通信情報保護學會論文誌
第 10 券 第 3 號, 2000. 9

복수의 비밀 분산을 위한 (2, n) 시각암호의 새로운 구성*

김 문 수**, 박 지 환***

New Construction of (2, n) Visual Cryptography for Multiple Secret Sharing

Moon-Soo Kim**, Ji-Hwan Park***

요 약

시각암호는 복잡한 암호학적 연산 없이 인간의 시각에 의해 비밀정보를 직접 복원할 수 있는 간단한 방식이다. 이 방식은 영상 형태의 비밀정보를 n개의 랜덤한 영상(슬라이드)으로 분산시킨 후, 일정 문턱 치 이상의 슬라이드를 겹치면 원래의 비밀정보를 복원할 수 있는 비밀 분산법의 일종이다. 본 논문에서는 n개의 슬라이드 중 2개 이상을 겹치면 비밀정보를 복원할 수 있는 (2, n) 시각암호에 있어서 표본행렬을 이용하여 확장 화소의 수를 줄일 수 있는 새로운 구성법을 제안한다. 제안기법은 상대 휘도 차에 따른 각 그룹에 복수의 비밀정보를 분산시킬 수 있는 특징을 갖는다.

ABSTRACT

Visual cryptography scheme is a simple method in which can be directly decoded the secret information in human visual system without performing any cryptographic computations. This scheme is a kind of secret sharing scheme in which if a secret of image type is scattered to n random images(slides) and any threshold (or more) of them are stacked together, the original image will become visible. In this paper, we consider (2, n) visual cryptography scheme and propose a new construction method in which the number of expanded pixels can be reduced by using the sample matrix. The proposed scheme can, futhermore, distribute the multiple secret image to each group according to the difference of relative contrast.

keyword : *Visual cryptography, (k,n) threshold scheme, BIBD, Sample matrix, Multiple secret sharing*

Ⅰ. 서 론

A. Shamir에 의해 (k, n) 비밀 분산법[1]이 제안된 이후, 비밀정보로서 영상의 형태를 취하는 시각 암호가 M. Naor & A. Shamir에 의해 제안되었다.[2] 시각암호에 의해 분산되는 비밀영상은 흑과 백의 화소(pixel)로 구성되어 슬라이드와 같이 물리적 중첩이 가능한 곳에 인쇄되는 경우를 가정한다. (k, n) 비밀 분산법과 같이 그룹 내의 n명에게 배포된 슬라이드 중 임의의 k명 이상의 슬라이드를 겹치면 비밀정보를 복원할 수 있지만, k명 미만의 슬라이드를 겹치는 경우에는 비밀정보를 복원할 수 없기 때문에 안전성이 보장된다.

M. Naor & A. Shamir에 의해 한 개의 비밀

* 본 연구는 부경대학교 1998년도 기성회 연구비 지원에 의해 수행되었음.
** 부경대학교 전자계산학과
*** 부경대학교 전자컴퓨터정보통신공학부 교수

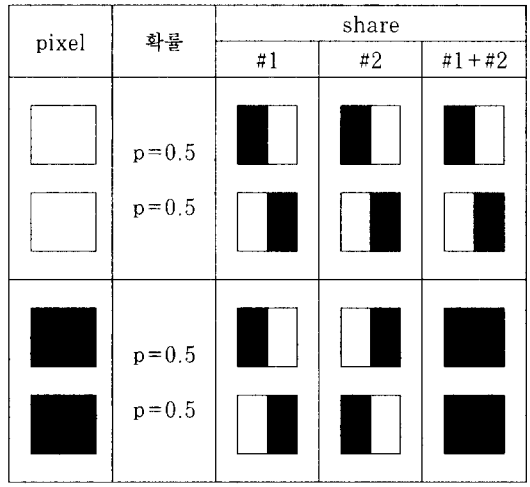
영상을 복원할 수 있는 시각암호가 고안된 후 많은 연구가 이루어지고 있다. T. Katoh & H. Imai는 겹친 슬라이드의 수에 따라 서로 다른 비밀영상을 복원할 수 있는 시각암호를 제안하였으며,[3] 휘도를 개선하기 위한 S. Droste의 연구[4]를 비롯하여 Ateniese 등은 일반적 접근구조를 갖는 경우로 확대하였고,[5] Koga와 Yamamoto는 칼라영상과 농담영상에 적용할 수 있는 Lattice-based Visual Secret Sharing Scheme을 제안하였다.[6] 또한, Choi 등은 계층적 접근 구조를 이용하여 비밀영상을 복원하는 방법을 제시하였다.[7]

본 논문에서는 (k, n)비밀 분산의 k가 2인 경우에 대하여 시각암호를 위한 기저행렬의 구성기법과 복수의 비밀영상을 분산시키는 방법에 대하여 고찰한다. 2장에서 Naor & Shamir 구성법과 BIBD를 이용한 구성법을 확장 화소의 수와 상대휘도의 관점에서 고찰한다. 3장에서 표본행렬을 이용하여 복수의 휘도를 허용함으로서 확장 화소의 수를 대폭적으로 줄일 수 있는 새로운 구성법을 제안한다. 또한, 상대휘도 차에 따른 그룹화에 의해 복수의 비밀정보를 분산 및 복원시킬 수 있는 새로운 응용을 보인다. 4장에서는 확장 화소의 수와 상대휘도의 관점에서 각 기법의 성능을 비교 분석하여 제안기법이 유용함을 보인다.

