韓國數學敎育學會誌 시리즈 E
<數學敎育 論文集>
제 22권 제 4호. 2008. 11. 515-531

J. Korea Soc. Math. Ed. Ser. E:
Communications of Mathematical Education
Vol. 22 No 4, Nov. 2008. 515-531

조합 ${}_nC_2$을 이용한 시각암호의 구현

김 문 수 (한국과학영재학교)
강 미 광 (동의대학교)

현대 사회에서 정보보안의 문제는 사회적 큰 이슈이므로 이에 필수적인 암호에 대한 사회적 관심도가 높아지고 있다. 암호기법 중 시각암호기법은 행렬과 조합, 이항정리와 같은 고등학교 수준의 수학내용이 실제로 어떻게 응용되는가를 보여줄 뿐 아니라 수학에 흥미가 있는 학생이라면 쉽게 접근할 수 있는 부분이다. 이 논문에서는 n개의 슬라이드 중 2개를 겹치면 비밀정보를 복원할 수 있는 $(2,n)$ 시각암호 기법에서 표본행렬을 이용하여 비밀분산을 가능하게 하는 방법을 소개한다. 간단한 표본행렬을 이용하여 복수의 휘도를 허용함으로서 확장 화소의 수를 대폭적으로 줄일 수 있는 구성법과 그룹화에 의해 복수의 비밀정보를 분산 및 복원시킬 수 있는 응용방법을 제안하며 이러한 방법이 확장 화소의 수와 상대 휘도의 관점에서 기존의 기법에 비해 성능이 우수함을 보이고자 한다.

1. 서 론

현대 사회는 신속한 정보처리와 전달로 인해 대량의 정보가 끊임없이 창출되어지고 급속하게 퍼져가는 정보화 사회이다. 컴퓨터 및 다양한 통신매체 기술의 발전으로 전자금융과 같이 컴퓨터를 활용한 경제활동이 일상화되고 중요한 정보는 경제적 부가가치가 높아짐에 따라 그에 따른 정보보안의 문제가 사회적 이슈로 등장하고 있다. 이처럼 정보보안 분야에 고급 인력이 많이 필요하게 될 것으로 예상되기 때문에 여느 때보다도 정보보안에 필수적인 암호에 대한 사회적 관심도가 높아지고 있다. 그래서 현재 암호는 학생들에게 수학 분야에 대한 호기심과 학문적 성취동기를 불러일으키고 수학적 지식이 어떻게 사회에 기여하는지를 알릴 수 있는 좋은 수학적 제재가 될 수 있다. 여기서 소개하는 시각암호 기법은 행렬과 조합, 이항정리와 같은 고등학교 수준의 수학내용이 실제로 암호 기법에서 어떻게 응용되는가를 보여줄 뿐 아니라 암호기법 중에서도 수학에 재능이 있는 고등학생들이라면 쉽게 접근할 수 있는 부분이므로 일부 고등학교에서 실시되고 있는 R&E 프로그램의 주제로 다루거나 대학에서 수학 관련 교양교과목의 내용으로 다루어도 좋은 실용수학의 주제이므로 소개한다.

시각암호는 복잡한 연산을 필요로 하는 일반적인 암호시스템과는 달리 인간의 시각에 의해 숨겨

* 2008년 8월 투고, 2008년 9월 심사완료
* ZDM 분류 : M95
* MSC2000 분류 : 97D99
* 주제어 : 시각암호, (k,n) 임계치 기법, 기저행렬, 표본행렬, 복수의 비밀분산

진 복원이 가능한 간편한 암호방식이다. 그림 형태의 비밀정보를 n개의 무의미한 영상으로 분산시킨 슬라이드를 사용자에게 분배한 후, 일정한 임계치 이상의 슬라이드를 겹치면 비밀 정보를 알 수 있는 비밀 분산 기법이다.

Shamir에 의해 (k,n) 비밀 분산법이 1979년에 처음으로 제안되었고, 영상 형태의 비밀정보를 갖는 시각암호가 Naor & Shamir에 의해 1994년에 제안되었다. 시각암호에서의 비밀영상은 흑과 백의 화소(pixel)로 구성되어 있으며 슬라이드와 같이 물리적 중첩이 가능한 곳에 인쇄되는 경우를 가정한다. (k,n) 비밀 분산법은 그룹 내의 n 명에게 배포된 슬라이드 중 임의의 k 명 이상의 슬라이드를 겹치면 비밀정보를 복원할 수 있지만, k 명 미만의 슬라이드를 겹치는 경우에는 비밀정보를 복원할 수 없기 때문에 안전성이 보장된다.

Naor & Shamir(1994)에 의해 하나의 비밀영상을 복원할 수 있는 시각암호가 고안된 후 많은 연구가 이루어지고 있다. Katoh & Imai(1996)는 겹친 슬라이드의 수에 따라 서로 다른 비밀영상을 복원할 수 있는 시각암호를 제안하였으며, 휘도를 개선하기 위한 Droste(1996)의 연구를 비롯하여 Ateniese, Blundo, Santis & Stinson (1996) 등은 일반적 접근구조를 갖는 경우로 확대하였고 Koga와 Yamamoto(1998)는 칼라영상과 농담영상에 적용할 수 있는 Lattice-based Visual Secret Sharing Scheme을 제안하였다. 또한, Choi 등은 계층적 접근 구조를 이용하여 비밀영상을 복원하는 방법을 제시하였다. 일반적인 비밀 분산법의 해는 유한체 상의 복잡한 연산을 수반하는 반면, (k,n) 시각 임계치 기법의 해는 그 구성을 가능하게 하는 기저 행렬을 찾아내는 것이므로 훨씬 간단하다고 할 수 있다.

