시각암호 구성법에 관한 고찰

최 창근* 박 상우** 박 지환*

부경대학교 전자계산학과* 한국전자통신연구소**

A Study on Visual Cyrptography Constructions

Chang Keun Choi* Sang Woo Park** Ji Hwan Park*

Dept. of Computer Science PuKyong Nat'l University*

Electronics and Telecommunications Research Institute**

요 약

Naor & Shamir는 시각 암호에 관한 기본 개념을 제시하고 이를 위한 구성법을 제안하고 있다. 이는 복잡한 암호학적인 계산 없이 숨겨진 비밀을 복호하는 새로운 암호 형태로서 대단히 안전하고 구현이 용이하다는 장점을 가지고 있다. 본 논문에서는 $(2, n)$ 시각 비밀 분산법의 여러 방법들에 대하여 고찰 한다. 또한, 시각 암호의 실질적인 응용의 효과를 기대할 수 있는 농담화상에 적용하기 위한 시각 암호의 구성법과 실제 구현결과를 보인다.

1. 서론

비밀 분산법이라는 것은 정당한 자격을 가진 참여자들의 부분집합으로서 자신에게 할당된 비밀키를 결합함으로써 비밀 값을 결정할 수 있는 것으로서 정당한 참여자가 아닌 경우에는 비밀 값의 결정이 불가능하도록 비밀을 분산하는 방법이다. 그러나, 이 방식은 비밀의 분산과 복호에 있어서 안전성을 유지하기 위해 방대한 연산량과 복잡한 구성 때문에 고성능 컴퓨터를 요구하였다. 최근, 새로운 형태의 비밀 분산법으로 비밀 키로서 화상을 이용함으로서 많은 연산을 하지 않아도 시각적으로 복호 할 수 있는 새로운 시각암호가 Naor & Shamir[1]에 의하여 제안 되었다.

시각암호는 주어진 n장 중에 임의의 k장 이상 겹쳐지게 되면 원래 복호하고자 하는 비밀정보가 나타나게 되나, k장 미만 겹쳐지게 되면 복호가 불가능 하게 되는 것으로서 단순히 인간의 시각으로도 복호가 용이한 비밀 분산법의 하나이다. 이 방법은 원래의 비밀 화상이 주어졌을 때 원화상의 한 화소에 대해서 m개의 부화소들로 나누어져 구성되는 슬라이드들로 표현된다.

본 논문에서는 먼저 Naor & Shamir[1]의 시각 암호에 대한 기본적 모델과 이의 결과를 보인다. 두 번째, $(2, n)$의 시각 암호의 일반적인 방법, Naor & Shamir의 새로운 방법[2], Katoh & Imai가 제시한 방법[3]과 보수화에 의한 새로운 방법에 대해 비교분석 한다. 마지막으로 시각 암호를 gray level에 적용 하기 위한 행렬 구성법과 이의 결과를 나타낸다.

2. Naor & Shamir 시각암호

2.1 기본 Model

시각 비밀 분배 문제의 가장 간단한 방법은 화상이 흑과 백의 집합으로 구성되어 있고, 각 화소는 모두 개별적으로 다루어지는 것으로 가정한다. 원 화상은 n개의 share로 구성되어지는 각각의 슬라이드에 일괄적으로 분배되어진다. 따라서, 각 share는 m개의 흑과 백의 부화소들의 집합이며, 시각적 인식이 가능하도록 근접하여 인쇄되어진다. 이 구조는 $n \times m$의 부울 행렬인 $S=[s_{ij}]$로 표현되어지며, s_{ij}=1의 의미는 i번째 슬라이드의 j번째 부화소가 흑임을 나타낸다. $i_1, i_2, \ldots, i_r$의 슬라이드들이 겹쳐졌을 때 해밍 가중치는 결합되는 share의 gray-level이 "or" 되어진 m벡터 V의 해밍 가중치 $H(V)$에 비례하게 된다. 이 gray 단계는 고정된 문턱치 $1 \le d \le m$와 상대적 차 $\alpha > 0$에 대하여 만약 $H(V) \ge d$이면 흑 그리고 $H(V) < d - \alpha m$이면 백으로 인간의 시각 체계에 의해 인식된다.