II. 시각암호

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

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



[그림 1] (2, 2)-VTS

일반 비밀 분산법의 해는 유한체 상의 복잡한 연산을 수반하지만, (k, n)-VTS의 해는 그 구성을 가능하게 하는 기저 행렬을 찾는 것이다.

[정의 2.1] 기저행렬의 정의

S_0와 S_1을 $n \times m$ 크기의 이진요소를 갖는 행렬이라고 하자. 이 때, S_0와 S_1이 k ($2 \leq k \leq n$)개 이상의 원소를 갖는 모든 부분집합 $X \subseteq \{1, \cdots, n\}$에 대하여, 다음의 성질을 만족한다면 확장 화소의 수 m과 상대휘도 γ를 갖는 (k, n)-VTS에 대한 기저 행렬로 정의된다.

1. 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.
2. 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 치환을 하면 동일해 진다.

n개 슬라이드 각각에 있는 m개의 부 화소들은 $n \times m$ 행렬 $B=[b_{ij}]$의 한 행에 의해 표현되며, i번째 슬라이드의 j번째 부 화소가 흑일 때만 $b_{ij}=1$ 이다. k개의 슬라이드를 겹쳤을 때, 계조(gray-evel)는 B의 k개 행에 대응하는 Boolean "or"의 가중치에 의해 결정된다. 보안성(security)을 보장하기 위하여 원영상의 흑 화소를 위해 k개 미만의 슬라이드를 겹칠

때와 백 화소를 위해 k개 미만의 슬라이드를 겹칠 때의 가중치가 동일해야 한다. 위의 조건1은 contrast를 나타내고, 조건2는 security를 나타낸다.

2.1 Naor & Shamir 시각암호

Naor & Shamir는 $(2, n)$-VTS에 대한 기저행렬을 다음과 같이 구성하였다.[2]

(1) S_0의 구성:
각 행의 크기가 n이고, 가중치가 1인 n개의 동일한 행을 갖는 행렬이다.
(2) S_1의 구성:
$n \times n$의 단위 행렬이다.

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 정수에 대하여, $m = 2^{n-1}$과 $\gamma = 1/2^{n-1}$을 갖는 (n, n)-VTS가 존재한다. 즉, S_0의 열은 짝수개의 1을 포함하는 모든 이진 n-tuples로 구성되어 있고, S_1의 열은 홀수개의 1을 포함하는 모든 이진 n-tuples로 구성된다.

[예 1] $m=4$, $\gamma=1/4$를 갖는 (3,3)-VTS

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

2.2 BIBD를 이용한 시각암호

C. Blundo, A. D. Santis, D. R. Stinson은 BIBD(Balanced Incomplete Block Design)를 이용하여 시각암호를 위한 기저행렬을 구성할 수 있음을 보였다.[8]

2.2.1 BIBD의 정의와 성질

[정의 2.3] n, k, λ는 $n > k \geq 2$를 만족하는 양의 정수라 하자. (n, k, λ)-BIBD는 다음의 성질을 만족하는 (X, A)의 짝으로 정의된다.

1. X는 n개의 점을 원소로 하는 집합이다.
2. A는 블록이라 불리는 X의 부분집합의 모임이다.
3. 각 블록은 정확히 k개의 점을 포함한다.
4. 서로 다른 점들로 된 모든 짝은 정확히 λ개의 블록에만 포함된다.

이 때, (X, A)는 (n, k, λ)-BIBD 또는 (n, b, r, k, λ)-BIBD로 표기한다. 여기서, 각 점들은 정확히 $r = \frac{\lambda(n-1)}{k-1}$개의 블록에만 나타나고, 블록의 개수 b는 정확히 $b = \frac{nr}{k} = \frac{\lambda(n^2-n)}{k^2-k}$개 이다.

[정의 2.4] (X, A)의 인접행렬은 다음과 같이 정의되는 $n \times b$ 행렬 $M = [m_{i,j}]$이다.

$$m_{i,j} = \begin{cases} 1 & \text{if } x_i \in A_j \\ 0 & \text{if } x_i \notin A_j \end{cases}$$

여기서 $X = \{x_i : 1 \leq i \leq n\}$이고, $A = \{A_j : 1 \leq j \leq b\}$이다.