본 논문에서는 n개의 슬라이드 중 2개를 겹치면 비밀정보를 복원할 수 있는 $(2,n)$ 시각암호기법에 있어서 표본행렬을 이용하여 비밀분산을 가능하게 하는 방법을 소개하고자 한다. $(2,n)$ 시각암호를 위한 기저행렬의 구성기법과 복수의 비밀영상을 분산시키는 방법에 대해 고찰하기 위하여, 2장에서는 시각암호에서 Naor & Shamir의 기저행렬 구성방법을 소개하고 (n,n) 시각 임계치 기법과 상대휘도의 상한을 다루었다. 3장에서는 표본행렬을 이용하여 복수의 휘도를 허용함으로서 확장 화소의 수를 대폭적으로 줄일 수 있는 새로운 구성법을 제안하고, 상대휘도 차에 따른 그룹화에 의해 복수의 비밀정보를 분산 및 복원시킬 수 있는 새로운 응용법을 보였다. 그리고 4장에서는 이러한 제안 기법이 확장 화소의 수와 상대휘도의 관점에서 기존의 기법과 비교 분석한 결과, 성능이 우수함을 보임으로써 앞으로도 연구할 가치가 있음을 보였다.

이 논문에서는 (k,n) 시각 임계치 기법에서 k=2인 k가 작은 경우를 다루므로 학생들에게 시각암호를 구성할 수 있겠다는 자신감을 줄 수 있으며, 원소가 0과 1로만 이루어진 표본행렬은 이항계수의 분포를 따르는 규칙을 적용하여 간단하게 구성할 수 있으면서도 확장 화소의 수를 효과적으로 줄일 수 있는 장점을 가지고 있다. 또한 시뮬레이션을 통해 처음에는 알 수 없는 이미지가 실제로 겹치면 인간의 시각으로 알아볼 수 있는 경험을 통해 수학에 대한 관심과 흥미도 이끌어 낼 수 있으므로 이 논문의 내용이 수학에 대한 가치와 학습효과를 높일 수 있는 학습 자료로 활용되기를 기대해

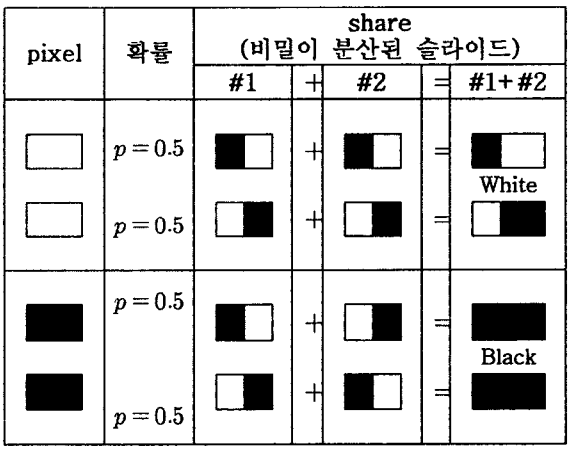
본다.

2. 시각암호에서의 기저행렬

A. Shamir(1979)는 $q \geq n+1$인 GF(q) 상의 다항식 보간법에 기초한 (k,n) 임계치 기법을 제시하여 비밀 분산법의 토대를 마련하였다. 일반 임계치 기법에서 비밀의 복원은 유한체 상의 복잡한 계산을 수반하지만, 시각 임계치 기법(Visual Threshold Scheme)에서는 인간의 시각체계를 이용하여 간단히 재구성할 수 있다. 여기서 비밀정보는 흑과 백의 화소로 구성되는 이진영상을 가정한다.

(k,n) 비밀 분산법에서는 Boolean[1] "xor"이지만, 인간의 시각체계는 Boolean "or"의 작용이 일어난다. 여기에 착안하여 Naor & Shamir(1994)는 비밀영상의 각 화소를 m개의 부 화소로 확장한 후, 휘도의 차를 이용하여 흑/백을 구별할 수 있는 시각암호를 제시하였다. <그림 1>은 $(2,2)$ 시각암호에서 흑과 백의 화소를 구성하는 예를 보이고 있다. 즉, #1 + #2의 결과가 절반이 흑인 경우는 백으로, 완전히 흑인 경우는 흑으로 인식된다.

<그림 1> (2,2)-시각 임계치 기법



일반적인 비밀 분산법의 해는 유한체 상의 복잡한 연산을 수반하지만, (k,n) 시각 임계치 기법은 화소를 분산시키는 방법을 행렬로 표시하여 구현하므로 이 기법의 해는 그 구성을 가능하게 하는 기저 행렬을 찾는 것으로 상대적으로 간단하며 정의는 다음과 같이 주어진다.

[정의 2.1] 기저행렬의 정의

$n \times m$ 크기의 이진요소를 갖는 행렬 S_0와 S_1이 $k(2 \leq k \leq n)$개 이상의 원소를 갖는 모든 부분집합 $X \subseteq \{1, \cdots, n\}$에 대하여, 성질 (i), (ii)를 만족한다면 이를 확장 화소의 수 m과 상대휘도

1) Boolean은 부울대수를 가리킨다.

γ을 갖는 (k,n)시각 임계치 기법(이후 (k,n)-VTS로 표현)에 대한 기저 행렬이라고 정의한다.

(i) 집합 $X=\{i_1, \cdots, i_k\}$에 대하여, 행렬 S_1에 있는 $i_1, \cdots, i_k$ 행들에 대한 "or" 가중치와 행렬 S_0에 있는 $i_1, \cdots, i_k$ 행들에 대한 "or" 가중치 사이의 차는 적어도 γm이다.

(ii) 집합 $X=\{i_1, \cdots, i_q\}$에 대하여, $q<k$일 때 행렬 S_0와 S_1의 행을 $i_1, \cdots, i_q$로 제한하여 얻어진 두 개의 $q\times m$ 행렬은 열 치환 동형이다.

n개 슬라이드 각각에 있는 m개의 부 화소들은 $n\times m$ 행렬 $B=[b_{ij}]$의 한 행에 의해 표현되므로, i번째 슬라이드의 j번째 부 화소가 흑일 때만 $b_{ij}=1$이 된다. 또한, k개의 슬라이드를 겹쳤을 때, 계조(gray-level)는 B의 k개 행에 대응하는 Boolean "or"의 가중치에 의해 결정된다. 즉, 두 슬라이드를 겹쳤을 때 같은 위치에서 1이나 0이 겹치면 휘도 차가 나지 않아 그림이 나타나지 않는다. 안전성을 보장하기 위하여 원 영상의 흑 화소와 백 화소 각각에 대해 k개 미만의 슬라이드를 겹쳤을 때, 그 가중치는 동일해야 한다. 기저행렬에서 조건 (i)은 휘도(contrast)를 나타내고, 조건 (ii)은 보안성(security)을 나타낸다.

