通信情報保護學會論文誌
第 8 卷 第 2 號, 1998. 6

시각암호에서 계층적 접근구조에 따른 휘도분석과 식별에 응용

최 창 근**, 박 지 환*

Contrast Analysis According to Hierarchical Access Structure on Visual Cryptography Scheme and Its Application into Human identification

Chang-Keun Choi**, Ji-Hwan Park*

요 약

시각암호는 비밀화상을 share라 불리는 암호화된 형태로 분산하는 방법으로서 n명의 참여자로 이루어진 집합 P에 대하여, 각 참여자는 share로 구성된 슬라이드(transparency)를 한장씩 부여받는다. 참여자들의 인가된 부분집합은 슬라이드를 중첩시켜 시각적으로 비밀정보를 복원할 수 있지만, 다른 부분집합은 비밀정보를 복원할 수 없다. 이 방법은 비밀정보를 복원하기 위하여 인간의 시각 체계를 이용하므로 컴퓨터를 사용한 복잡한 연산이 필요 없는 이점이 있는 반면에 복원화상의 휘도가 손실되는 단점이 있다.

이 논문에서는 참여자의 계층화를 고려한 (2, n) VCS(Visual Cryptography Scheme)를 구성하기 위한 새로운 모델을 제안하고 계층적 접근구조에 의해 휘도를 개선하는 방법을 보인다. 제안하는 방법의 효율을 평가하기 위하여 (2, n) VCS로 재구성되는 화상의 휘도를 분석한다. 또한, 그 응용으로서 한 장의 슬라이드로 사용자와 시스템 사이에 상호식별이 가능한 메카니즘을 제시한다

Abstract

The visual cryptography scheme for a set P with n participants is one of the ways to manage a secret image by dividing it into some encrypted images called shares. At that time, each participant receives one transparency consists of share. The permitted subset of participants can visually recover an original image, but another subset of participants has no information. There is a merit that need not to have complex computations by replacing human visual system to decrypt the original image, whereas it has a loss of contrast of reconstructed image.

*부경대학교 전자계산학과
**요코하마국립대학 전자정보공학과

In this paper, we propose a new model to construct 2 out of n visual cryptography scheme considering group of participants and show the methods improving the contrast according to hierarchical access structure. We derive a formula to evaluate the efficiency of the proposed method and analyze the contrast of reconstructed image in 2 out of n visual cryptography scheme. Futhermore, we suggest a mechanism for the interactive identification between user and system with only one transparency.

1. 서 론

컴퓨터 네트워크의 발달과 더불어 다양한 형태의 정보를 네트워크를 통하여 접근할 수 있지만, 인가되지 않은 공격자로부터 비밀정보를 보호해야 할 필요성이 강조되고 있다. 이를 위한 비밀 분산법[1]은 정당한 자격의 참여자들이 자신에게 할당된 비밀키를 결합하여 비밀 값을 결정하는 것이며, 정당한 참여자가 아닌 경우에는 비밀 값의 결정이 불가능하도록 하는 방법이다. 그러나, 이 방식은 비밀의 분산과 복호에 있어서 안전성을 유지하기 위하여 방대한 연산과 복잡한 구성 때문에 고성능 컴퓨터가 요구된다. 따라서, 새로운 형태의 비밀 분산법으로 분산하고자 하는 비밀을 흑과 백으로 이루어진 화상을 이용하여 시각적으로 간단히 복호할 수 있는 시각암호가 Naor & Shamir[2]에 의해 제안되었다.

(k, n) 시각암호 방식(Visual Cryptography Scheme : VCS)은 비밀정보를 share로 이루어지는 n장의 슬라이드(transparency)에 분산시켜 k이상의 임의의 슬라이드를 중첩해야만 비밀을 복원할 수 있는 형태이다. 이에 대한 연구로 시각 복호형 다중 비밀 분산법[3], 일반 접근구조에 의한 시각 복호형 비밀 분산법[4], 계층적 접근구조에 따른 시각 비밀 분산법[5] 등이 있다.

VCS의 기본은 흑과 백의 화소로 구성된 원화상에 대하여 각 화소는 n개의 share로 분산되고, 각 share는 m개의 부화소(subpixel)로 확장된다. 상대적 차이(relative difference) $\alpha(m)$을 결정하는 중요한 파라미터인 m이 커지면 $\alpha(m)$이 너무 작아져 복원화상의 시각적 인식이 어렵다. 따라서, m을 작게 하여 상대적 차이 $\alpha(m)$를 높이거나, m에 의존하지 않으면서 복원화상의 흑과 백화소 사이의 휘도를 높이는 방법이 요구된다. 본 논문에서는 여러 가지 응용이 기대되는 $k=2$일 때, m이 커지더라도 복원화상의 휘도를 증가시킬 수 있는 새로운 모델과 구성법을 제안한다.

네트워크를 이용한 서비스의 제공을 정당한 사용자만이 받기 위하여 개인 식별 등의 기술이 도입되었으나, 부정사용이나 패스워드에 대한 공격을 목적으로 하는 엿보기 공격(peeping attack) 또는 무작위 공격 등으로 인한 위협을 받게 되었다. 이를 해결하기 위한 방법으로 시스템과 사용자 사이에 미리 비밀정보를 규정하여 시스템이 제시한 질문에 대하여 간단한 연산을 수행한 결과를 응답으로 입력하는 대화형 개인 식별[6]이 제안되었으며, 나아가 시각 복호형 비밀 분산법을 적용시킨 응용[7]이 연구되어 왔다. 그러나, 기존의 시각 복호형 개인 식별에서는 1회에 한하여 시각암호를 적용하므로 엿보기 공격 등에 약한 취약점이 있다. 따라서, 본 논문에서는 2단계 식별을 적용하여 이 문제점을 해결한다.