[예 2] (7,7,3,3,1)-BIBD와 그 인접행렬
$X = \{1,2,3,4,5,6,7\}$, $A = \{\{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,5,7\}, \{1,5,7\}, \{2,6,7\}, \{1,3,7\}\}$일 때, (X, A)는 (7,7,3,3,1)-BIBD이며, 인접행렬 M은 다음과 같다.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

2.2.2 BIBD로부터 $(2, n)$-VTS의 구성

(n, b, r, k, λ)-BIBD의 인접행렬을 M_1이라 하자. 모든 행의 앞부분에 r개의 1, 나머지 부분에 $b-r$개의 0이 채워지는 $n \times b$ 행렬을 M_0로 정의한다. 확장 화소의 수 m은 b가 된다. 또한 M_0와 M_1의 모든 행에 대한 가중치는 r이며, M_0의 두 행에 대한 "or"의 가중치도 r이다. M_1의 어떤 두 행에 대하여 모두 "1"이 있는 열은 정확히 λ개가 존재한다. 따라서, M_1의 두 행에 대한 "or"의 가중치는 $2r-\lambda$가 되고, 상대휘도는 $\gamma = \frac{2r-\lambda-r}{b} = \frac{r-\lambda}{b}$가 된다. 따라서 다음의 결과를 얻는다.

[정리2.5] (n, b, r, k, λ)-BIBD가 있다고 하면, 확장 화소의 수 $m=b$, 상대휘도 $\gamma=(r-\lambda)/b$인 $(2, n)$-VTS가 존재한다.

특히, $b=n$일 때 symmetric이라 하고, (n, k, λ)-BIBD가 symmetric일 때, 그 derived BIBD는 $(k, \lambda, \lambda-1)$-BIBD로, residual BIBD는 $(n-k, k-\lambda, \lambda)$로 구해지며 역시 BIBD가 되는 것이 알려져 있다. 한편, $2<t\leq n$인 정수 t에 대하여, 차수가 $4t$인 Hadamard 행렬이 존재한다는 것은 symmetric $(4t-1, 2t-1, t-1)$-BIBD가 존재한다는 것과 동치라는 사실에서 다음의 계를 얻는다.

[계 2.6] 차수 $4t$인 Hadamard 행렬이 존재한다면, 확장 화소의 수가 $m=4t-1$이고, 상대휘도가 $\gamma=t/(4t-1)$인 $(2, 4t-1)$-VTS가 존재한다.

[예 3] $m=7$과 $\gamma=2/7$인 (2,7)-VTS를 위한 기저 행렬

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

2.2.3 최적의 휘도를 갖는 $(2, n)$-VTS

Blundo, Santis and Stinson은 $(2, n)$-VTS에서 휘도에 대한 상한을 구하였다.[9]

[정리2.7] 임의의 $(2, n)$-VTS에 대하여, $\gamma^*(n)\geq\gamma$이 성립하고, 여기서 γ^*는

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

이 기법은 계2.6에 의하여 다음이 성립하므로 모두 최적인 휘도를 가진다.

$$\gamma^*(4t-1)=\frac{2t(2t-1)}{(4t-1)(4t-2)}=\frac{t}{4t-1}$$

BIBD를 이용하여 최적의 휘도를 갖는 $(2, n)$-VTS를 구성하여 보자. 먼저 $n=1 \bmod 4$인 경우를 $n=4t+1$로 나타낸다.만일 $(4t+1, 2t, 2t-1)$-BIBD가 존재한다면 $b=8t+2$ 이고 $\gamma=4t$이다. 정리2.5를 적용하여 확장 화소의 수 $m=8t+2$와 최적인 상대휘도 $\gamma=\gamma^*(4t+1)$을 갖는 $(2, 4t+1)$-VTS를 얻을 수 있다. 만일, symmetric$(8t+3, 4t+1, 2t)$-BIBD가 존재한다면 그 derived BIBD로서 $(4t+1, 2t, 2t-1)$-BIBD를 구성할 수 있다. 이 때, symmetric BIBD의 존재는 사실상 차수 $8t+4$의 Hadamard 행렬의 존재를 의미하므로 정리2.5의 계로서 다음을 얻는다.

[계2.8] 차수 $8t+4$의 Hadamard행렬이 존재한다면, 확장 화소의 수 $m=8t+2$와 상대휘도 $\gamma=\gamma^*(4t+1)$를 갖는 $(2, 4t+1)$-VTS가 존재한다.

다음으로 n이 짝수일 때, $n=2t$로 쓰자. 만일 $(2t, t, t-1)$-BIBD가 존재한다면 $b=4t-2$이고 $\gamma=2t-1$이다. 정리2.5를 적용하여 확장 화소의 수 $m=4t-2$와 최적인 상대휘도 $\gamma=\gamma^*(2t)$를 갖는 $(2, 2t)$-VTS를 얻을 수 있다. 만일, symmetric $(4t-1, 2t-1, t-1)$-BIBD가 존재한다면 그 residual BIBD로서 $(2t, t, t-1)$-BIBD가 구성될 수 있음을 뜻한다. 이 때, symmetric BIBD의 존재는 사실상 차수 $4t$의 Hadamard 행렬의 존재를 뜻하므로 정리2.5의 계로서 다음을 얻는다.