Naor & Shamir는 $(2,n)$-VTS에 대한 기저 행렬을 다음과 같이 구성하였다.

[예] Naor & Shamir의 기저행렬

S_0는 각 행의 크기가 n이고, 가중치가 1인 n개의 동일한 행을 갖는 행렬이고 S_1은 단위행렬로 구성한다. 따라서 다음과 같은 기저행렬이 구성되고, 확장 화소의 수 m과 상대휘도 γ는 각각 $m=n$, $\gamma=1/m$이 된다.

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

[정리 2.2] (n, n)-VTS의 존재

$n\geq 2$인 임의의 정수 n에 대하여, $m=2^{n-1}$과 $\gamma=\dfrac{1}{2^{n-1}}$을 갖는 (n,n)-VTS가 존재한다.

S_0의 열은 짝수개의 1을 포함하는 모든 이진 n-tuples로 구성하고, S_1의 열은 홀수개의 1을 포함하는 이진 n-tuples로 구성하면 S_0와 S_1은 (n,n)-VTS의 기저행렬이 된다. 다음은 $n=3$인 경우이다.

[예] $m=4$, $\gamma=\dfrac{1}{4}$을 갖는 (3, 3)-VTS

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

Blundo, Santis and Stinson(1999)은 다음과 같이 $(2,n)$-VTS에서 휘도에 대한 상한을 구하였다.

[정리 2.3] 임의의 $(2,n)$-VTS에 대하여, $\gamma \leq \gamma^*(n)$이 성립하고, 여기서 γ^*는

$$\gamma^*(n) = \frac{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor}{n(n-1)}$$ 이다.

그들은 또한 BIBD[2](Balanced Incomplete Block Design: 균형불완비블록설계)를 이용하여 시각암호를 위한 기저행렬을 구성하였으며 최적의 상대휘도를 가지는 $(2,n)$-VTS가 Hadamard 행렬에서 얻어지는 BIBD로부터 구성될 수 있음을 보였다.

다음은 $n=7$일 때, 최적의 상대 휘도를 가지는 $(2,7)$-VTS의 예이다.

[예] $m=7$과 $\gamma=2/7$인 $(2,7)$-VTS의 기저행렬

$$S_0 = \begin{pmatrix} 1110000 \\ 1110000 \\ 1110000 \\ 1110000 \\ 1110000 \\ 1110000 \\ 1110000 \end{pmatrix}, \quad S_1 = \begin{pmatrix} 1000101 \\ 1100010 \\ 0110001 \\ 1011000 \\ 0101100 \\ 0010110 \\ 0001011 \end{pmatrix}$$

3. ${}_nC_2$를 이용한 시각암호의 구성법

Naor & Shamir의 방법은 그 구성이 간결하지만, n이 커지면 상대휘도 γ가 너무 작아져 실용적이지 못하다. 또, BIBD를 이용하는 방법은 확장 화소의 수와 상대휘도 값이 최적이지만, BIBD를 찾는 것이 매우 어려운 문제점이 있고 확장 화소의 수는 적어도 $m \geq n$이다. 본 장에서는 휘도가 일정한 기존의 방법과 달리 복수의 휘도를 허용하고 표본행렬을 생성하여 확장 화소의 수가 $m \leq n$으로 개선되는 새로운 구성법을 제안한다.

3.1 Cardinality[3]가 2인 기저행렬의 구성

Naor & Shamir는 (n,n)-VTS의 기저행렬을 구성하기 위하여 S_0는 모든 열에서 짝수 cardinality를, S_1은 홀수 cardinality를 갖는 행렬로 구성하였다. 여기서는 S_1이 짝수 cardinality 2인

2) 여기서 BIBD의 정의와 구하는 방법은 생략한다.

3) cardinality는 (k,n)에서 k의 수를 의미한다

경우로 제한한다. 즉, S_0는 각 행에서 1의 개수인 가중치가 ${}_{n-1}C_1$이면서 전부 동일한 행을 가지는 행렬로 구성하고, S_1은 각 행에서 가중치는 같으나, 각 열의 가중치가 2인 모든 경우를 나열한 행렬로 잡는다. 이렇게 구성된 S_0와 S_1는 각 행렬에서 임의의 두 행을 겹치면 가중치의 차는 항상 $n-2$이므로 상대휘도는 $\frac{n-2}{{}_nC_2}$가 되어 흑과 백의 구별이 가능하다. 다음은 $n=5$인 경우의 기저 행렬이다.

[예] $m=10$, $\gamma=3/10$인 (2,5)-VTS

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

3.2 표본행렬에 의한 구성법

3.1에서 제시한 방법은 Naor & Shamir(1994)의 방법과 비교하여 휘도는 좋지만, n이 커짐에 따라 확장 화소의 수가 너무 증가되어 구현이 어렵게 된다. 따라서 S_1을 전치하여 얻어지는 표본 행렬[4]을 정의하여 이를 이용한 기저행렬의 구성법을 다음과 같이 제안한다.

[표본행렬에 의한 구성법- 제안방법 I]

표본 행렬에 의한 $(2,n)$-VTS의 기저 행렬을 다음과 같이 구성한다.

(i) 주어진 n에 대하여 확장 화소의 값 m을 $\min\{m \mid n \le {}_mC_2\}$인 정수로 한다.

(ii) m값에 따라 결정되는 표본행렬 S을 다음과 같이 구한다.

① 각 행의 가중치가 $m-1$이고, 열의 가중치는 2인 $m \times {}_mC_2$ 행렬 M을 구성한다.