2장에서 기본 모델과 접근구조를 위한 가상 그룹을 정의하고, 3장에서는 시각암호 적용을 위한 행렬 구성의 일반화, Stronger Access Structure Group(SASG :Γ_{ss}), General Access Structure Group(GASG :Γ_{gs}) 및 Prohibited

Access Structure Group(PASG : Γ_{PS})으로 그룹화 하여 계층적 접근구조로 분류하고 휘도를 분석한다. 4장에서는 제안 방법의 휘도를 개선하기 위한 행렬 구성과 그 휘도를 분석한다. 5장에서는 대화형 개인 식별에 적용하기 위하여 (2, n) VCS를 2단계 식별에 응용하는 메카니즘을 제안하고, 6장에서 결론과 향후 연구과제를 도출한다.

2. 모 델

2.1 기본모델

시각 비밀 분산법의 가장 간단한 형태는 숨기고자 하는 비밀정보가 흑과 백 화소의 집합으로 구성되고 서로 개별적으로 조작된다고 가정한다. 각 화소는 n개의 share로 확장되어 각 슬라이드에 분산된다. 각 share는 한 화소에 대하여 흑과 백으로 구성되는 m개의 부화소로 확대된다.

이는 결과적으로 i번째 share에서 j번째 부화소가 흑이면 $m_{ij}=1$인 $n \times m$부울 행렬 $M=m_{ij}$로 표현되는 것이다. 각각의 share i_1, i_2, ..., i_r이 함께 중첩되었을 때 결합된 share의 계조(gray-level)는 "or 된" m벡터 V의 해밍 가중치 $w(V)$에 비례한다. P={1, ... , n}을 참여자로 불리는 원소의 집합으로 둔다. Γ_0는 (1)식과 같이 정의한다.

$$\Gamma_0=\{C : C=\{i,j\}\text{는 } \binom{n}{2}\text{로 생성 가능한 부분집합}, 1 \le i < j \le n\} \quad (1)$$

또한, Γ_{PS}는 (2)식과 같이 정의한다.

$$\Gamma_{PS}=\{a=(i+j) \bmod n,\ b=(i+k) \bmod n\} \in \Gamma_0 : \exists i \in \text{P에 대하여}, 0 \le j \le n-2,\ 1 \le k \le n-1,\ j\text{는 짝수},\ k\text{는 홀수} \quad (2)$$

단, a 또는 b가 0일 때는 n으로 대치.

따라서, $\Gamma_{PS} \subseteq \Gamma_0$이고 $\Gamma_0 \setminus \Gamma_{PS}=\Gamma_{SS} \cup \Gamma_{SS}$로 정의하면 $\{\Gamma_{SS} \cup \Gamma_{SS}\} \cap \Gamma_{PS} = \varnothing$이다.

[예제1] $n=10$일 때,

Γ_0는 45개의 원소로 이루어지는 집합이다. 임의의 홀수 i를 3이라고 할 때 $\Gamma_{PS}=\{\{3, 4\}, \{5, 6\}, \{7, 8\}, \{9, 10\}, \{1, 2\}\}$이며, $\Gamma_{SS} \cup \Gamma_{SS}=\Gamma_0 \setminus \Gamma_{PS}$는 Γ_{PS}를 제외한 원소를 포함한다.

[정의1] $\langle \Gamma_{SS} \cup \Gamma_{SS}, \Gamma_{PS} \rangle$는 n명의 참여자 집합의 접근구조이다. $A \in \{\Gamma_{SS}, \Gamma_{SS}\}$에 대하여 임의의 행의 집합을 $E_A=i_1, ..., i_r$, 문턱치를 $stack_A$라 하자. 만약 $\alpha(m)$과 $stack_A$가 아래의 조건을 만족하면, $n \times m$의 다중 부울 행렬의 집합 C^0와 C^1은 $\langle \Gamma_{SS} \cup \Gamma_{SS}, \Gamma_{PS}, m \rangle$ VCS를 구성한다.

(1) C^0에 대하여, E_A 원소의 "or" 벡터 V의 $w(V) \le stack_A - \alpha(m)$. m를 만족하고, C^1에 대하여, E_A 원소의 "or" 된 벡터 V의 $w(V)=stack_A$를 만족하면 비밀정보를 복원할 수 있다.

(2) $A \in \{\Gamma_{PS}\}$에 대하여, $n \times m$의 C^0와 C^1 다중행렬에 각각 제한을 가하여 얻을 수 있는 $r \times m$ 크기의 다중행렬 R^0와 R^1에서 E_A의 각 share를 중첩하여도 비밀정보를 복원할 수 없다.

(1)은 화상의 휘도에 관한 성질로서 $\{\Gamma_{SS} \cup \Gamma_{SS}\}$의 사용자가 슬라이드를 중첩할 때 분산된 정보를 복원할 수 있음을 의미하며, $\alpha(m) \cdot m$은 화상의 휘도, $stack_A$는 접근그룹에서의 문턱치이다. (2)는 안전성(security)에 관한 성질로서 Γ_{PS}의 사용자 share를 중첩하여도 분산된 비밀 정보를 복원할 수 없음을 의미한다.