[계2.9] 차수 $4t$의 Hadamard 행렬이 존재한다면, 확장 화소의 수 $m=4t-2$와 상대휘도 $\gamma=\gamma^*(2t)$을 갖는 $(2, 2t)$-VTS가 존재한다.

정리2.5, 계2.6, 계2.8 및 계2.9로부터 다음의 정리를 얻을 수 있다.

[정리2.10] Hadamard Matrix Conjecture가 성립한다면 $n\geq 2$인 모든 정수에 대하여, 최적의 상대휘도 $\gamma^*(n)$을 갖는 $(2, n)$-VTS가 존재하며, 이 때 확장 화소의 수 m은 다음과 같다.

$$m=\begin{cases}2n-2, & \text{if } n \text{ is even}\\ n, & \text{if } n\equiv 3 \bmod 4\\ 2n, & \text{if } n\equiv 1 \bmod 4\end{cases}$$

결과적으로 모든 $(2, n)$-VTS는 Hadamard 행렬에서 얻어지는 BIBD로부터 구성될 수 있고, 확장

화소의 수는 최적의 상대휘도를 갖는 모든 $(2, n)$-VTS중에서 최적임이 증명되어 있다.

Ⅲ. 새로운 시각암호 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 2의 기저행렬 구성

Naor & Shamir는 (n, n)-VTS의 기저행렬을 구성하기 위하여 S_0는 모든 열에서 짝수 cardinality를, S_1은 홀수 cardinality를 갖는 행렬로 구성하였다. 여기서는 S_1을 구성하기 위하여 모든 열의 해밍 가중치가 2인 경우로 제한한다. 즉, S_0는 각 행의 가중치가 ${}_{n-1}C_1$인 같은 행으로 구성하며, S_1의 각 행의 가중치는 같으나 각 열의 가중치가 2인 모든 경우를 나열한 것이 된다. 이렇게 구성된 S_0, S_1의 각 행렬에서 임의의 두 행을 겹치면 가중치의 차는 항상 $n-2$가 되므로 상대휘도는 $n-2/{}_nC_2$이 되어 흑과 백의 구별이 가능하게 된다. 예를 들어, $n=5$인 경우의 기저행렬은 다음과 같다 ($m=10$, $\gamma=3/10$).

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

이 방법은 Naor & Shamir의 방법과 비교하여 휘도는 좋지만, n이 커짐에 따라 확장 화소의 수가 너무 증가되어 구현이 어렵게 된다. 따라서 S_1을 전치하여 얻어지는 표본 행렬을 정의하여 이것을 이용한 새로운 구성법을 다음에 제시한다.

3.2 표본행렬에 의한 구성법-제안방법 I

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

(1) 주어진 n에 대하여, 확장 화소의 값을 $\min\{m | n \leq {}_mC_2\}$인 정수 m으로 한다.

(2) m값에 따라 결정되는 표본행렬 S를 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.

(3) 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.

[예4] $n=16$에 대한 $(2, n)$-VTS를 위한 기저행렬 S_0, S_1:

(1) $n \leq {}_mC_2$를 만족하는 최소의 $m=7$

(2) 표본행렬 S와 기저 행렬 S_0, S_1은 각각 다음과 같다.

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

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

구성 가능한 ${}_{21}C_{16}$개 중에서 위에 선택된 임의의

S_0, S_1에서 두 행의 겹침에 의한 가중치의 차는 1 또는 2가 된다.

3.3 확장 표본행렬에 의한 구성법-제안방법 II

3.2의 표본행렬 구성에서 확장 화소의 수를 $n \le {}_mC_2$를 만족하는 최소의 m으로 제한하였으나, $n \le {}_mC_{\lfloor m/2 \rfloor}$을 만족하는 최소 정수로 하면 표본행렬의 행의 수가 최대로 되어 상대적으로 확장 화소의 수를 더욱 줄이는 효과를 얻을 수 있다.

(1) 주어진 n에 대하여, $n \le {}_mC_{\lfloor m/2 \rfloor}$을 만족하는 최소의 정수 m을 구한다.
(2) m에 따라 결정되는 표본행렬 S를 다음과 같이 구성한다.
  ① 각 행의 가중치가 ${}_{m-1}C_{\lfloor m/2 \rfloor - 1}$이고, 각 열의 가중치가 $\lfloor m/2 \rfloor$인 $m \times {}_mC_{\lfloor m/2 \rfloor}$ 행렬 M을 구성한다.
  ② M을 전치하여 얻어진 ${}_mC_{\lfloor m/2 \rfloor} \times m$ 행렬을 확장된 표본행렬 S로 둔다. 즉, S는 각 행의 가중치가 $\lfloor m/2 \rfloor$인 모든 경우를 나열한 것과 같다.
(3) S_0와 S_1은 3.2의 표본행렬에 의한 구성법과 같은 방법으로 얻어진다.

