 비밀을 복호할 수 있는 시각암호가 1994년 M. Naor와 A. Shamir에 의해 제안되었다[2].

(k, n) 시각암호 방식(VCS:Visual Cryptography Scheme)은 비밀정보를 n개의 share의 형태로 분산하여 각 share를 슬라이드 형태로 인쇄하여 n명에게 배포한 후, k장 이상의 서로 다른 슬라이드를 중첩해야만 비밀정보를 복원할 수 있도록 하는 것이다.

시각암호 방식의 기본은 흑과 백의 화소(pixel)로 구성된 원 화상에 대하여 각 화소는 n개의 share로 분산되고, 각 share는 m개의 부화소(subpixel)로 확대된다. 상대적 차이(relative difference) α를 결정하는 중요한 파라미터인 부화소의 크기 m이 커지면, α가 너무 작아져서 복원화상의 시각적 인식이 어렵다. 따라서 m을 작게하여 상대적 차이 α를 높이거나[3-6], m에 의존하지 않으면서 복원화상의 흑과 백화소 사이의 휘도를 높이는 방법이 요구된다. 이 때 m의 크기가 너무 커지게 되면 현실

이 연구는 1997년도 한국과학재단 연구비 지원에 의한 결과의 일부임. 과제번호 971-0905-030-1

적으로 구현하는데 어려움이 따르므로 m의 크기를 줄이기 위해서 복수 휘도를 허용하는 구조를 고안하게 되었다[7].

본 논문에서는 m에 의존하지 않으면서 복원 화상의 휘도를 높이는 (k, n) 시각암호 방식의 일반적인 구성법에 있어서 모든 경우에 동일한 휘도를 유지하면서 m의 크기를 줄일 수 있는 새로운 방법을 제안한다.

2. 시각암호

2.1 기본모델

시각암호에 의한 비밀분산 문제의 가장 간단한 형태는 흑(1)과 백(0)의 화소로 구성된 이진화상(binary image)에 적용하는 것이다. 이때, 각 화소는 따로 조작될 수 있다고 가정한다. 비밀화상의 각 화소는 n장의 슬라이드에 각각 m개의 부화소로 확장되어 분산되며, 이것을 share라 부른다.

이 구조는 비밀화상의 각 화소를 $n \times m$ 부울 행렬 $S=[\,s_{ij}\,]$로 표현할 수 있으며, 이때 s_{ij}의 값은 i번째 share 중 j번째 부화소가 흑인 경우에 1, 백인 경우에 0이 된다. share들을 정확히 일치하도록 겹쳤을 때, 행렬 S의 행의 불리언 "or"로 표현되는 결합 share를 볼 수 있다. 결합 share의 grey레벨은 "or" 연산을 한 m차 벡터 V의 해밍 가중치 $H(V)$에 비례한다. 이 grey레벨은 어떤 고정된 문턱치 $1 \le d \le m$와 상대적인 차 $\alpha > 0$에 대해서 $H(V) \ge d$이면 흑으로, $H(V) \le d - \alpha \cdot m$이면 백으로 인식된다.

[정의] (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 세 가지 조건을 만족하면 (k, n)-VCS의 해가 유효하게 된다.

1. C_0의 임의의 행렬 S_0에 대해서, n행 중 임의의 k행의 "or" 연산시 m차 벡터 V의 해밍 가중치는 $H(V) \le d - \alpha \cdot m$을 만족한다.
2. C_1의 임의의 행렬 S_1에 대해서, n행 중 임의의 k행의 "or" 연산시 m차 벡터 V의 해밍 가중치는 $H(V) \ge d$를 만족한다.
3. $q < k$인 $\{1, 2, \cdots, n\}$의 임의의 부분집합 $\{i_1, i_2, \cdots, i_q\}$에 대해서, $C_t(t \in \{0, 1\})$의 각 $n \times m$ 행렬을 $i_1, i_2, \cdots, i_q$행으로 제한하여 얻은 $q \times m$ 행렬의 집합 $D_t(t \in \{0, 1\})$는 동일한 빈도를 갖는 동일한 행렬을 포함한다.