정의1에 의하여 "or" 된 벡터 V의 $w(V)$에 비례하는 결합된 share의 계조는 문턱치의 집합인 $\{stack_A\}_{A \in \{\Gamma_{SS}, \Gamma_{SS}\}}$와 $\alpha(m)$에 따라 시각적인

차이를 보일 수 있다. 이는 그룹에 따라 비밀 정보를 복원할 수 있는 그룹과 그렇지 않는 그룹으로 분류할 수 있음을 의미한다.

[정의 2] $\langle \Gamma_{sg} \cup \Gamma_{gg}, \Gamma_{pg} \rangle$는 n명의 참여자 집합의 접근구조라 하자. Γ_{sg}, Γ_{gg} 및 Γ_{pg}에 대한 각각의 $n \times m$ 부울 행렬 C_{sg}^0와 C_{sg}^1, C_{gg}^0와 C_{gg}^1및 C_{pg}^0와 C_{pg}^1의 다중 집합들은 만약 $\alpha(m)$과 stack_A가 아래의 조건을 만족하면 $\langle \Gamma_{sg}, \Gamma_{gg}, \Gamma_{pg}, m \rangle$ VCS를 구성할 수 있다.

(1) C_{sg}^0에 대하여 E_A의 *"or"* 된 벡터 V는 $w(V) \le stack_A - \alpha(m) \cdot m$, 반면에 C_{sg}^1에 대하여 E_A의 "or" 된 벡터 V는 $w(V) = stack_A$이면 분산된 비밀 정보를 완전 복원할 수 있다.

(2) $n \times m$의 C_{gg}^0와 C_{gg}^1에서 행 $i_1, \ldots, i_r$로 제한함으로서 얻어지는 $r \times m$행렬은 흑과 백의 해밍 가중치가 같거나 다른 경우가 동시에 발생하기 때문에 $E_A \in \Gamma_{gg}$는 분산된 비밀 정보를 제한적으로 복원하게 된다.

(3) 백과 흑에 대한 $n \times m$의 행렬인 C_{pg}^0와 C_{pg}^1에서 행 $i_1, \ldots, i_r$로 제한함으로서 얻어지는 $r \times m$행렬은 동일한 해밍 가중치를 가지기 때문에 $E_A \in \Gamma_{pg}$는 분산된 비밀 정보를 복원할 수 없다.

(1)은 화상의 휘도에 관계되는 성질로서 SASG에 속하는 임의의 원소 집합은 그들의 슬라이드를 중첩함으로서 비밀을 복원할 수 있다. (2)는 비밀에 대하여 접근을 제한하는 GASG 구조로서 비밀이 불완전하게 인식된다. 이것은 C_{gg}^1에서의 해밍 가중치가 C_{gg}^0에서의 가중치와 같거나 큰 것이 동시에 존재하므로 비밀이 부분적으로 복원되기 때문이다. (3)은 PASG에 속하는 임의의 원소 집합의 흑과 백에 대한 해밍 가중치가 동일하므로 어떠한 정보에 대하여 접근 효력이 없음을 나타낸다. 따라서, 제안 모델은 기존의 모델과는 달리 접근구조에 따라 $(2,n)$ VCS의 비밀을 달리 인식할 수 있어 계층적 접근이 가능한 특징을 갖는다.

2.2 접근구조를 위한 가상그룹

계층적 접근구조에 기초한 시각암호를 위하여 그룹화가 선행되어야 한다. 이는 행렬을 사용하여 실현할 수 있으며, 그 구성법은 다음과 같다. 참여자의 수 n 에 대하여 $h=(n/2)-1$로 한다. F는 모든 원소가 1인 $h \times 1$ 크기의 행렬이며, I는 대각선상의 원소만이 1인 $h \times h$ 크기의 단위행렬이다. $F \circ I$ 는 F 와 I의 연결(concatenation)로 얻어지는 $h \times (h+1)$ 크기의 행렬로 정의한다. $(F \circ I)^c$ 는 $F \circ I$의 부울 보수 행렬이며, RM(Real Matrix)은 $(F \circ I)^T \circ ((F \circ I)^T)^c$로 이루어지는 행렬이다. $(F \circ I)$와 $(F \circ I)^c$를 연결하여 만들어지는 행렬 MM(Medium Matrix)에 대하여, T는 이를 다시 전치 함으로서 획득할 수 있는 크기가 $2(h+1) \times h$인 행렬이다. 임의의 두 행의 "or" 연산에 따라 다양한 해밍 가중치를 가지는 가상행렬 VM(Virtual Matrix)은 T와 T^c를 연결하여 크기 $2\{(h+1) \times h\}$의 행렬로 만들어진다. 참여자가 $P=\{1, 2, \ldots, n\}$으로 이루어진 집합에서 $(2,n)$ VCS의 적용을 위한 전체집합을 Γ_0 로 정의하였다. Γ_0내의 원소들은 VM상의 임의의 두 벡터가 *"or"*된 해밍 가중치에 따라 i개의 그룹으로 분할된다. 해밍 가중치가 w인 i번째 그룹을 $\Gamma_i(w)$, $1 \le i \le 5$ 로 나타내고, 이를 가상그룹(Virtual Group)이라 한다. 이와 같이 $\Gamma_i(w)$로 분할된 그룹들은 Γ_{sg}, Γ_{gg}및 Γ_{pg}의 구조를 고려할 수 있는 기본 그룹이 된다.