[예5] $n=16$에 대한 $(2, n)$-VTS를 위한 기저행렬 S_0, S_1:

(1) $n \le {}_mC_{\lfloor m/2 \rfloor}$를 만족하는 최소의 $m=6$.
(2) 표본 행렬 S와 기저 행렬 S_0와 S_1은 각각 다음과 같다.

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

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

구성 가능한 ${}_{20}C_{16}$개 중에서 위에 선택된 임의의 S_0, S_1에서 두 행의 겹침에 의한 가중치의 차는 1, 2 또는 3이 된다.

단계 (2)에서 각 행의 가중치를 2 대신 $\lfloor m/2 \rfloor$으로 하면 표본행렬 S의 행의 수 n이 최대가 되므로 확장 화소의 수를 줄이는 효과가 발생한다. 한편, 비밀 영상을 복원할 때 가중치가 다른 짝들이 생기게 되며, 그 범위는 1~ $\lfloor m/2 \rfloor$으로 된다. 결과적으로 제안 방법의 확장 화소의 수 m은 $n \le {}_mC_{\lfloor m/2 \rfloor}$을 만족하는 최소 정수가 되고, 상대휘도 γ의 범위는 $\frac{1}{m} \le \gamma \le \frac{\lfloor m/2 \rfloor}{m}$로 된다.

3.4 그룹화에 의한 복수의 시각 비밀 분산법

3.3에서 두 행의 겹침에 의한 가중치의 차가 두 가지 이상의 다른 값을 갖게 되므로 그룹화에 의해 복수의 비밀영상을 분산시킬 수 있다. 즉, 표본행렬 S의 임의의 한 행을 기준으로 각 행을 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 $n \le {}_mC_{\lfloor m/2 \rfloor}$을 만족하는 최소 정수로 한다. m값에 따라 구해진 표본행렬 S에 대하여 편의상 첫째 행을 base로 하면 base와 각 행을 겹쳐서 나타날 수 있는 가중치의 차에 따라 $\lfloor m/2 \rfloor$개의 그룹으로 나눌 수 있다. 이 때 각 그룹의 크기는 다음과 같다.

1) 가중치의 차가 1인 그룹의 크기:

$|G_1| = {}_{m-\lfloor m/2 \rfloor}C_1 \times {}_{\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor - 1}$,

2) 가중치의 차가 2인 그룹의 크기:

$|G_2| = {}_{m-\lfloor m/2 \rfloor}C_2 \times {}_{\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor - 2}$,

3) 가중치의 차가 3인 그룹의 크기:

$|G_3| = {}_{m-\lfloor m/2 \rfloor}C_3 \times {}_{\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor - 3}$,

...

4) 가중치의 차가 $\lfloor m/2 \rfloor$ 인 그룹의 크기:

$$|G_{\lfloor m/2 \rfloor}| = {}_{m-\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor} \times {}_{\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor - \lfloor m/2 \rfloor}$$

여기서 크기가 가장 적은 그룹의 가중치의 차는 항상 $\lfloor m/2 \rfloor$ 이 되고, 그 크기는 다음과 같다.

$$\min|G_i| = \begin{cases} 1 & , \ m = even \\ (m+1)/2 & , \ m = odd. \end{cases}$$

위의 각 그룹은 base행을 기준으로 겹치면 가중치의 차가 1씩 증가하여 $\lfloor m/2 \rfloor$ 까지 달라지게 되므로 복수의 비밀영상을 분산시키는 VTS를 구현할 수 있다. 또한, 각 그룹내의 행을 겹쳐감에 따라 가중치의 차가 커지므로 슬라이드를 겹칠수록 휘도가 좋아지는 특징을 갖는다.

{복수의 비밀영상을 분산시키기 위한 기저행렬 구성}

그룹의 수를 g라 하고, 크기가 가장 작은 그룹에서 $\min|G_i| = p$라 하자.

(1) 확장 화소의 수 m:
$\min\{m | g \le \lfloor m/2 \rfloor$ and $n < {}_mC_{\lfloor m/2 \rfloor}$ and $(p \le {}_{m-\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor} \times {}_{\lfloor m/2 \rfloor}C_{\lfloor m/2 \rfloor - \lfloor m/2 \rfloor})\}$

(2) 주어진 m에 대한 표본행렬 S를 구한다.

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

$m=9$일 때, 표본행렬 S는 다음과 같고, 첫 번째 행을 base로 하여 임의의 행과 겹치면 가중치의 차가 1, 2, 3, 4인 4가지의 그룹이 발생하게 된다.

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

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 집합을 A, B, C, D의 네 그룹으로 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 및 D의 회원이 3명, 5명, 4명 및 5명일 경우, 'A', 'B', 'C' 및 'D'라는 비밀정보를 분산시키기 위한 경우를 가정한다. 표본행렬 S를 이용하여 기저행렬 S_0, S_1을 아래와 같이 구성한다.