② M을 전치하여 얻어진 ${}_mC_2 \times m$ 행렬을 표본행렬 S로 둔다.

(iii) S_0는 행의 가중치가 2인 동일한 행으로 구성된 $n \times m$ 행렬로 한다. S_1은 표본행렬 S에서 필요한 n개의 행을 임의로 선택한 $n \times m$ 행렬로 한다.

여기서 표본행렬의 행의 개수를 ${}_mC_2$로 택한 이유는 share(슬라이드)를 두 장 겹칠 때 비밀을 복원할 수 있는 방법의 가지 수이므로 여러 장의 슬라이드를 구성하기 위함이다.

[예] $n=16$에 대한 표본행렬을 이용한 $(2,n)$-VTS의 기저행렬 S_0와 S_1의 한 예

---

4) 표본행렬을 도입하는 이유는 일반적인 방법으로 수를 순서대로 가로 배열하여 행렬을 구성한 후 그 행렬을 전치시키거나 90도 회전시킨 행렬을 이용하여 share를 만들기 위한 것이다.

(i) $16 \leq {}_mC_2$을 만족하는 최소의 수는 $m=7$이다.

(ii) ${}_7C_2 = 21$이므로 표본행렬 S는 21×7 행렬이고 기저행렬 S_0와 S_1은 다음과 같이 구할 수 있다.

S_1은 S에서 두 행을 뽑는 가지 수만큼 있으므로 아래의 예를 포함하여 ${}_{21}C_{16}$가지[5]가 생성된다. 이때 S_0와 S_1에서 두 행의 겹침에 의한 가중치의 차는 1 또는 2이다.

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

3.3 확장 표본행렬에 의한 구성법

3.2의 표본행렬 구성에서 확장 화소의 수 m을 $n \leq {}_mC_2$을 만족하는 최소의 정수로 제한하였으나, $n \leq {}_mC_{\lfloor m/2 \rfloor}$[6]을 만족하는 최소 정수로 하면 표본행렬의 행의 수가 최대로 되어 상대적으로 확장 화소의 수를 더욱 줄이는 효과를 얻을 수 있다. 기본적으로 두 슬라이드를 겹칠 때 반은 흑으로 반은 백으로 나타나야하므로 1의 수가 전체의 반을 넘지 않도록 하기 위해서 $\lfloor m/2 \rfloor$ 으로 제한하였다.

[확장 표본행렬에 의한 구성법-제안방법 II]

확장된 표본 행렬에 의한 $(2,n)$-VTS의 기저 행렬을 다음과 같이 구성한다.

(i) m은 $n \leq {}_mC_{\lfloor m/2 \rfloor}$을 만족하는 최소의 정수이다.

(ii) m값에 따라 결정되는 확장된 표본행렬 S을 다음과 같이 구한다.

---

5) 서로 다른 ${}_{21}C_{16}$종류의 행렬들은 슬라이드를 구성할 때 부 화소의 위치만 달라지며 비밀 복원이 가능하고 휘도도 같게 된다.

6) ${}_mC_{\lfloor m/2 \rfloor}$에서 $\lfloor\ \rfloor$ 는 함수기호로 $\lfloor x \rfloor$ 는 x를 넘지 않는 최대정수를 의미한다.

① 각 행의 가중치가 ${}_{m-1}C_{\lfloor m/2 \rfloor -1}$이고, 각 열의 가중치가 $\lfloor m/2 \rfloor$ 인 $m \times {}_{m}C_{\lfloor m/2 \rfloor}$ 행렬 M을 구성한다.

② M을 전치하여 얻어진 ${}_{m}C_{\lfloor m/2 \rfloor} \times m$ 행렬을 확장된 표본행렬 S로 둔다. 즉, S는 각 행의 가중치가 $\lfloor m/2 \rfloor$ 인 모든 경우를 나열한 것과 같다.

(iii) S_0와 S_1은 3.2의 표본행렬에 의한 구성법 (iii)과 동일한 방법으로 구성한다.

[예] $n=16$에 대한 확장된 표본행렬 S을 이용한 $(2,n)$-VTS의 기저행렬 S_0과 S_1

(i) $16 \leq {}_{m}C_{\lfloor m/2 \rfloor}$ 을 만족하는 최소의 정수는 m=6이다.

(ii) ${}_{6}C_{3}=20$이므로 확장된 표본행렬 S는 20×6 행렬이다.

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

여기서 서로 다른 행렬 S_1은 ${}_{20}C_{16}$가지가 생성된다. 이 때, S_0와 S_1에서 두 행의 겹침에 의한 가중치의 차는 1, 2 또는 3이 된다. 단계 (ii)에서 각 행의 가중치를 2 대신 $\lfloor m/2 \rfloor$ 으로 하면 표본행렬 S의 행의 수 n이 최대가 되므로 확장 화소의 수를 줄이는 효과가 있다. 한편, 비밀 영상을 복원할 때 가중치가 다른 짝들이 생기게 되며, 그 범위는 1에서 $\lfloor m/2 \rfloor$ 까지가 된다. 결과적으로 제안 방법 II의 확장 화소의 수 m은 $n \leq {}_{m}C_{\lfloor m/2 \rfloor}$ 을 만족하는 최소 정수가 되고, 상대휘도 γ의 범위는 $\frac{1}{m} \leq \gamma \leq \frac{\lfloor m/2 \rfloor}{m}$ 가 된다.

3.4 그룹화에 의한 복수의 시각 비밀 분산법

3.3에서 복원영상의 상대휘도가 두 가지 이상의 다른 값을 갖게 되므로 그룹화에 의해 복수의 비밀영상을 분산시킬 수 있다. 즉, 표본행렬 S의 임의의 한 행을 기준으로 겹쳤을 때의 휘도가 같은 행을 묶어서 그룹화하고, 각 그룹에 대하여 다른 비밀영상을 할당함으로써 복수의 비밀을 분산시킬 수 있다.