[예제2] $n=12$일 때, 가상행렬 VM과 가상그룹 $\Gamma_i(w)$는 다음과 같게 된다.

$$VM = \begin{pmatrix} 1111100000 \\ 0000011111 \\ 1000001111 \\ 0111110000 \\ 0100010111 \\ 1011101000 \\ 0010011011 \\ 1101100100 \\ 0001011101 \\ 1110100010 \\ 0000111110 \\ 1111000001 \end{pmatrix}$$

♦ $i=1$ 일 때

$\Gamma_{PS} = \{\{1,2\},\{3,4\},\{5,6\},\{7,8\},\{9,10\},\{11,12\}\}$,

$\Gamma_1(10) = \Gamma_{PS} = \{\{1,2\},\{3,4\},\{5,6\},\{7,8\},\{9,10\},\{11,12\}\}$,

$\Gamma_2(9) = \{\{1,3\},\{1,5\},\{1,7\},\{1,9\},\{1,11\},\{2,4\},\{2,6\},$
$\{2,8\},\{2,10\},\{2,12\}\}$,

$\Gamma_3(8) = \{\{3,6\},\{3,8\},\{3,10\},\{3,12\},\{4,5\}\{4,7\},\{4,9\},$
$\{4,11\},\{5,8\},\{5,10\},\{5,12\},\{6,7\},\{6,9\},\{6,11\},$
$\{7,10\},\{7,12\},\{8,9\},\{8,11\},\{9,12\},\{10,11\}\}$,

$\Gamma_4(7) = \{\{3,5\},\{3,7\},\{3,9\},\{3,11\},\{4,6\},\{4,8\},\{4,10\},$
$\{4,12\},\{5,7\},\{5,9\},\{5,11\},\{6,8\},\{6,10\},\{6,12\},$
$\{7,9\},\{7,11\},\{8,10\},\{8,12\},\{9,11\},\{10,12\}\}$,

$\Gamma_5(6) = \{\{1,4\},\{1,6\},\{1,8\},\{1,10\},\{1,12\},\{2,3\},\{2,5\},$
$\{2,7\}\},\{2,9\},\{2,11\}\}$.

$\Gamma_{SS} \cup \Gamma_{SS} = \{\Gamma_0 \setminus \Gamma_{PS}\} = \{\Gamma_2(9) \cup \Gamma_3(8) \cup \Gamma_4(7) \cup \Gamma_5(6)\}$

3. 시각암호를 위한 행렬과 휘도 분석

3.1 행렬 구성의 일반화

시각암호를 이용한 비밀정보 분산을 위하여 share를 구성하려면 흑과 백의 화소에 대한 행렬이 필요하게 된다. 이를 위한 행렬 구성의 일반화는 다음과 같다. 휘도의 차를 가지는 비밀화상을 획득하기 위하여 먼저 백의 화소를 위한 행렬 W를 정의한다. $(h+1) \times (h+1)$크기의 단위행렬 I의 부울 보수 행렬 I'와 $(h+1) \times (2h - h + 1))$ 크기의 모든 원소가 0으로 이루어진 영 행렬(zero matrix)을 연결한 후, 같은 행을 한번씩 반복하여 $n \times (n-2)$크기의 행렬 W를 구성한다.

다음은 흑의 화소를 위한 행렬 RM^* 와 $\tilde{RM}^*$를 정의한다. RM^*는 RM의 모든 행을 한번씩 반복한 $n \times (n-2)$크기의 행렬을 구성하여 만들며, $\tilde{RM}^*$ 는 RM^*을 구성하는 방법과 동일하나 최초의 F대신에 모든 원소가 0인 크기 $h \times 1$ 인 행렬 F' 를 사용하여 만드는 점이 다르다. 행렬 $\tilde{RM}^*$의 행의 수는 참여자 n의 $n/2$이 되는 형태이다. 따라서, RM ($\tilde{RM}$)의 각 행을 $n/2$의 참여자에게 분산하고, 나머지 $n/2$의 참여자에게는 동일한 행을 할당한다. 이는 임의의 한 행을 서로 다른 두 참여자에게 할당하여 $n \times (n-2)$의 구조인 RM^*($\tilde{RM}^*$)로 확대하는 것이다.

[예제3] $n=12$일 때, 위에서 제시된 방법으로 백의 화소 행렬 W와 흑의 화소 행렬 RM^*와 $\tilde{RM}^*$ 를 구성하면 다음과 같다.

$$W = \begin{pmatrix} 1111100000 \\ 1111100000 \\ 1111010000 \\ 1111010000 \\ 1110110000 \\ 1110110000 \\ 1101110000 \\ 1101110000 \\ 1011110000 \\ 1011110000 \\ 0111110000 \\ 0111110000 \end{pmatrix} \quad RM^* = \begin{pmatrix} 1111100000 \\ 1111100000 \\ 1000001111 \\ 1000001111 \\ 0100010111 \\ 0100010111 \\ 0010011011 \\ 0010011011 \\ 0001011101 \\ 0001011101 \\ 0000111110 \\ 0000111110 \end{pmatrix}$$

$$\tilde{RM}^* = \begin{pmatrix} 0000011111 \\ 0000011111 \\ 1000001111 \\ 1000001111 \\ 0100010111 \\ 0100010111 \\ 0010011011 \\ 0010011011 \\ 0001011101 \\ 0001011101 \\ 0000111110 \\ 0000111110 \end{pmatrix}$$

3.2 접근구조의 분류

2장에서 정의한 가상그룹 $\Gamma_i(w)$를 흑과 백의 화소의 분산을 위한 행렬들(W, RM^*, $\tilde{RM}^*$)에 적용하면 표1과 같은 해밍 가중치를 얻게 된다.