[정의 1]

만약 다음의 세가지 조건들을 만족하게 되면 contrast $\alpha(\ge 1/m)$ 그리고 문턱치 d인 n개에서 k개를 뽑아내는 시각 비밀 분배 문제는 $n \times m$부울 행렬 C_0와 C_1인 두 개의 집합으로 구성된다.

1. **C_0내의 임의의 S에 대해서, S의 n행들 중에서 임의의 k에 대해 "or"되어진 V는 $H(V)(<d-\alpha \cdot m)$를 가진다.**
2. **C_1내의 임의의 S에 대해서, S의 n행들 중에서 임의의 k에 대해 "or"되어진 V는 $H(V)(\ge d)$를 가진다.**
3. **$q < k$인 $\{1, 2, \ldots, n\}$의 임의의 부분집합$\{i_1, i_2, \ldots, i_q\}$에 대하여, C_0와 C_1에 제한을 가함으로써 얻어지는 행들 $i_1, i_2, \ldots, i_q$는 항상 모두 동일한 확률을 가지게 된다.**

조건3의 경우는 아무리 강력한 암호 분석이 가능한 컴퓨터조차 k개 보다 작은 share의 "or"에서는 분배되어진 화소의 흑/백에 관한 결정을 할 수 있는 정보의 획득이 불가능하다. 위의 조건1과 2는 contrast를 의미하고 조건3은 security를 의미한다. 이 방식에서의 중요한 파라미터들로서 α는 원화상이 얼마나 잘 나타날 수 있는지를 결정하는 "or"되어진 share간에서의 contrast의 상대적인 차를 의미하며, m은 원화상의 분배시 해상도의 손실을 나타내는 것으로 가능한 이의 크기를 작게 해야 하는 부화소의 수를 의미하며, r은 화질의 영향을 주지 않는 C_0와 C_1의 크기로서 $\log r$은 share를 나타내기 위해 필요한 임의의 비트수를 의미한다.

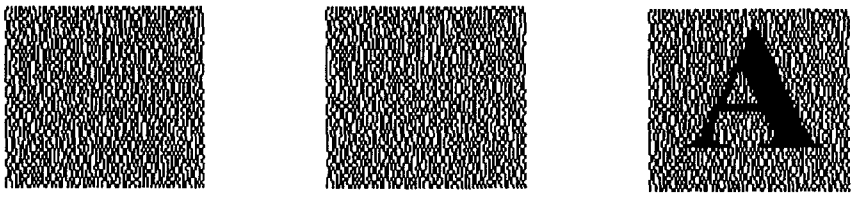
2.2 시각 암호를 위해 제안된 여러 구성법

n개의 시각 비밀 분배 문제에서 두 개를 추출해내는 경우는 아래의 $n \times n$ 부울 행렬들의 집합에서 가능하다.

$$C_0 = \{ \begin{pmatrix} 100\ldots0 \\ 100\ldots0 \\ \cdots \\ 100\ldots0 \end{pmatrix} \text{의 열들을 교환함으로써 생성되는 모든 행렬들} \}$$

$$C_1 = \{ \begin{pmatrix} 100\ldots0 \\ 010\ldots0 \\ \cdots \\ 000\ldots1 \end{pmatrix} \text{의 열들을 교환함으로써 생성되는 모든 행렬들} \}$$

C_0와 C_1 각각에서 임의의 한 share는 한 개의 흑과 $n-1$개의 백 부화소들로 구성되는데, C_0에서 임의의 두 share의 "or"되어진 $H(V)$의 값은 1인, 반면에 C_1에서 임의의 두 share의 "or"되어진 $H(V)$의 값은 2로서 더 어두워지게 된다. 시각암호의 기본 문제는 두 개의 시각 비밀 분배 문제에서 두 개를 추출해내는 아주 간단한 경우로부터 시작한다. 이는 원화소에 대해 부화소를 두 개를 할당하는 방법으로 이루어지지만, 종횡비의 왜곡을 방지하기 위해 부화소의 상태를 정방향으로 m을 구성하여 원화상에 대한 왜곡의 차를 줄일 수 있으나 반드시 정방향의 형태를 유지할 필요는 없다. 그림1에 (2,2) 시각 비밀분산법의 결과를 나타냈다.