각 그룹에 대하여 백의 부 화소를 위하여 S_0행렬에서 선택하고, 그룹A에 대한 흑의 부 화소를 위하여 S_1행렬의 a중의 임의의 행을, 그룹B에 대한 흑의 부 화소를 위하여 S_1행렬의 b중의 임의의 행을, 그룹C에 대한 흑의 부 화소를 위하여 S_1행렬의 c중의 임의의 행을, 그룹D에 대한 흑의 부 화소를 위하여 S_1행렬의 d중의 임의의 행을 각각 할당한다.

그 결과, 복원 시 그룹에 대한 휘도 차에 의해서 같은 그룹 내에서 선택된 임의의 두 슬라이드를 겹치면 각각 'A', 'B', 'C' 및 'D' 가 나타나고, base와 겹쳐도 역시 'A', 'B', 'C' 그리고 'D' 가 나타난다. 또, 슬라이드를 여러 장 겹쳐감에 따라 가중치가 증가하므로 휘도가 더욱 좋아지는 특징을 갖게 된다.

$$S_0=\begin{bmatrix}1\,1\,1\,1\,0\,0\,0\,0\,0\\ 1\,1\,1\,1\,0\,0\,0\,0\,0\\ 1\,1\,1\,1\,0\,0\,0\,0\,0\\ 1\,1\,1\,1\,0\,0\,0\,0\,0\\ 1\,1\,1\,1\,0\,0\,0\,0\,0\\ 1\,1\,1\,1\,0\,0\,0\,0\,0\\ 1\,1\,1\,1\,0\,0\,0\,0\,0\\ 1\,1\,1\,1\,0\,0\,0\,0\,0\\ 1\,1\,1\,1\,0\,0\,0\,0\,0\end{bmatrix},\ S_1=\begin{bmatrix}1\,1\,1\,1\,0\,0\,0\,0\,0\\ 1\,1\,1\,0\,1\,0\,0\,0\,0\\ 1\,0\,1\,1\,0\,0\,0\,1\,0\\ 1\,1\,0\,1\,0\,1\,0\,0\,0\\ 1\,1\,0\,0\,0\,0\,0\,1\,1\\ 1\,0\,1\,0\,1\,0\,0\,0\,1\\ 1\,1\,0\,0\,0\,1\,1\,0\,0\\ 0\,0\,1\,1\,1\,0\,0\,1\,0\\ 0\,1\,0\,1\,0\,1\,0\,1\,0\\ 1\,0\,0\,0\,1\,1\,1\,0\,0\\ 0\,1\,0\,0\,0\,1\,1\,0\,1\\ 0\,0\,0\,1\,1\,1\,1\,0\,0\\ 0\,0\,1\,0\,0\,0\,1\,1\,1\\ 0\,0\,0\,0\,1\,1\,1\,1\,0\\ 0\,0\,0\,0\,1\,1\,1\,0\,1\\ 0\,0\,0\,0\,1\,1\,0\,1\,1\\ 0\,0\,0\,0\,1\,0\,1\,1\,1\\ 0\,0\,0\,0\,0\,1\,1\,1\,1\end{bmatrix}$$

(base, a, b, c, d)

N. 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 γ가 1/36 이상이면 흑과 백의 화소를 구별할 수 있는 것으로 알려져 있으므로 제안 방법을 기준으로 사용자 수 n가 $3\le n\le 630$인 범위에 대하여 m과 γ를 비교한다.

(1) Naor & Shamir방법(Na & SH)

$m=n,\ \gamma=1/m$

(2) BIBD방법(BIBD)

$$m=\begin{cases}2n-2, & \text{if } n \text{ is even}\\ n, & \text{if } n\equiv 3 \bmod 4,\\ 2n, & \text{if } n\equiv 1 \bmod 4\end{cases}$$

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

(3) 제안방법(Proposed I)

$$m=\min\{m|n\le {}_mC_2\},\ 1/m\le\gamma\le\frac{\lfloor m/2\rfloor}{m}$$

(4) 제안방법(Proposed II)

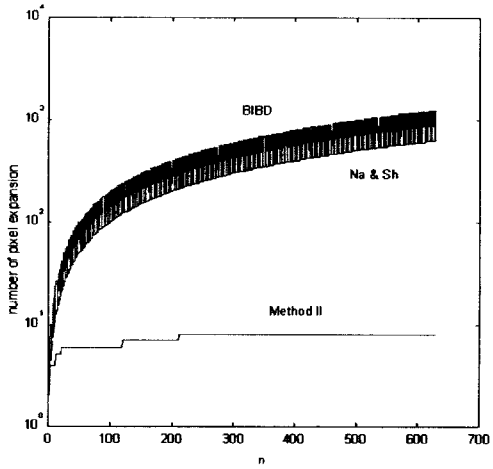
$$m=\min\{m|n\le {}_mC_{\lfloor m/2\rfloor}\},$$