〈표 1〉 각 행렬에 가상 그룹 적용시의 해밍 가중치
〈Table 1〉 Hamming weight as applying VG to each matrix

가상그룹 \ 행렬	W	RM^*	$\tilde{RM}^*$	접근구조
$\Gamma_1(w)$	$\frac{m}{2}$	$\frac{m}{2}$	$\frac{m}{2}$	PASG
$\Gamma_2(w)$	$\frac{m}{2}+1$	$m-1$	$\frac{m}{2}+1$	GASG
$\Gamma_3(w)$	$\frac{m}{2}+1$	$\frac{m}{2}+2$	$\frac{m}{2}+2$	SASG
$\Gamma_4(w)$	$\frac{m}{2}+1$	$\frac{m}{2}+2$	$\frac{m}{2}+2$	SASG
$\Gamma_5(w)$	$\frac{m}{2}+1$	$m-1$	$\frac{m}{2}+1$	GASG

행렬 RM^*와 백의 화소 행렬 W의 흑백의 차이를 고려하면 $\Gamma_1(w)$을 제외한 그룹은 흑과 백의 시각적 차이를 인식할 수 있다. 반면, $\Gamma_2(w)$와 $\Gamma_5(w)$그룹의 경우 행렬 $\tilde{RM}^*$와 행렬 W의해밍 가중치를 고려하면 모두 같은 값을 가지므로 시각적 차이를 인식할 수 없으나, 행렬 RM^*와 행렬 W의 해밍 가중치는 다르므로 시각적인 차이를 보인다. 결국, 흑의 화소 행렬 RM^*, $\tilde{RM}^*$와 백의 화소 행렬 W의 해밍 가중치의 차로 비밀정보를 모두 복원하는 것과 부분적으로 복원할 수 있는 성질에 의해 $\Gamma_2(w)$와 $\Gamma_5(w)$는 **GASG**(Γ_{SG})로, $\Gamma_3(w)$와 $\Gamma_4(w)$는 **SASG**(Γ_{SG})로 그룹화 된다. 그리고, $\Gamma_1(w)$는 비밀정보를 복원할 수 없는 PASG(Γ_{PG})로 분류된다.

3.3 휘도의 분석

제안 방법에 의한 $(2,n)$ VCS의 기본행렬에서 백행렬을 $M^0 \in C^0$ 그리고 흑 행렬을 $M^1 \in C^1$이라 하고, $w(r)$는 임의의 행 r의 해밍 가중치로 정의한다. $M_g^t[i]$, $(1 \le i \le n,\ t=\{0,\ 1\},\ g=\{pg,\ gg,\ sg\})$. 는 행렬 M_g^t의 i번째 행으로서 i번째 참여자를 위한 share에 해당한다. 원 화소의 암호화로 간주되는 임의의 share sh_i와 sh_j의 중첩은 비트별 "or" 연산($\vee$)으로 볼 수 있다. 즉, $w(sh_i \vee sh_j) = w(M_g^t[i] \vee M_g^t[j])$, $1 \le i < j \le n$이다.

계층적 접근구조에 따른 $(2,n)$ VCS는 share 크기 m과 상대적 차이 $\alpha(m)$을 가지는 기본행렬 M^0와 M^1으로 구성되며, 그룹 $g=\{pg, gg, sg\}$에 따라 $w(M_g^1[i] \vee M_g^1[j]) - w(M_g^0[i] \vee M_g^0[j]) \ge \alpha(m) \cdot m$이다. 즉,

$g=pg$일때, $w(M_g^1[i] \vee M_g^1[j]) = w(M_g^0[i] \vee M_g^0[j])$

$g=gg$일때,

$$w(M_g^1[i] \vee M_g^1[j]) \le w(M_g^0[i] \vee M_g^0[j]) + \frac{m}{2} - 2 \quad (3)$$

$g=sg$일 때,

$w(M_g^1[i] \vee M_g^1[j]) = w(M_g^0[i] \vee M_g^0[j]) + 1$

원 화소에 대하여 크기 m의 부화소로 확대되는 $(2,n)$ VCS에서 $\alpha(m)$은 다음의 정리와 같은 범위를 가진다.

[정리1] 접근그룹 SASG와 GASG에 따라 m에 의존하는 상대적 차이 $\alpha(m)$의 범위는 $1/m \le \alpha(m) < 1$이다.

(증명) 표1에 의하여 SASG와 GASG의 각각에 속하는 임의의 두 행에 대하여, $w(M^1)=v_1$은 RM^*와 $\widetilde{RM}^*$의 해밍 가중치이고, $w(M^0)=v_0$는 W의 해밍 가중치이다. 따라서, 흑과 백의 화소의 상대적 차이 $\alpha(m)=(v_1-v_0)/m$ 이므로 SASG 및 GASG 각각에 대한 $\alpha(m)$은 (4)식과 같다.

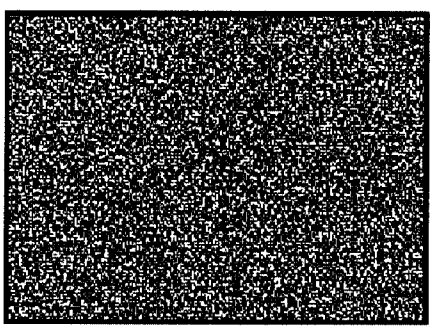
$$\alpha(m)=\frac{(v_1-v_0)}{m}=\begin{cases}\dfrac{1}{m}, & if\ v_1=\dfrac{m}{2}+2\ (SASG)\\[2ex] \dfrac{m-4}{2m}, & if\ v_1=m-1\ (GASG)\end{cases}$$

Naor와 Shamir[2]의 경우는 n의 증가에 따라 선형적으로 m값이 증가하나, 상대적 차이 $\alpha(m)$은 $1/m$로서 유지된다. 이는 접근구조를 고려하지 않고 m값을 작게 하여 $\alpha(m)$의 값을 크게 한 것으로 복원되는 비밀 정보는 하나이다. 그러나, 제안 방법은 $\binom{n}{2}$의 모든 조합의 접근 구조를 고려하여 복원 정보의 차별화와 휘도의 향상을 도모하였다. 〈표2〉에 제안 방식의 휘도를 나타내며, 그림1은 PASG, GASG 및 SASG에 따른 $(2,n)$VCS의 구성에 따라 시뮬레이션 한 결과이다.