(a)슬라이드1 (b)슬라이드2 (c)슬라이드1,2의 중첩시

그림1. (2,2) VSS의 시각암호

다음은 Naor & Shamir에 의해 제안된 일반화된 (k,k)의 구성법에 관한 것으로 2^{k-1}의 부화소를 사용하여 k에서 k를 추출해내는 시각 비밀 분배 문제를 보인다. k개의 원소들을 가지는 전체 집합 $W=\{e_1, e_2, \ldots, e_k\}$를 고려하자. 그리고 $\pi_1, \pi_2, \ldots, \pi_{2^{k-1}}$는 짝수의 모든 부분 집합들의 리스트로 두고, $\sigma_1, \sigma_2, \ldots, \sigma_{2^{k-1}}$은 W의 홀수의 모든 부분 집합들의 리스트라 두자.

S^0와 S^1은 $1 \le i \le k$와 $1 \le j \le 2^{k-1}$에 대하여, $e_i \in \pi_j$일 때만 $S^0[i,j]=1$, 반면에 $e_i \in \sigma_j$일 때만 $S^1[i,j]=1$을 가지는 $k \times 2^{k-1}$행렬들로 정의된다. 파라미터 $m=2^{k-1}$, $\alpha = 1/2^{k-1}$ 그리고 $r=2^{k-1}!$을 가지는 (k,k)이다. 예를 들면, $k=4$일 때

$W=\{e_1, e_2, e_3, e_4\}$

$$\begin{cases} \pi_1=\{\}, & \pi_2=\{e_1,e_2\}, \ \pi_3=\{e_1,e_3\}, \\ \pi_4=\{e_1,e_4\}, & \pi_5=\{e_2,e_3\}, \ \pi_6=\{e_2,e_4\}, \\ \pi_7=\{e_3,e_4\}, & \pi_8=\{e_1,e_2,e_3,e_4\} \end{cases} \quad \begin{cases} \sigma_1=\{e_1\}, \sigma_2=\{e_2\}, \ \sigma_3=\{e_3\}, \ \sigma_4=\{e_4\}, \\ \sigma_5=\{e_1,e_2,e_3\}, \ \sigma_6=\{e_1,e_2,e_4\}, \\ \sigma_7=\{e_2,e_3,e_4\}, \ \sigma_8=\{e_1,e_3,e_4\} \end{cases}$$

$$S^0 = \begin{pmatrix} 01110001 \\ 01001101 \\ 00101011 \\ 00010111 \end{pmatrix}, \qquad S^1 = \begin{pmatrix} 10001101 \\ 01001110 \\ 00101011 \\ 00010111 \end{pmatrix}$$

치환행렬	모두 0인 열의 수	x개 행을 "or"시 1의 수	
		x=k=4	x=k-1=3
S^0	1	$2^{4-1}-1=7$	7
S^1	0	$2^{4-1}=8$	7

즉, S^0와 S^1중의 임의의 $(k-1)$행을 겹치면 $H(V)$가 모두 7로 되어 구별이 되지 않으나, k행 겹치면 7과 8로 되어 백과 흑을 구별 할 수 있게 된다. 그림2에 $k=4$에 대한 (k,k) 시각 비밀 분산법의 결과를 보인다.