조건1과 2는 share를 겹쳤을 때 복원된 화상에서의 휘도를 나타내고, 조건3은 k장미만의 share를 겹쳤을 때 분산된 화소가 흑인지 백인지를 구분할 수 없는 안전성(security)을 나타낸다.

2.2 (k, k)-VCS

(k, k)-VCS를 구성하기 위하여 k개의 원소를 갖는 전체집합 $W=\{e_1, e_2, \cdots, e_k\}$와 원소의 개수가 짝수인 부분집합 리스트 π_1, π_2, $\cdots$, $\pi_{2^{k-1}}$과 원소의 개수가 홀수인 부분집합 리스트 σ_1, σ_2, $\cdots$, $\sigma_{2^{k-1}}$을 생각하자.

$1 \le i \le k$와 $1 \le j \le 2^{k-1}$에 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 $k \times 2^{k-1}$ 행렬이다. C_0와 C_1은 S_0와 S_1의 열들을 교환해서 만든 행렬의 집합을 나타낸다. 이 때, $m=2^{k-1}$, $\alpha = \frac{1}{2^{k-1}}$이 된다.

3. 휘도개선을 위한 (k, n)-VCS의 일반화 구성법

3.1 구성원리

먼저, 이미 구성되어 있는 (k, k)-VCS의 S_0와 S_1의 각 행에 인덱스 r_1, r_2, $\cdots$, r_k를 부여한다. 이 때, 각 화소의 크기를 m_k라 하면 $m_k=2^{k-1}$이 되고, $r_i(S_j)$ $(i \in \{1, 2, \cdots, k\}, j \in \{0, 1\})$는 S_j상의 r_i행을 구성하는 행 벡터를 나타낸다.

둘째, 각 행 r_1, r_2, $\cdots$, r_k를 각각 p, q, $\cdots$, s개씩 중복하여 n행으로 된 벡터 V를 구성한다. 단, $p+q+\cdots+s=n$, $p \ge q \ge \cdots \ge s \ge p-1$이다.

끝으로 행 교환에 의한 모든 열들을 연결하여

$$m=\frac{m_k\times {}_nC_p\times {}_{n-p}C_q\times\cdots\times {}_sC_s}{R_1!\times R_2!} \qquad (1)$$

인 백 화소를 위한 S_0'와 흑 화소를 위한 S_1'의 행렬을 구할 수 있다. 단, R_1, R_2는 중복 횟수가 같은 행의 가지수를 나타낸다.

[예제1] (2, 4)-VCS의 구성 예

(2,2)-VCS의 $S_0=\begin{pmatrix}1&0\\1&0\end{pmatrix}$, $S_1=\begin{pmatrix}1&0\\0&1\end{pmatrix}$이므로 $r_1(S_0)=(1,0)$, $r_1(S_1)=(1,0)$, $r_2(S_0)=(1,0)$ 및 $r_2(S_1)=(0,1)$이 된다.

$n=4$이므로 2번씩 중복하면 각 행벡터 $V=(r_1, r_1, r_2, r_2)$가 된다. 따라서, (2,4)-VCS에서의 S_0'와 S_1'은 $S_0'=\begin{pmatrix}1&0\\1&0\\1&0\\1&0\end{pmatrix}$, $S_1'=\begin{pmatrix}1&0\\1&0\\0&1\\0&1\end{pmatrix}$로 된다.

V에 대하여 모든 행 교환에 의한 열의 연결을 취하면

$$M=\begin{pmatrix}r_1 r_1 r_1 r_2 r_2 r_2\\ r_1 r_2 r_2 r_1 r_1 r_2\\ r_2 r_1 r_2 r_1 r_2 r_1\\ r_2 r_2 r_1 r_2 r_1 r_1\end{pmatrix}$$

가 된다. 그런데 모든 열에는 r_1과 r_2가 각각 2번씩 있으므로 교환에 의하여 중복된 부분을 제거하면

$$M'=\begin{pmatrix}r_1 r_1 r_1\\ r_1 r_2 r_2\\ r_2 r_1 r_2\\ r_2 r_2 r_1\end{pmatrix}$$

로 된다. 따라서, M'를 S_0와 S_1에 적용시키면

$$S_0'=\begin{pmatrix}1&0&1&0&1&0\\1&0&1&0&1&0\\1&0&1&0&1&0\\1&0&1&0&1&0\end{pmatrix} \qquad S_1'=\begin{pmatrix}1&0&1&0&1&0\\1&0&0&1&0&1\\0&1&1&0&0&1\\0&1&0&1&1&0\end{pmatrix}$$

로 되며, m의 크기는 $\frac{2^{2-1}\times {}_4C_2\times {}_2C_2}{2!\times 0!}=6$, $\alpha=\frac{1}{3}$이 된다.