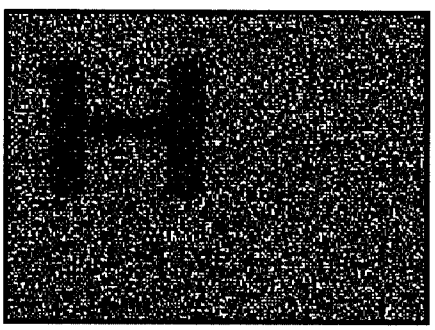
〈표 2〉 제안방법 I 에 의한 휘도

〈Table 2〉 Contrast by the proposed method I

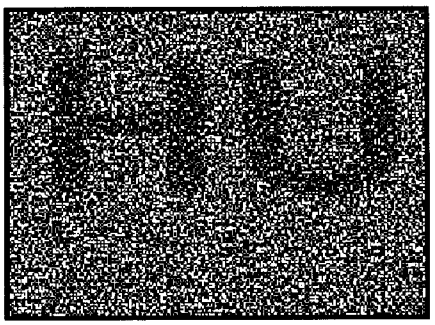
n		8	10	12	14	16	18	20	접근 구조
m		6	8	10	12	14	16	18	
$\alpha(m)\cdot m$	$\Gamma_2(w)$ $\Gamma_5(w)$	1	2	3	4	5	6	7	GASG
	$\Gamma_3(w)$ $\Gamma_4(w)$	1	1	1	1	1	1	1	SASG



(a) PASG 그룹



(b) GASG 그룹, $\alpha(12)=3/10$



(c) SASG 그룹, $\alpha(12) = 1/10$

[그림1] 접근구조에 따른 복원화상
[Fig.1] Reconstructed image according to access structures

4. 휘도의 개선

3장에서 제안한 행렬 구성법은 m의 크기가 커져도 SASG의 경우 휘도가 증가하지 않는 단점이 있다. 만약 시각암호에서 비밀의 복원 형태가 반전되는 경우도 성공적 복원으로 간주하면 휘도를 향상시킬 수 있는 새로운 모델을 위한 행렬(NM: New Matrix)을 구성할 수 있다.

[정의3] 각 기본그룹에 대하여 $n \times m$ 부울 행렬 C^0와 C^1의 다중 집합에서 임의의 한 기본 행렬M^0 와 M^1은 $\alpha(m)$과 $\{\text{stack}_i\}_{i\in\{\Gamma_i(w)\}}$가 다음 조건을 만족하면 $\Gamma_i(w), m\ \rangle$ VCS를 구성할 수 있다. 또한, 1차 식별 그룹 AU_1, 2차 식별 그룹 AU_2로 이루어지는 $\langle AU_1, AU_2, m\rangle$ VCS를 구성할 수 있다.

(1) 각 그룹의 두 행의 "or"된 벡터 V에 대하여
  (1.1) $M^0 \in C^0$ 에서 $w(V) \le \text{stack}_i - \alpha(m)\cdot m$, $M^1 \in C^1$에서 $w(V) = \text{stack}_i$ 또는
  (1.2) $M^0 \in C^0$ 에서 $w(V) \ge \text{stack}_i$, $M^1 \in C^1$ 에서 $w(V) \le \text{stack}_i + \alpha(m)\cdot m$

(2) 각 그룹에 대하여, 흑과 백의 화소를 구분할 수 없는 상태, 즉, M^0 와 M^1에서 두 행의"or"된 벡터 V의 해밍 가중치 $w(M_i^0) = w(M_i^1)$이어야 한다.

(1)은 흑과 백을 구별할 수 있는 휘도를 의미하고 반전의 형태도 의미 있는 복원정보로 간주한다. (2)는 흑과 백의 해밍 가중치가 같으므로 의미 있는 정보를 복원 할 수 없음을 나타낸다. 또한, (1)의 조건을 만족하나 (2)의 조건을 만족하지 않는 경우는 (1)과 (2) 모두를 만족하는 경우에 비하여 복원할 수 있는 정보가 많아진다.

4.1 행렬 구성

행렬 NM은 원소가 모두 1로 이루어진 크기 $(h-1)\times 1$의 행렬 $\tilde{F}$와 그 보수 행렬 $\tilde{F}^c$에 기초한다. $\tilde{F}\circ\tilde{F}^c$를 전치 시킨 행렬$(\tilde{F}\circ\tilde{F}^c)^T$와 행렬$(\tilde{F}^c\circ\tilde{F})^T$를 연결한 크기 $2\times 2(h-1)$인 행렬을 B라 한다. RM^*, $\tilde{RM}^*$의 크기가 $n\times(n-2)$이므로 B를 같은 크기로 확대하려면 행방향으

로 h번 반복하여 크기 $n\times(n-4)$ 크기의 행렬 $\tilde{B}$를 생성한다. 여기에 열의 원소가 모두 1 또는 0인 열을 각각 $\tilde{B}$에 연결하면 크기 $n\times(n-2)$인 행렬NM을 구성할 수 있다.