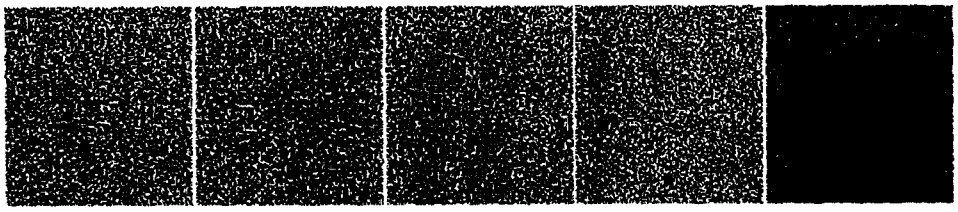


그림2. (4,4) VSS의 시각암호

3. (2 , n) Visual Secret Sharing(VSS)

3.1 Naor & Shamir의 (2 , n) VSS

2.2절의 행렬에서와 같이 C_0를 위한 행렬은 $m-1$의 0을 가진 행을 n개의 행들이 모두 같은 자리에서 1을 가지도록 구성하고, C_1을 위한 행렬은 $m-1$의 0을 가진 행을 n개의 행들이 모두 다른 자리에서 1을 갖도록 하는 단위 행렬을 구성하면 $(2,n)$ VSS를 위한 C_0와 C_1행렬을 구성할 수 있다. 따라서, 이 방식은 share의 수(n)가 증가함에 따라 share의 크기(m)가 비례하여 증가하는 단점이 있다.

3.2 Katoh & Imai의 (2 , n) VSS

Katoh & Imai는 n장중 두장을 겹쳤을때 고정 가중치 부호를 이용하여 더 효과적으로 인식할 수 있는 방법을 제시하고 있다[3]. 고정 가중치 부호에 있어서 모든 shrare들이 어떤 minimum semi-distance를 만족하는 모든 행들을 길이 m이고 가중치가 $m/2$이 되는 $\binom{m}{m/2}$ 개의 부호어중에서 C_1의 행렬을 구할 수 있다. C_0의 행렬을 위해서는 C_1의 부호어의 길이와 가중치가 같은 부호어로 1의 자리는 동일한 위치에 있도록 구성하면 겹친 해밍 가중치의 값이 항상 동일한 결과를 가진다.

이는 Naor & Shamir[1]방식에서 모든 열을 랜덤하게 교환하면 되는데 비해, 행도 열과 마찬가지로 교환을 해야하는 형태이다. 결국, 두 장을 겹쳤을때 인식의 효과는 백과 흑의 차이 뿐만 아니라, 흑과 흑 사이에서도 해밍 가중치의 차를 가지게 되어 백과의 차이는 훨씬 커진다. 그러므로 3.1의 방식보다는 초기에 시각적으로 인식이 용이하게 된다. 다음은 $(n, m)=(14, 8)$의 고정 가중치 부호를 이용하여 구성한 C_0와 C_1의 구성 예를 나타낸다.

$$C_0 = \begin{pmatrix} 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \end{pmatrix} \qquad C_1 = \begin{pmatrix} 11110000 \\ 00001111 \\ 11001100 \\ 00110011 \\ 11000011 \\ 00111100 \\ 10101010 \\ 01010101 \\ 10100101 \\ 01011010 \\ 10011001 \\ 01100110 \\ 10010110 \\ 01101001 \end{pmatrix}$$

따라서, C_1에 있어서 i장 중첩시 해밍 가중치 $H_i(V)$는 다음과 같게 된다. $H_1(V)=4$, $H_2(V) = H_3(V) = 6$ or 8, $H_4(V) = \cdots = H_{14}(V) = 8$

3.3 Naor & Shamir의 새로운 (2, n) VSS

고정의 m에 대하여 $\binom{m}{m/2} \geq n$의 조건을 만족하는 모든 부분 집합을 고려하면 $(2, n)$ VSS를 위한 행렬을 구성 할 수 있다. S^1은 위의 조건을 만족하는 모든 부분 집합들의 원소로 구성되어지고, S^0의 임의의 한 행은 $1^{m/2}0^{m/2}$으로 구성함으로서 흑/백 행렬 C_1과 C_0의 구성이 가능하게 되며 $\binom{m}{m/2}$의 수만큼 분배할 수 있는 행의 수 n이 생성된다.