3.2 휘도 분석

(k, k)-VCS가 구성되면 행렬의 구성원리에 따라 (k, n)-VCS로의 확장이 가능하다. 이 때, 임의의 k장을 선택할 때의 S_0'와 S_1'의 각 열의 연결 중 $(r_1, r_2, \cdots, r_k)$가 각각 한 개씩 포함될 때 상대적인 차가 생긴다. 전체 조합의 수가 $2^{k-1}\times {}_nC_k$ (단, $p+q+\cdots+s=n$)일 때 $(r_1, r_2, \cdots, r_k)$를 포함하는 열은 $p\times q\times\cdots\times s$회 나타나므로 휘도

$$\alpha=\frac{p\times q\times\cdots\times s}{2^{k-1}\times {}_nC_k} \qquad (2)$$

이다. 여기서 $n\le pk$이므로 $\lim_{n\to\infty}\alpha=\frac{(k-1)!}{(2k)^{k-1}}$가 된다. 즉, n이 증가할 때 m에 의존하지 않고 k에만 의존하므로 휘도가 매우 뛰어난 (k, n)-VCS를 구성할 수 있다.

[예제2] (3, 7)-VCS의 구성 예

(3, 3)-VCS의 S_0와 S_1을 구하면

$$S_0=\begin{pmatrix}1&1&0&0\\1&0&1&0\\0&1&1&0\end{pmatrix}, \quad S_1=\begin{pmatrix}1&1&0&0\\1&0&1&0\\1&0&0&1\end{pmatrix}$$

가 된다. 이 때,

$r_1(S_0)=(1,1,0,0)=r_1(S_1)$

$r_2(S_0)=(1,0,1,0)=r_2(S_1)$

$r_3(S_0)=(0,1,1,0)$, $r_3(S_1)=(1,0,0,1)$

이 된다. $n=7$이므로 각 행 벡터는 $V=(r_1, r_1, r_1, r_2, r_2, r_3, r_3)$가 된다. 여기에서 r_2와 r_3는 중복 횟수가 같으므로 교환 가능하다. 따라서 식(1)과 식(2)에 의해 $m=840$, $\alpha=\frac{3}{35}$이 된다.

3.3 특수한 경우의 휘도 개선

S_0와 S_1의 임의의 한 열에 있는 1의 수가 같을 때 그 열을 제거한 후, 행 교환에 의하여 S_0'와 S_1'를 구성한다. 제거된 열의 수를 e라 하면

$$\alpha=\frac{p\times q\times\cdots\times s}{(2^{k-1}-e)\times {}_nC_k} \qquad (3)$$

로 개선된다.

[예제3] (3,4)-VCS에서 S_0'와 S_1'을 구성하면 다음과 같다.

$$S_0'=\begin{pmatrix}1&1&0&0\\1&1&0&0\\1&0&1&0\\0&1&1&0\end{pmatrix}, \quad S_1'=\begin{pmatrix}1&1&0&0\\1&1&0&0\\1&0&1&0\\1&0&0&1\end{pmatrix}$$

여기에서 S_0'의 3열과 S_1'의 2열은 각각 1을 2개씩 포함하므로 이 두 부분을 제거하면($e=1$)

$$M'=\begin{pmatrix}r_1 r_1 r_1 r_2 r_2 r_2\\ r_1 r_2 r_2 r_1 r_1 r_3\\ r_2 r_1 r_3 r_1 r_3 r_1\\ r_3 r_3 r_1 r_3 r_1 r_1\end{pmatrix}$$

이 된다. 여기서 $m_k=3$이므로 $m=18$인 S_0''와 S_1''

를 구성할 수 있다. 이 때 식(3)에 의해 $\alpha=1/6$이 되어 식(2)에 의한 $\alpha=1/8$ 보다 휘도가 개선됨을 알 수 있다.