[표본행렬의 그룹화]

주어진 n에 대하여 확장 화소의 수 m은 $n \leq {}_mC_{\lfloor m/2 \rfloor}$을 만족하는 최소 정수로 한다. m값에 따라 구해진 표본행렬 S에 대하여 편의상 첫째 행을 base로 하면, base와 겹쳐서 나타날 수 있는 가중치의 차에 따라 $\lfloor m/2 \rfloor$ 개의 그룹으로 나눌 수 있다. 이 때 각 그룹의 크기는 다음과 같이 된다.

(i) 가중치의 차가 1인 그룹의 크기: ${}_{m-\lfloor m/2 \rfloor}C_1 \times {}_{\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor - 1}$

(ii) 가중치의 차가 2인 그룹의 크기: ${}_{m-\lfloor m/2 \rfloor}C_2 \times {}_{\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor - 2}$

(iii) 가중치의 차가 3인 그룹의 크기: ${}_{m-\lfloor m/2 \rfloor}C_3 \times {}_{\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor - 3}$

.....

(iv) 가중치의 차가 $\lfloor m/2 \rfloor$ 인 그룹의 크기: ${}_{m-\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor} \times {}_{\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor - \lfloor m/2 \rfloor}$.

여기서 크기가 가장 작은 그룹의 가중치의 차는 항상 $\lfloor m/2 \rfloor$ 이 되고, 그 크기는 m이 짝수인 경우는 한 개이고 m이 홀수인 경우는 $m-\lfloor m/2 \rfloor = \frac{m+1}{2}$개가 된다. 위의 각 그룹은 base행을 기준으로 겹치면 가중치의 차가 1씩 증가하여 $\lfloor m/2 \rfloor$ 까지 다르게 되므로 복수의 비밀영상을 분산시키는 시각 임계치 기법을 구현할 수 있다. 또한, 각 그룹의 행에 대해서도 가중치의 차가 발생하므로 슬라이드를 겹칠수록 휘도가 좋아지는 특징을 갖는다.

[복수의 비밀영상을 분산시키기 위한 기저행렬 구성]

그룹의 수를 g라 하고, 크기가 가장 작은 그룹의 원소를 p라 하자.

(i) 확장 화소의 수 m:

$$\min\{m \mid g \leq \lfloor m/2 \rfloor,\ n < {}_mC_{\lfloor m/2 \rfloor},$$
$$p \leq {}_{m-\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor} \times {}_{\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor - \lfloor m/2 \rfloor}\}$$

(ii) 주어진 m에 대한 표본행렬 S을 구한다.

(iii) 그룹의 원소 수와 표본행렬 S을 각각 대응시키고, 복수의 비밀영상을 분산시키기 위한 기저행렬을 구성한다.

[예] $m=9$일 때, 표본행렬이 다음과 같다고 하자

$$S = \begin{array}{c} 1 \\ 2 \\ 3 \\ \\ \\ \cdot \\ \cdot \\ \cdot \\ \\ \cdot \\ \cdot \\ \cdot \\ \\ \\ 124 \\ 125 \\ 126 \end{array} \begin{pmatrix} 1&1&1&1&0&0&0&0&0 \\ 1&1&1&0&1&0&0&0&0 \\ 1&1&1&0&0&1&0&0&0 \\ & & & \cdots & & & & & \\ & & & \cdots & & & & & \\ 1&1&0&0&1&1&0&0&0 \\ 1&1&0&0&1&0&1&0&0 \\ 1&1&0&0&1&0&0&1&0 \\ & & & \cdots & & & & & \\ & & & \cdots & & & & & \\ 1&0&0&0&1&1&1&0&0 \\ 1&0&0&0&1&1&0&1&0 \\ 1&0&0&0&1&1&0&0&1 \\ & & & \cdots & & & & & \\ & & & \cdots & & & & & \\ 0&0&0&0&1&0&1&1&1 \\ 0&0&0&0&0&1&1&1&1 \end{pmatrix}$$

첫 번째 행을 base로 하여 임의의 행과 겹치면 가중치의 차가 1, 2, 3, 4인 네 그룹이 생기게 된다. 가중치의 차가 1인 행의 수는 20개, 2인 행의 수는 60개, 3인 행의 수는 40개, 4인 행의 수는 5개이므로 네 가지의 비밀 영상을 분산시킬 수 있다. 즉, 전체 참가자 집합 중 A, B, C, D의 네 그룹을 나눌 때, 가중치의 차가 1인 경우 A, 2인 경우 B, 3인 경우 C, 4인 경우 D의 순서로 할당하면 복수의 비밀을 갖는 시각 비밀분산이 가능하다.

예를 들어, 그룹 A, B, C, D의 회원이 각각 3명, 5명, 4명, 5명일 경우, '수', '학', '교', '육'이라는 비밀정보를 분산시키기 위한 경우에 대해 생각해 보자. 표본행렬 S을 이용하여 기저행렬 S_0, S_1을 아래와 같이 구성한다.

(i) 각 그룹에 대하여 백의 부 화소의 구성은 S_0 행렬에서 선택하고,

(ii) A 그룹에 대한 흑의 부 화소의 구성은 S_1 행렬의 A 그룹의 임의의 행을,

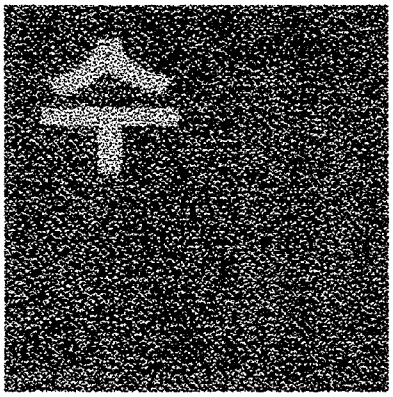
(iii) B 그룹에 대한 흑의 부 화소의 구성은 S_1 행렬의 B 그룹의 임의의 행을,