3.2절과 같은 맥락으로 이 방법을 고려하게 되면 최소 거리를 만족하는 행렬을 구할 수 있다. 더욱이 3.2절의 Katoh & Imai 방법보다 훨씬 많은 share들을 생성할 수 있으므로서 비밀을 더 많은 사용자에게 분산할 수 있지만, 시각적 복호 면에서 휘도는 Katoh & Imai 방법보다 떨어지는 상호보완적인 결과를 가진다.

$$C_0 = \begin{pmatrix} 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ \vdots \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \\ 11110000 \end{pmatrix} \qquad C_1 = \begin{pmatrix} 11110000 \\ 11101000 \\ 11011000 \\ 10111000 \\ 01111000 \\ \vdots \\ 10000111 \\ 01000111 \\ 00100111 \\ 00010111 \\ 00001111 \end{pmatrix}$$

3.4 보수화에 의한 (2, n)VSS

위에서 언급한 것과 같이 share를 겹쳤을 때의 비밀화상의 선명도를 고려하면 다음의 구성법으로 선명도를 개선할 수 있다.

(1) 길이 m의 임의의 부호어를 선택한다.
(2) 위 부호어에서 1의 가중치를 가진 부분만 고려하여 서로 보수인 부호어를 생성한다.
(3) 길이 $m/2$의 단위행렬을 첨가한다.
(4) 행렬3의 각 행에 대해, 보수를 취하여 길이 m의 행으로 확대한다.
(5) 행렬4에서 처음 기준행과 그의 보수 행을 제외한 모든 행의 보수 행을 첨가 한다. $\Rightarrow C_1$

$$(11110000)\quad \begin{pmatrix}1111\\0000\end{pmatrix}\quad \begin{pmatrix}1111\\0000\\1000\\0100\\0010\\0001\end{pmatrix}\quad \begin{pmatrix}11110000\\00001111\\10000111\\01001011\\00101101\\00011110\end{pmatrix}\quad C_1 = \begin{pmatrix}11110000\\00001111\\10000111\\01111000\\01001011\\10110100\\00101101\\11010010\\11100001\\00011110\end{pmatrix}\quad C_0 = \begin{pmatrix}11110000\\11110000\\11110000\\11110000\\11110000\\11110000\\11110000\\11110000\\11110000\\11110000\end{pmatrix}$$

(1) (2) (3) (4) (5) (6)

3.5 각종 $(2, n)$ VSS의 비교 분석

3.1절의 Naor & Shamir방법 [1]보다 Katoh & Imai방법이 휘도적인 면은 양호 하지만, 3.3절의 $(2, n)$의 방법과 비교하게 되면 비밀 분산의 면에서는 큰 효능을 발휘 한다고는 할 수 없다. 이 점들을 고려할 때 보수화에 의한 비밀 분산의 크기 n은 Naor & Shamir[2] 및 Katoh & Imai[3]에 비해 떨어지지만, 휘도면에서는 양호한 $(2, n)$ 행렬 구성법이다.

고정의 m에 대해, 두 장의 share를 겹쳤을때의 각 해밍 가중치의 출현 빈도를 기준으로 백에 대한 흑의 평균 출현빈도를 계산하여 비교한다. 위의 각 $(2, n)$ VSS들은 모두 m=8일때를 기준으로 n장 중에 두 장을 겹쳤을 때 나타나는 가중치의 값 $H_2(V)$는 5, 6, 7, 8중의 한 값들을 취하게 된다. 따라서, 아래와 같이 계산되는 평균 빈도율은

$$\text{평균 빈도율} = \{\frac{1}{m}\sum_{i=1}^{m/2}[(m/2+i) \times (m/2+i)\text{의 발생 빈도}]\} \times 100\ [\%]$$

표1과 같이 되어 제안 방식이 휘도면에서 약간 우수함을 알 수 있다.