$$1/m\le\gamma\le\gamma\le\frac{\lfloor m/2\rfloor}{m}$$

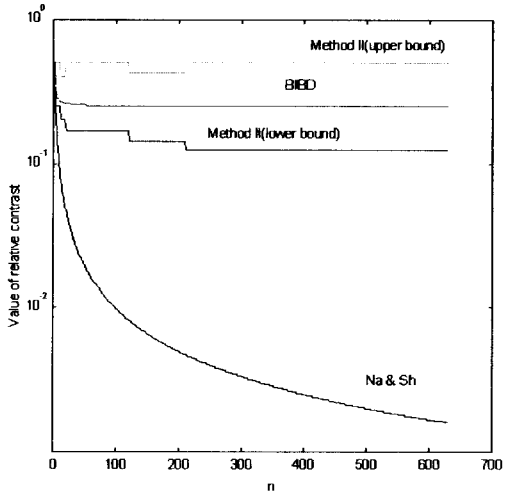
확장 화소의 수 m은 제안방법이 가장 우수하고, Naor & Shamir방법, BIBD 방법의 순서로 커진다. 또한 상대휘도 값 γ은 BIBD방법, 제안방법, Naor & Shamir방법의 순서로 작아진다. 그림2, 3에서 n의 증가에 따른 확장 화소의 수 m과 상대휘도 γ의 변화를 알 수 있다.

결과적으로 제안방법은 확장 화소수의 관점에서 가장 양호하고, 상대휘도의 관점에서는 BIBD가 제안방식의 상한과 하한 사이에 위치하게 되며, Naor & Shamir방법보다 상당히 개선됨을 알 수 있다. 한편, 행렬을 구성하기 위한 BIBD의 발견이 매우 어려우므로 제안방법이 더욱 실용적이라 할 수 있다. 또한, 제안방법은 슬라이드를 겹쳐감에 따라 휘도가 더욱 좋아지는 장점을 가지고 있다.

시뮬레이션 결과를 그림 4~9에 제시한다. 그림 4는 그룹 A의 두 슬라이드를 겹친 결과이고, 그림 5,

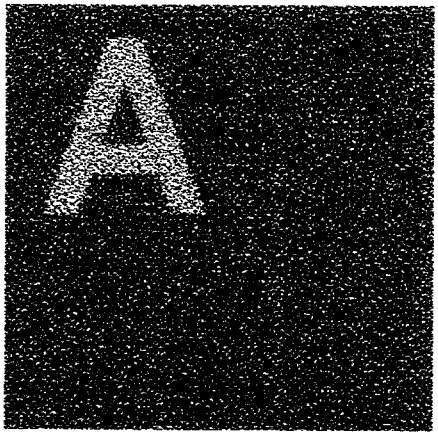


〔그림 2〕 n에 따른 확장 화소의 수 m

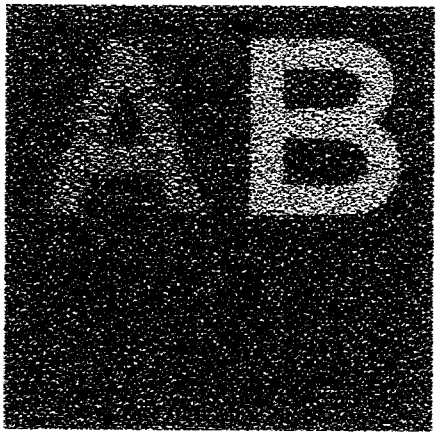


〔그림 3〕 n에 따른 상대휘도 γ

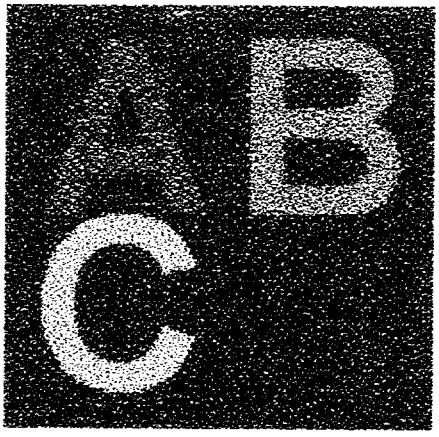
6, 7은 각각 *a*, *b*, *c*, *d*에서 한 장씩 선택한 슬라이드를 차례로 겹쳐감에 따라 복원되는 결과를 나타내고 있다. 그림 8, 9는 한 그룹 내에서 슬라이드를 겹쳐감에 따라 휘도가 좋아짐을 보이고 있다.