(iv) C 그룹에 대한 흑의 부 화소의 구성은 S_1 행렬의 C 그룹의 임의의 행을,

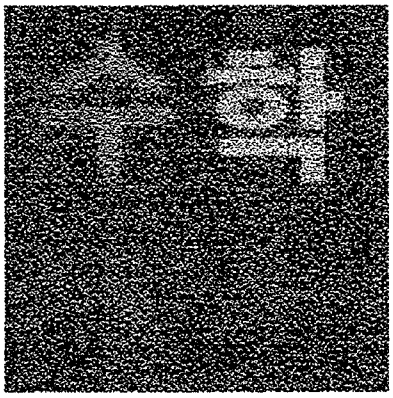
(v) D 그룹에 대한 흑의 부 화소의 구성은 S_1 행렬의 D 그룹의 임의의 행을 각각 할당한다.

$$S_0=\begin{pmatrix}
\text{---------}\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
\text{---------}\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
\text{---------}\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
\text{---------}\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
\text{---------}\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\\
\text{---------}
\end{pmatrix},\qquad
S_1=\begin{pmatrix}
\text{---------} & \text{--}\\
1\ 1\ 1\ 1\ 00\ 0\ 0\ 0 & \text{⌂}\\
\text{---------} & \text{--}\\
1\ 1\ 1\ 0\ 10\ 0\ 0\ 0 & \\
1\ 0\ 1\ 1\ 00\ 0\ 1\ 0 & \leftarrow A\\
1\ 1\ 0\ 1\ 01\ 0\ 0\ 0 & \\
\text{---------} & \text{--}\\
1\ 1\ 0\ 0\ 00\ 0\ 1\ 1 & \\
1\ 0\ 1\ 0\ 10\ 0\ 0\ 1 & \\
1\ 1\ 0\ 0\ 01\ 1\ 0\ 0 & \leftarrow B\\
0\ 0\ 1\ 1\ 10\ 0\ 1\ 0 & \\
0\ 1\ 0\ 1\ 01\ 0\ 1\ 0 & \\
\text{---------} & \text{--}\\
1\ 0\ 0\ 0\ 11\ 1\ 0\ 0 & \\
0\ 1\ 0\ 0\ 01\ 1\ 0\ 1 & \\
0\ 0\ 0\ 1\ 11\ 1\ 0\ 0 & \leftarrow C\\
0\ 0\ 1\ 0\ 00\ 1\ 1\ 1 & \\
\text{---------} & \text{--}\\
0\ 0\ 0\ 0\ 11\ 1\ 1\ 0 & \\
0\ 0\ 0\ 0\ 11\ 1\ 0\ 1 & \\
0\ 0\ 0\ 0\ 11\ 0\ 1\ 1 & \leftarrow D\\
0\ 0\ 0\ 0\ 10\ 1\ 1\ 1 & \\
0\ 0\ 0\ 0\ 01\ 1\ 1\ 1 & \\
\text{---------} & \text{--}
\end{pmatrix}$$

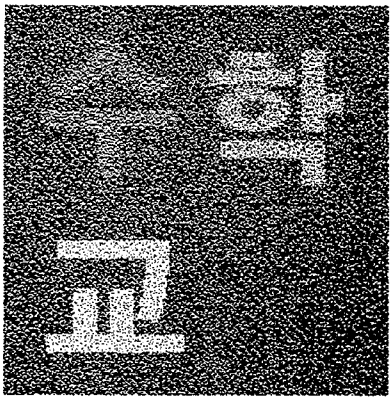
그 결과, 복원 시 그룹에 대한 휘도 차에 의해서 같은 그룹 내에서 선택된 임의의 두 슬라이드를 겹치면 각각 '**수**', '**학**', '**교**', '**옥**'이라는 정보가 나타나고, base와의 겹침도 역시 '**수**', '**학**', '**교**', '**옥**'이 나타난다. 시뮬레이션 결과를 보면 <그림 2>는 그룹 A의 두 슬라이드를 겹친 것이고, <그림 3, 4, 5>은 각각 그룹 A, B, C, D에서 한 장씩 선택한 슬라이드를 차례로 겹쳐감에 따라 복원되는 결과를 나타내고 있다.



<그림 2> A 그룹에서 두 슬라이드의 겹침



<그림 3> A, B 그룹에서 한 장씩을 겹침

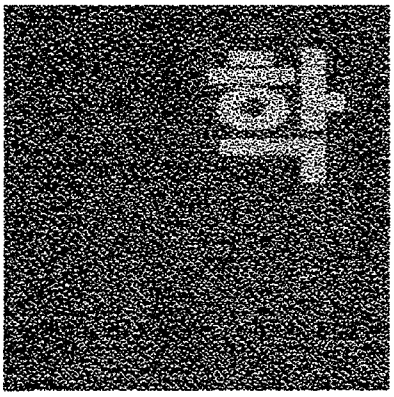


<그림 4> A, B, C, D 그룹에서 한 장씩을 겹침

<그림 5> A, B, C, D 그룹에서 한 장씩을 겹침

아래의 <그림 6>과 <그림 7>는 한 그룹 내에서 슬라이드를 겹쳐감에 따라 휘도가 좋아짐을 보여주고 있다. 이와 같이, 슬라이드를 여러 장 겹쳐감에 따라 휘도가 더욱 좋아지게 된다.

<그림 6> 그룹 B에서 두 장을 겹침



<그림 7> 그룹 B에서 네 장을 겹침

4. 성능비교 및 분석

지금까지 언급된 세 가지 구성법에 대하여 확장 화소의 수 m과 상대휘도 γ 그리고 행렬 구성의 복잡성 관점에서 성능을 비교 분석한다. 일반적으로 상대휘도 값이 1/36 이상이면 흑과 백의 화소를 구별할 수 있는 것으로 알려져 있으므로 제안 방법을 기준으로 n 값이 $3 \leq n \leq 630$의 범위에 대하여 m과 γ을 비교한다.