[예제 4] $n=12$일 때

$$NM=\begin{pmatrix}1111100000\\0000111110\\1111100000\\0000111110\\1111100000\\0000111110\\1111100000\\0000111110\\1111100000\\0000111110\\1111100000\\0000111110\end{pmatrix}$$

여기서, 행렬 $\tilde{RM}^*$, NM 및 RM^*는 정의3을 만족하도록 흑과 백 행렬로 구분된다.

4.2 휘도의 분석

가상그룹 $\Gamma_i(w)$를 NM에 적용하면 해밍 가중치가 $m-1$과 $m/2$인 두 가지만 나타난다. RM^*, $\tilde{RM}^*$에 적용하면 최대 해밍 가중치는 m-1이며, 최소 해밍 가중치는 $m/2$이다. 따라서, NM, $\tilde{RM}^*$ 상의 최소(최대) 해밍 가중치와 RM^*상의 최대(최소) 해밍 가중치의 차가 가장 크기 때문에 실제 복원화상의 휘도도 커진다.

흑의 화소를 위하여 행렬 NM과 $\tilde{RM}^*$에서 기본행렬 M^1, 백의 화소를 위하여 RM^*에서 기본행렬 M^0로 된다. $m = n-2$이고 모든 행의 해밍 가중치가 $m/2$인 $n\times m$ 행렬 M^1과 M^0에 대하여 VM상의 가상그룹 $\Gamma_i(w)$를 각 행렬에 적용시키면 〈표3〉과 같은 해밍 가중치를 얻는다.

〈표 3〉 가상그룹을 적용시 해밍 가중치

〈Table 1〉 Hamming weight as applying VG to each matrix

해밍 가중치 / 가상그룹	$w(M^1)=v_1$		$w(M^0)=v_0$
	NM	$\tilde{RM}^*$	RM^*
$\Gamma_1(w)$	$m-1$	$\frac{m}{2}$	$\frac{m}{2}$
$\Gamma_2(w)$	$\frac{m}{2}$	$\frac{m}{2}+1$	$m-1$
$\Gamma_3(w)$	$m-1$	$\frac{m}{2}+2$	$\frac{m}{2}+2$
$\Gamma_4(w)$	$\frac{m}{2}$	$\frac{m}{2}+2$	$\frac{m}{2}+2$
$\Gamma_5(w)$	$m-1$	$\frac{m}{2}+1$	$m-1$

NM 과 RM^*에서 $g=1, 2, 3, 4$에 대하여, $w(M_g^1[i]\ or\ M_g^1[j]) \neq w(M_g^0[i]\ or\ M_g^0[j])$, $\tilde{RM}^*$과 RM^*에서 $g=2, 5$에 대하여, $w(M_g^1[i]\ or\ M_g^1[j]) \neq w(M_g^0[i]\ or\ M_g^0[j])$이므로 흑의 화소를 위한 행렬($NM$, $\tilde{RM}^*$)에 따라 차등적으로 정보를 복원할 수 있다. 즉, NM과 RM^*, $\tilde{RM}^*$와 RM^*에서 해밍 가중치가 같지 않으면 비밀을 복원할 수 있음을 나타낸다. 휘도는 $\alpha(m)\cdot m = v_1-v_0$이므로 각 가상그룹의 휘도는 〈표4〉와 같으며, 음수는 반전된 형태로 복원됨을 의미한다.

〈표 4〉 가상그룹의 휘도

〈Table 4〉 Contrast of Virtual Group

해밍 가중치의 차 / 가상그룹	$w(NM)-w(RM^*)$	$w(\tilde{RM}^*)-w(RM^*)$
$\Gamma_1(w)$	$\frac{m}{2}-1$	0
$\Gamma_2(w)$	$-(\frac{m}{2}-1)$	$-(\frac{m}{2}-2)$
$\Gamma_3(w)$	$\frac{m}{2}-3$	0
$\Gamma_4(w)$	-3	0
$\Gamma_5(w)$	0	$-(\frac{m}{2}-1)$

이 결과, m값의 변동에 따른 휘도의 변화는 〈표5〉와 같게 된다.

〈표 5〉 제안방법 II에 의한 휘도의 변화

〈Table 5〉 Contrast by the proposed method II

n		8	10	12	14	16	18	20
m		6	8	10	12	14	16	18
$\alpha(m)\cdot m$	$\Gamma_1(w)$	2	3	4	5	6	7	8
	$\Gamma_2(w)$	-2, -1	-3, -2	-4, -3	-5, -4	-6, -5	-7, -6	-8, -7
	$\Gamma_3(w)$	0	1	2	3	4	5	6
	$\Gamma_4(w)$	-2	-2	-2	-2	-2	-2	-2
	$\Gamma_5(w)$	-1	-2	-3	-4	-5	-6	-7

5. 시각암호의 2단계 식별에 응용

앞장에서 구성된 각 행렬(VM, RM^* $\tilde{RM}^*$ NM)상에서 $\{i, j\} \in \Gamma_{ps}$ 의 쌍은 아래와 같이 이루어진다. VM 의 경우, i와 j행은 서로 보수가 되고, NM의 경우는 "or"연산하여 해밍 가중치가 m-1이 되는 i와 j가 선택된다. 또한 RM^*, $\tilde{RM}^*$ 의 경우는 "or" 연산하여 해밍 가중치가 $m/2$ 이 되는 i와 j가 선택된다. 행렬 VM에서 해밍 가중치에 따라 그룹 $\Gamma_i(w)$를 분류하고, NM, RM^* 및 $\tilde{RM}^*$ 에서 $\binom{n}{2}$의 모든 조합에 대하여 $\Gamma_i(w)$의 쌍들을 적용하면 그룹 i는 바뀌지만 그룹을 형성하는 요소는 같다. 즉, 동일한 해밍 가중치별로 분류되는 성질은 변하지 않는다. RM^*와 $\tilde{RM}^*$ 에서 서로 보수가 되는 한 쌍$\{i, j\}$를 제외하고는 같은 행에서의 패턴은 동일하다. 이때 패턴이 다른 쌍을 비동치 쌍이라고 하자.