4. (k, n)-VCS의 새로운 구성법

3.1절의 구성방법을 이용하면 n의 크기가 $2k$이상으로 커질 때 S.Droste의 구성법[3]에 비해서 휘도는 상당히 개선할 수 있으나(표1), m의 크기가 너무 커져 현실적으로는 구현이 곤란하게 된다. 이 장에서는 [7]에서 제안한 방법과 휘도는 같고 임의의 k장을 선택할 때에 동일 휘도를 유지하면서 m의 크기를 줄일 수 있는 (k, n)-VCS의 새로운 구성법을 제안한다.

(k, k)-VCS에서의 S_0, S_1의 행을 $r_1, r_2, \cdots, r_k$로 구분하여 중복할 때, (k, n)-VCS에서는 S_0', S_1'의 각 열을 분석하면 흑(1)과 백(0)의 중복횟수가 같은 열이 존재한다. 이 열들을 제거한 후, 각각의 열들의 모든 조합을 비율에 맞게 중복하여 나열하면 m의 크기를 줄일 수 있는 새로운 모델을 구성할 수 있다. 이 조건을 만족하면서 m의 크기를 최소로 하는 알고리즘은 다음과 같다.

[알고리즘]

(1) (k, k)-VCS의 S_0, S_1을 구성한다.

(2) S_0와 S_1의 각 행을 $r_1, r_2, \cdots, r_k$로 구분한다.

(3) 각 행을 중복시켜 $n(=p+q+\cdots+s)$행으로 구성된 S_0'와 S_1'의 각 열을 비교하여 흑(1)과 백(0)의 중복횟수가 같은 열들을 제거한다.

(4) S_0'와 S_1'의 남은 각 열에서 흑(1)의 개수가 같은 열의 수를 확인하고 이들의 모든 조합을 찾아 개수에 따른 비례로서 중복 나열한다.

(5) m의 크기를 최소로 하는 백화소 S_0''와 흑화소 S_1''를 구성한다.

[예제4] (3,4)-VCS의 구성

예제3에서 구성된 S_0'와 S_1'의 각 열을 비교하면 흑(1)의 개수가 2인 열을 하나 제거할 수 있다. S_0'의 남은 각 열에서 흑(1)의 개수가 0인 것이 한 개, 흑(1)의 개수가 3인 것이 두 개 있다. 또 행 교환에 의한 열의 연결을 취하면 ${}_4C_3=4$, ${}_4C_0=1$이 된다. 따라서 ${}_4C_3:2\cdot{}_4C_0=2:1$이 되고 $m={}_4C_3+2\cdot{}_4C_0=6$이 된다. 같은 방법으로 S_1'의 남은 각 열에서도 $m=6$이 되어 다음과 같이 백화소 S_0''와 흑화소 S_1''를 구성할 수 있다.

$$S_0''=\begin{pmatrix}111000\\110100\\101100\\011100\end{pmatrix},\quad S_1''=\begin{pmatrix}111000\\110100\\110010\\110001\end{pmatrix}$$

위의 접근법을 적용하면 [7]에서 제안된 방법에 비해서 m의 크기를 줄일 수 있다(표2).

[예제5] (3,9)-VCS의 구성

$$S_0'=\begin{pmatrix}1100\\1100\\1100\\1010\\1010\\1010\\0110\\0110\\0110\end{pmatrix},\quad S_1'=\begin{pmatrix}1100\\1100\\1100\\1010\\1010\\1010\\1001\\1001\\1001\end{pmatrix}$$

이 된다. S_0'에서 ${}_9C_6$의개수:${}_9C_0$의개수$=3:1$이므로 S_0''의 m=84+28=112이고 S_1'에서도 같은 방법으로 m=112를 구할 수 있다. 이를 이용하여 구성된 S_0''와 S_1''는 [7]의 구성법에 비해서 같은 휘도를 유지하면서도 m이 $\frac{1}{10}$로 줄어드는 것을 알 수 있다(표2).