표1. 각 $(2, n)$ VSS에서 휘도 비교 ($m=8$)

방 식	Katoh & Imai	Naor & Shamir	제안방식
평균 빈도율	75.36	76.91	77.78

4. 농담 화상을 위한 시각 암호 구성법

Naor & Shamir[1] 및 Katoh & Imai[3]에 의해서 제안된 기존의 방식들은 비밀로 하고자 하는 화상에 관한 정보는 흑과 백으로만 이루어지는 이진 화상에 한하여 연구되어 왔으나, gray-level을 갖는 농담 화상이나 궁극적인 응용이 기대 되는 컬러 화상에 적용을 위한 구성법과 그 성질의 분석에 관하여는 미흡한 상태이다. 따라서, 본 논문에서는 레벨의 농담 화상에 시각암호를 적용함으로서 각 share를 겹쳤을 때 $H(V)$가 l 레벨을 가지는 구성법과 그 결과를 보인다.

4.1 (3,3) VSS에서 4 Gray Level 부호어의 존재성

[표기법]

m : 부호어의 길이
d : 임의의 두 부호어의 같은 자리에서의 가중치의 차 ⇐ Hamming distance
w : 해밍 가중치 (부호어에서 1의 개수)
c : 임의의 두 부호어 사이에서 공통의 1의 수
l : gray level
$+$: 논리적 OR
$H_i(V)$: i개의 부호어를 겹쳤을때의 해밍 가중치
$W_2^{\min}(V)$: 임의의 두 장의 슬라이드를 겹쳤을 때의 최소 가중치
$W_3^{\max}(V)$: 세 장의 슬라이드를 겹쳤을 때의 최대 가중치
M_j : 각 level j에 할당된 행렬, $j \in \{0, 1, \ldots, l-1\}$
Z_j : 모든 원소 값이 0 인 열의 수

[준비]

1. $d=w$를 고려한다.
2. $m=2w$를 만족하는 $\binom{m}{w}$ 인 전체 부호어를 고려한다.
   $m=2w$의 조건은 d를 어떤 값으로 고정하더라도 가장 많은 부호어의 생성을 가질 수 있기 때문이다[4]. 결국, w의 결정으로 인해 $H_1(V)$, c 그리고 d는 즉시 결정된다.
3. $l=\{W_3^{\max}(V)-W_2^{\min}(V)\}+1$

□

$W_3^{\max}(V) = |m|$라 가정 한다.

[정의 2]

1. 주어진 c에 대한 $H_2(V) = W_2^{\min}(V)$.
2. $H_3(V)$ 내의 임의의 두 share는 $W_2^{\min}(V)$를 만족하며, $H_3(V)$는 아래 범위의 값을 취한다.
   $$W_2^{\min}(V) \le H_3(V) \le W_3^{\max}(V)$$
   단, w는 짝수이여야 한다.

파라미터 w 가 주어지면 $H_i(V)$ ($i \in \{1, 2, 3\}$), m, d, c 그리고 M_j ($0 \le j < l$)는 결정된다. M_j의 j와 Z_j($0 \le j < l$)는 서로 차례로 대응함으로써 2의 멱승배의 gray-level을 적용하기 위해 M_j에 따른 서로 다른 $H_3(V)$를 가지는 부호어 행렬을 구성 할 수 있게 된다.

m=8의 경우를 예를 들면 $W_3^{max}(V)$의 값이 8이 되지만 $W_2^{min}(V)$를 만족하면서 구성할 수 있는 level은 최대 3가지 이상 생길 수 없으므로, 4 level을 위한 행렬의 집합 구성이 불가능하게 된다. 따라서 n=3 일때 최소의 m은 12가 된다.