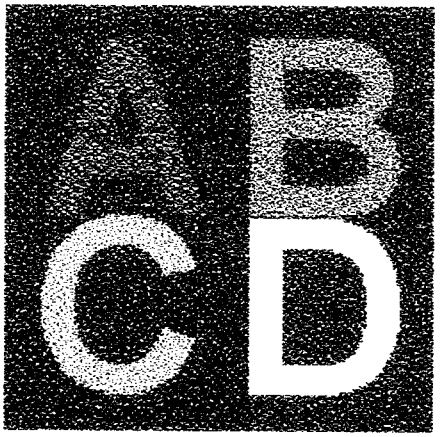
〔그림 4〕 그룹 A의 두 슬라이드를 겹친 결과



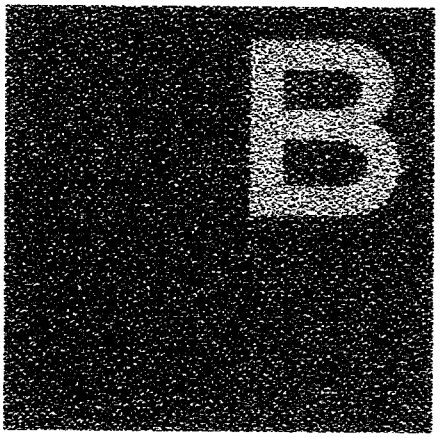
〔 그림 5〕 그룹A, B의 한 장씩 겹친 결과



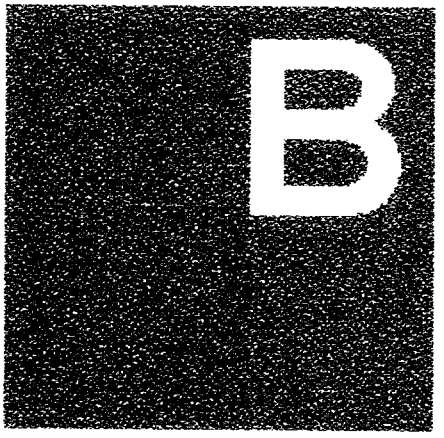
〔그림 6〕 그룹A, B, C의 한 장씩 겹친 결과



〔그림 7〕 그룹A, B, C, D의 한 장씩 겹친 결과



〔그림 8〕 그룹 B의 두 장을 겹친 결과



〔그림 9〕 그룹 B의 네 장을 겹친 결과

V. 결 론

(k, n)비밀 분산법에 기초한 시각암호를 위한 기저 행렬의 구성에 대하여 여러 가지 기법이 연구되어 왔다. Naor & Shamir의 기법은 그 구성이 간결하지만 확장 화소의 수가 너무 커지는 결점이 있다. 또한 BIBD 방법은 Hadamard 행렬을 이용하며 주어진 n에 대한 상대휘도의 관점에서 최적인 것으로 알려져 있다. 그러나, BIBD의 구성이 쉽지 않은 문제점이 있다.

본 연구에서는 (k, n)비밀 분산의 k가 2인 경우에 대하여 확장 화소의 측면에서 BIBD의 한계를 포함하면서 그 구성이 간단할 뿐만 아니라 n을 상당히 크게 하여도 휘도가 많이 개선되는 실용적인 방법을 제안하였다. 나아가 복원 시의 휘도 차에 따라 복수의 비밀영상을 분산시킬 수 있으며 겹치는 슬라이드의 수를 증가시킬수록 휘도가 좋아지는 시각 비밀 분산법을 제안하였다. 향후의 과제로서 임의의 k로 확장 가능한 구성법에 대하여 연구할 예정이다.

참 고 문 헌

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

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

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

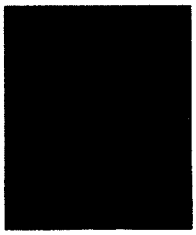
[5] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, "Visual Cryptography for General Access Structures", *Information and Compuation* 129, pp. 86~106, 1996.

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

[7] C. K. Choi, J. H. Park, R. Kohno, "Contrast Analysis According to Hierachical Access Structure on Visual Cryptography Scheme and Its Application into Authentication", *Proc. of SITA*, Vol. 20 No. 1 pp. 217~220 1997.12.

[8] D. R. Stinson, "Combinatorial Designs with Selected Applications Lecture Notes," *Dept. of Computer Science, Univ.of Manitoba*, Dec. 1996.

〈著者紹介〉



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

박 지 환 (Ji-Hwan Park)
1984년 2월 : 경희대학교 전자공학과 졸업 (공학사)
1987년 3월 : 일본 전기통신대학 정보공학과 졸업 (공학석사)
1990년 3월 : 일본 요코하마국립대학 전자정보공학 졸업 (공학박사)
1990년 3월~현재 : 부경대학교 전자컴퓨터정보통신공학부 부교수
1994년 9월~1995년 3월 : 동경대학 생산기술연구소 객원연구원
1996년 4월~현재 : 동경대학 생산기술연구소 협력연구원
1998년 1월~1998년 2월 : 전기통신대학 정보시스템 연구과 방문연구
1999년 7월~1999년 8월: 호주 Monash University, Visiting Research
〈관심분야〉 정보이론 및 응용, 암호 및 정보보안
http://unicorn.pknu.ac.kr/~jhpark