1. Naor & Shamir 방법 (Na & Sh) : $m=n,\ \gamma=1/m.$

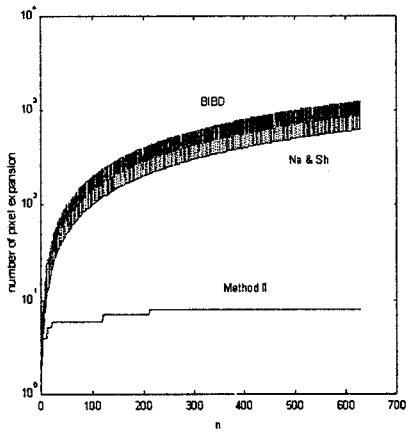
2. BIBD방법(BIBD) : $m=\begin{cases}2n-2, & \text{if } n=2t\\ n, & \text{if } n=4t+3,\\ 2n, & \text{if } n=4t+1\end{cases}$ $\gamma=\dfrac{\lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil}{n(n-1)}$

3. 제안법 I, II (Proposed I, II) : $m=\min\{m|n \leqq {}_mC_{\lfloor m/2 \rfloor}\},\ 1/m \leq \gamma \leq \dfrac{\lfloor m/2 \rfloor}{m}$

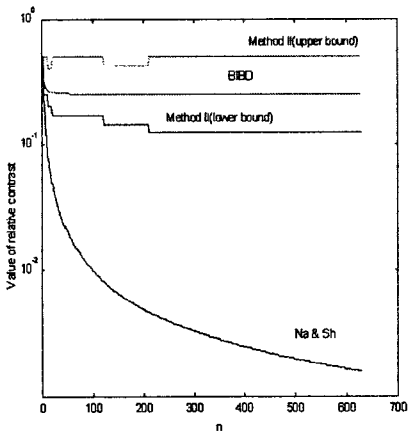
부록에 제시한 <표 1>은 위의 네 가지 기법을 사용했을 때, n에 따른 확장 화소의 수 m과 상대휘도 γ을 비교한 것이다. 확장 화소의 수 m은 제안방법 I, II(Proposed I, II), Naor & Shamir방법, BIBD 방법의 순서로 커지고 상대휘도 값 γ는 BIBD방법, 제안방법, Naor & Shamir방법의 순서로 작아진다.

<그림 8>와 <그림 9>에서는 n이 커짐에 따른 확장 화소의 수 m과 상대휘도 γ의 변화를 알 수 있다.

결과적으로 제안방법은 확장 화소의 수 관점에서 가장 좋고, 상대휘도의 관점에서는 BIBD방법보다 다소 떨어지지만, Naor & Shamir방법보다는 많이 개선됨을 알 수 있다. 한편, 행렬 구성의 관점에서 BIBD의 발견이 매우 어려우므로 제안방법이 더욱 실용적이라고 할 수 있다. 또한, 제안방법은 슬라이드를 겹쳐감에 따라 휘도가 더욱 좋아지는 장점을 가지고 있다.



<그림 8> n의 값에 따른 확장 화소의 수



<그림 9> n의 값에 따른 상대휘도

5. 결 론

(k,n) 비밀 분산법에 기반을 둔 시각암호에서 $(2,n)$-VTS에 대한 기저행렬의 구성에 대하여 여러 가지 기법이 연구되어 왔다. Naor & Shamir의 기법은 간결하지만 확장 화소의 수가 너무 크므로 상대휘도가 상대적으로 작아져 실용적이지 못하다. 그리고 BIBD 방법은 Hadamard 행렬을 이용하면

주어진 n에 대해 확장 화소의 수와 상대휘도 값이 최적이도록 할 수 있지만 BIBD의 구성이 매우 어렵다는 문제점이 있다.

본 연구에서는 이진요소로 이루어지고 이항계수의 분포를 이용하여 간단히 구성할 수 있는 표본행렬을 도입하여 확장 화소의 수가 $m \leq n$으로 개선되면서도 확장 화소의 측면에서 최상이고 n의 값을 상당히 크게 하여도 휘도가 많이 개선되는 실용적인 시각암호 기법을 선보였다. 표본행렬 구성에서 확장 화소의 수 m을 $n \leq {}_mC_{\lfloor m/2 \rfloor}$을 만족하는 최소 정수로 두면 표본행렬의 행의 수가 최대로 되어 상대적으로 확장 화소의 수를 더욱 줄이는 효과를 얻을 수 있음을 검증하였고 복원 시의 휘도 차에 따라 복수의 비밀영상을 분산시킬 수 있으면서, 슬라이드를 겹칠수록 휘도가 좋아지는 시각 비밀 분산법을 구현하였다.

특히, 시각 비밀 분산법은 표본행렬 S의 임의의 한 행을 기준으로 겹쳤을 때의 휘도가 같은 행끼리 그룹화하고 각 그룹에 대하여 다른 비밀영상을 할당함으로써 복수의 비밀을 분산시킬 수 있으므로 학생들은 다양한 조합적 사고로 행렬의 구성을 달리함으로써 어떤 다양한 결과가 나타나는지를 확인할 수 있다. 그리고 이 기법으로 구현한 슬라이드를 수업시간에 학생들에게 배부하여 친구들의 슬라이드와 겹치게 함으로써 처음에는 알 수 없었던 자신의 슬라이드의 이미지가 시각적으로 확인할 수 있는 이미지로 나타남을 직접 보여줄 수 있다. 자신의 슬라이드에 어떠한 비밀이 숨어있는지를 확인해 보는 과정에서 수학 수업을 더욱 재미있고 현실감 있게 이끌어 갈 수 있을 것이고 암호기법에 대한 호기심과 수학에 대한 학습동기도 유발시킬 수도 있을 것이다. 특히, 작은 k와 n값에 대한 구현은 학생들에게 자신도 시각암호를 구성할 수 있겠다는 자신감과 성취동기를 부여할 수 있으면서도 수학적 연산으로는 복원이 불가능하므로 안전성의 측면에서 암호로서의 가치도 높다.