5. 고찰 및 향후 과제

시각암호의 휘도를 개선하기 위하여 $(2, n)$-VCS에 대한 여러 가지 연구가 있었고[4,5], $(2, n)$-VCS 이상의 시각암호에 대해서는 S. Droste에 의해 m을 줄임으로서 휘도를 개선하기 위한 연구가 있었다[3]. m에 의존하지 않으면서 휘도를 개선하기 위한 구성법에서는 S.Droste 방법에 비해서 n이 $2k$이상일 경우에 휘도가 많이 개선되는 특징이 있으나(표1), m의 크기가 커지는 단점이 있어서 복수 휘도를 허용하는 경우에 m의 크기를 줄이기 위한 구성법이 제시되었다[7].

본 논문의 제안방식은 [7]과 같은 휘도를 유지하면서 m의 크기를 최소화하기 위한 새로운 접근법으로서 동일 휘도를 유지해야 할 필요가 있을 때 유용하다.

앞으로 접근구조에 따라 m의 크기를 더욱 줄일 수 있는 구성법을 모색하거나 휘도를 개선하기 위한 새로운 방법 모색, 복수의 휘도를 허용할 경우의 일반화된 행렬 구성법의 연구 및 제안방식을 적용하여 m의 크기를 최소화 하기 위한 연구가 향후의 과제이다.

[참고문헌]

[1] A. Shamir, "How to Share a Secret", Communications of the ACM, Vol. 22, no 11, pp.612-613, Nov. 1979.

[2] M.Naor and A. Shamir, "Visual cryptography", in Advances in Cryptology-Eurocrypt'94, Springer-Verlag, pp.1-12, 1995.

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

[4] D. R. Stinson, "Combinatorial Designs with Selected Applications Lecture Notes", Dec. 1996.

[5] 최창근, 박지환, "시각암호의 접근구조에 따른 비밀 정보의 계층적 접근과 contrast의 분석", 정보처리학회 춘계학술발표대회 4권 1호 pp.1032-1037, 1997. 4.

[6] 김미라, 박지환 "시각암호에 의한 비밀 분산법", 통신정보보호학회 논문지 제 7권 4호, pp.37-50, 1997. 12.

[7] 양신석, 김미라, 박지환 "시각암호에서 휘도개선을 위한 새로운 구성법", 정보처리학회 춘계학술발표대회, 1998. 4.

표1. S.Droste방식과 YKP[7]방식과의 휘도 비교

k\n	방식	2	3	4	5	6	7	8	9	10	11	12	n→∞
2	S · D	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9	1/10	1/11	1/12	1/n
	YKP[7]	1/2	1/3	1/3	3/10	3/10	2/7	2/7	5/18	5/18	3/11	3/11	1/4
3	S · D		1/4	1/6	1/8	1/10	1/12	1/14	1/16	1/18	1/20	1/22	$1/2(n-1)$
	YKP[7]		1/4	**1/6**		1/10	3/35	9/112	9/112	3/40	4/55	4/55	1/18
4	S · D			1/8	1/15	1/24	1/35	1/48	1/63	1/80	1/99	1/120	$1/\{(n-1)^2-1\}$
	YKP[7]			1/8	**1/15**	**2/45**	8/245	1/35	1/42	3/140	9/440	9/440	3/256
5	S · D				1/16	1/30	1/48	1/70	1/96	1/126	1/160	1/198	$1/2\{(n-2)^2-1\}$
	YKP[7]				1/16	**1/30**				1/126	1/154	**1/165**	3/1250

* 음영은 휘도 개선이 안된 부분이고, 강조체는 특수한 경우에 휘도 개선이 된 부분임.

표2. YKP[7]방식과 제안방식과의 m크기 비교

k\n	방식	2	3	4	5	6	7	8	9	10	11	12
2	YKP[7]	2	6	6	20	20	70	70	252	252	462	462
	제안	2	6	6	20	20	70	70	252	252	462	462
3	YKP[7]		4	18	60	60	840	1120	1120	8400	23100	23100
	제안		4	6	20	20	420	112	112	840	660	660
4	YKP[7]			8	60	270	840	840	10080	25200	61600	61600
	제안			8	30	90	280	280	672	5040	6160	6160
5	YKP[7]				16	60	1155	4620	15120	15120	277200	386100
	제안				16	30	231	308	1008	1008	18480	7040