4-2. l – level을 위한 행렬 구성 알고리즘

1. $\binom{m}{w}$ 인 모든 고정 가중치 부호를 생성 한다.
2. 길이는 m이고 w의 가중치를 가진 한 행을 기준으로 파라미터 c를 만족하는
   즉, $H_2(V) = W_2^{low}(V)$ 인 두 행을 찾는다.
   2-1. $W_2^{min}(V)$의 두 share와 또 새로운 한 행과의 "+"를 수행하여 $H_3(V)$가 $W_3^{max}(V)$와 같으면 이를 가장 높은 level 즉, 흑화소에 대응하는 행렬로 할당 한다.
   2-2. 2번의 과정을 반복 시행하여 새로운 제3의 행이 $W_2^{min}(V)$의 두 행과 새로운 행과의 "+" 하여 $H_3(V)$가 $W_2^{low}(V)$와 같으면 이는 가장 낮은 level 즉, 백화소에 대응하는 행렬로 할당한다.
   2-3. 2번의 루틴의 수행에서 $W_2^{min}(V) < H_3(V) < W_3^{max}(V)$를 만족하는 $H_3(V)$들을 가중치가 m의 크기와 같은 흑과 $H_1(V)$와 같은 가중치를 가진 백을 위한 level들을 제외한 level에 할당을 하게 되는데 이는 Z_j의 수에 따라 상위 level과 하위 level로 할당 할 수 있다.
3. 위의 수행으로 구성된 행렬군들 즉, $H_3(V)$의 값들로 각각 M_j에 할당 할 수 있게 된다. 즉, 이들 행렬들은 각각 서로 다른 Z_j의 값을 가지게 됨으로써 $H_3(V)$가 서로 다른 가중치를 가지는 gray level 행렬들을 가지게 된다.

그림3. 160*100 원화상(256 level)

그림4. 160*100 비밀화상 (4 level)

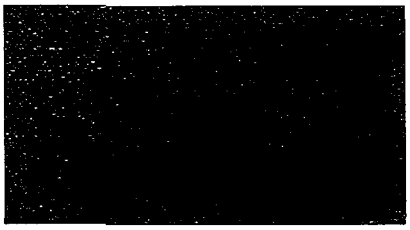


그림5. 슬라이드 1

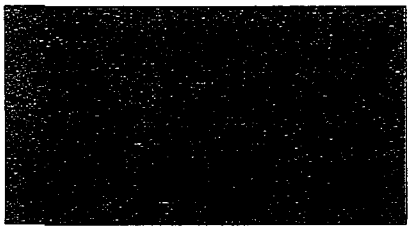


그림6. 슬라이드 2

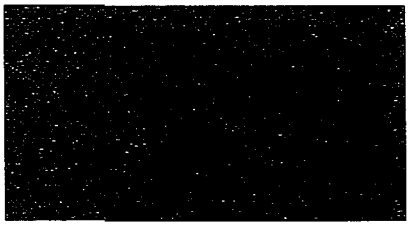


그림7. 슬라이드 3

그림8. 두 장의 슬라이드 중첩시

그림9. 세 장의 슬라이드 중첩시

5. 결론

시각암호의 기본 개념과 구성법을 소개하였으며, 간단한 실현 결과를 보였다. $(2, n)$ 시각암호의 여러 방법들을 비교하고 Katoh & Imai의 방법이 Naor & Shamir[1] 방법보다는 효과적이지만, Naor & Shamir[2]의 $(2, n)$ 방법보다는 비밀 분산의 면에서는 효과적이지 않다는 점을 지적 하였으며, 보수화에 의한 방법을 제시 하였다. 시각암호를 농담화상에 적용하기 위한 행렬의 존재성과 구성법을 보였다. 향후의 연구 과제로는 먼저 시각암호의 인증 부분에의 효과적인 활용 방안을 모색하는 것이며, (k, n) 방법에 농담 화상의 적용을 위한 새로운 행렬 구성법의 고안이다. .

6. 참고 문헌

1. M. Naor, A. Shamir, "Visual Cryptography", Proc. of Eurocrypt'94, pp.1-12, 1994
2. M. Naor, A. Shamir, "Visual Cryptography", An update version of reference 1. (http://www.wisdom.weizmann.ac.il/Papers/trs/Papers/)
3. T. Katoh, H. Imai, "On Reducing the Share Size of Visual Secret Sharing Schemes", Proc. of ISITA, vol. 4 no. 1, pp. 67-70, Sept. 1996
4. R. L. Graham N. J. A. Sloane, "Lower Bounds for Constant Weight Codes", IEEE Trans. Inform. Theory, vol. IT-26, pp. 37-43, Jan. 1980