이와 같이, 시각암호는 고등학교 수준의 수학적 지식이 있으면 깊이 있는 연구에 쉽게 접근할 수 있는 점이 있으므로, 수학적 재능이 뛰어난 고등학생들에게 대학수준의 연구에 접근할 수 있는 기회를 제공하기 위해 실시되는 R&E(Research & Education) 프로그램의 한 주제로 적당하다고 판단된다. 또한, 학생들이 앞으로 살아가야 할 정보화 사회에서 정보보안에 대한 의식을 고취시키고 암호에 대한 흥미를 높이며, 진로선택에 있어서도 시야의 폭을 넓혀주는 교육적 제재의 역할을 해낼 수 있을 것이다. 현재 암호학은 응용수학의 한 분야로 자리 잡아가고 있으므로 수학을 좋아하고 전공하고 싶어 하는 학생들에게 수학에 대한 가치부여와 비전 제시에 적절한 소재이다.

참 고 문 헌

G. Ateniese; C. Blundo; A. De Santis & D. R. Stinson. (1996). "Visual Cryptography for General Access Structures", *Information and Compuation* **129**, pp.86-106.

C. Blundo; A. De Santis & R. D. R. Stinson. (1999). "On the Contrast in Visual Cryptography Schemes", *Journal of Cryptology* **12**, pp.261-289.

C. K. Choi; J. H. Park & R. Kohno. (1997). "Contrast Analysis According to Hierachical Access Structure on Visual Cryptography Scheme and Its Application into Authentication", *Proceeding of SITA*, **20(1)**, pp.217-220

S. Droste. (1996). "New Results on Visual Cryptography", *Advanced in Cryptology-CRYPTO'96*, pp.401-415.

T. Katoh & H. Imai. (1996). "An Extended Construction Method of Visual Secret Sharing Scheme," *IEICE Trans.* **J79-A(8)**, pp.1344-1351.

H. Koga & H. Yamamoto. (1998). "Proposal of a Lattice-Based Visual Secret Sharing Scheme for Color and Gray-Scale Images," *IEICE Trans. on Fundamentals* **E81-A(6)**, pp.1262-1269.

M. Naor & A. Shamir. (1994). "Visual Cryptography", *Advances in Cryptology- EUROCRYPT'94*, Perugia, Italy, pp.1-12.

A. Shamir. (1979) "How to Share a Secret", *Commun. of the ACM* **22(1)**, pp. 612-613.

D. R. Stinson (1996). *"Combinatorial Designs with Selected Applications Lecture Notes,"* Department of Computer Science University of Manitoba.

Visual Cryptography Using the Number of ${}_nC_2$

Moon-Soo Kim
Korea Science Academy, 899 Danggam 3-dong, Busanjin-Gu, Busan, Korea, 614-822
E-mail: kms5812@hanmail.net

Meekwang Kang
Dongeui University, 995 Eomgwangno Busanjin-Gu, Busan, Korea, 614-714
E-mail: mee@deu.ac.kr

The visual cryptography scheme is a simple method which can be decoded directly the secret information in human visual system without performing any cryptographic computations. For some secret of image type, we scatter them to random n images and if any threshold (or more) of them are stacked together then original image is visible.

In this paper we consider $(2,n)$ visual cryptography scheme and show a construction method of the sample matrix using the rule of binomial coefficients ${}_nC_2$. This scheme can contribute interesting and effectiveness to the study of mathematics.

* ZDM Classification : M95
* 2000 Mathematics Subject Classification : 97D99
* Key Words : visual cryptography, visual threshold scheme, BIBD, sample matrix, multiple secret sharing

<부록 1>

<표 1> n에 따른 확장 화소의 수 m과 상대휘도 γ

n	Na & Sh		Proposed I		Proposed II		BIBD	
	m	γ	m	γ	m	γ	m	γ
2	2	0.5000	2	0.5000	2	0.5	2	0.5000
3	3	0.3333	3	0.3333	3	0.3333	3	0.3333
4	4	0.2500	4	0.2500-0.5000	4	0.2500-0.5000	6	0.3333
5	5	0.2000	4	0.2500-0.5000	4	0.2500-0.5000	10	0.3000
10	10	0.1000	5	0.2000-0.4000	5	0.2000-0.4000	18	0.2777
15	15	0.0666	6	0.1666-0.3333	6	0.1666-0.5000	15	0.2666
16	16	0.0625	7	0.1428-0.2857	6	0.1666-0.5000	30	0.2666
20	20	0.0500	7	0.1428-0.2857	6	0.1666-0.5000	38	0.2631
22	22	0.0454	8	0.1250-0.2500	7	0.1428-0.4285	42	0.2619
25	25	0.0400	8	0.1250-0.2500	7	0.1428-0.4285	50	0.2600
30	30	0.0330	9	0.1111-0.2222	7	0.1428-0.4285	58	0.2586
35	35	0.0285	9	0.1111-0.2222	7	0.1428-0.4285	35	0.2571
40	40	0.0250	10	0.1000-0.2000	8	0.1250-0.5000	78	0.2564
45	45	0.0222	10	0.1000-0.2000	8	0.1250-0.5000	90	0.2555
50	50	0.0200	11	0.0909-0.1818	8	0.1250-0.5000	98	0.2551
60	60	0.0166	12	0.0833-0.1666	8	0.1250-0.5000	118	0.2542
70	70	0.0142	13	0.0769-0.1538	8	0.1250-0.5000	138	0.2536
80	80	0.0125	14	0.0714-0.1428	9	0.1111-0.4444	158	0.2531
90	90	0.0111	14	0.0714-0.1428	9	0.1111-0.4444	178	0.2528
100	100	0.0100	15	0.0666-0.1333	9	0.1111-0.4444	198	0.2525
200	200	0.0050	21	0.0476-0.0952	10	0.1000-0.5000	398	0.2512
300	300	0.0033	25	0.0400-0.0800	11	0.0909-0.4545	598	0.2508
400	400	0.0025	29	0.0344-0.0689	11	0.0909-0.4545	798	0.2506
500	500	0.0020	33	0.0303-0.0606	12	0.0833-0.5000	998	0.2505
600	600	0.0016	36	0.0277-0.0555	12	0.0833-0.5000	1198	0.2504
630	630	0.0015	36	0.0277-0.0555	12	0.0833-0.5000	1258	0.2503