4장에서 제안된 $(2,n)$ VCS를 식별에 적용하기 위하여 Γ_{ps} 에 기초하여 시스템이 가져야 할 1차 식별용의 $\Gamma_{system1}$, 2차 식별용의 $\Gamma_{system2}$와 사용자에게 분배되는 슬라이드 Γ_{user}는 식(5)와 같은 관계를 가진다.

$\Gamma_{system2}$ = 비동치 쌍의 원소 $\{i,j\} \subseteq \Gamma_{pg}$,

$\Gamma_{user} = P \setminus \Gamma_{system2} = \Gamma_{system1}$, $\Gamma_{user} = n-2$. (5)

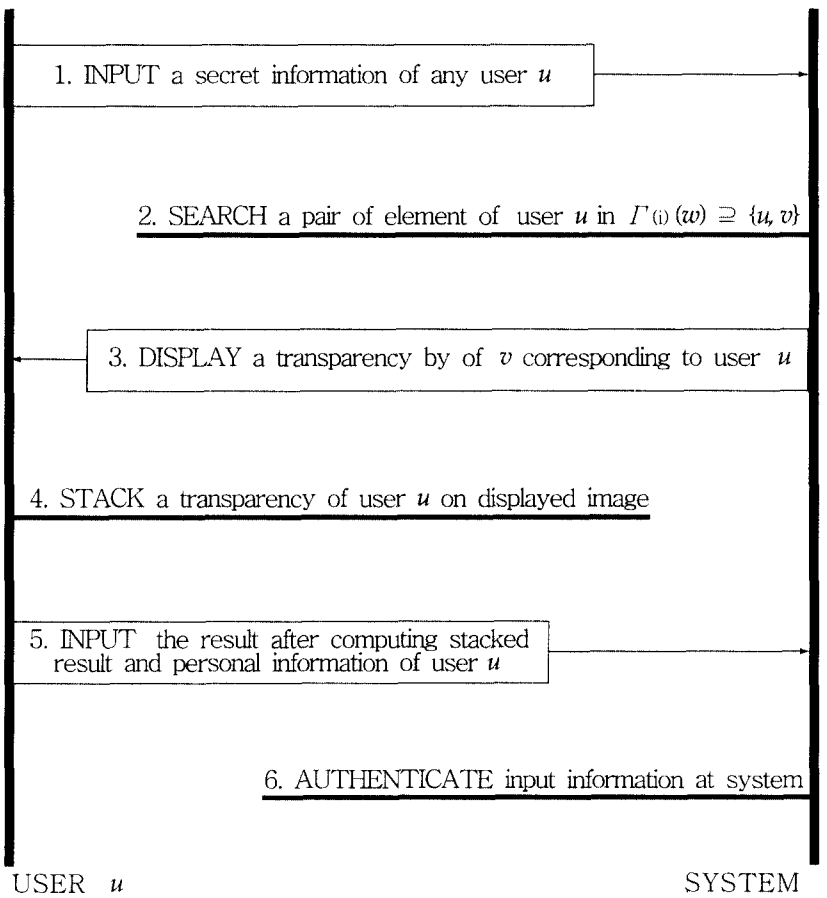
〈표4〉의 결과에 따라 $\Gamma_1(w)$, $\Gamma_3(w)$, $\Gamma_4(w)$, 및 $\Gamma_5(w)$ 는 하나의 정보를 복원할 수 있는 그룹이고, $\Gamma_2(w)$ 는 두 가지의 정보를 복원할 수 있는 그룹으로 된다. 이와 같은 정보 복원의 차등화를 이용하여 2단계 식별에 응용하는 메카니즘을 다음에 보인다.

5.1 식별 메카니즘

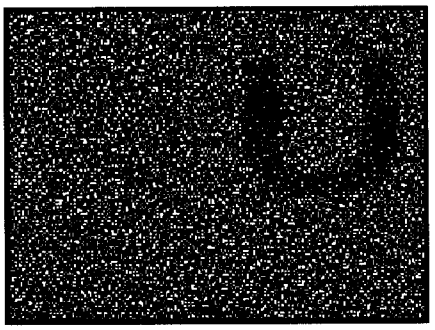
1차 식별을 위하여 그룹 $\Gamma_1(w)$, $\Gamma_3(w)$ 및 $\Gamma_4(w)$ 가 2차 식별을 위하여 그룹$\Gamma_2(w)$, 가 이용될 수 있다. 여기서는 그룹 $\Gamma_1(w)$가 $\Gamma_3(w)$와 $\Gamma_4(w)$보다 큰 휘도를 얻을 수 있으므로 $\Gamma_1(w)$를 1차 식별용으로 사용하기로 한다. 식(5)로부터 그룹 $\Gamma_5(w)$는 $\Gamma_{system2}$의 슬라이드가 사용자들에게 분배되지 않으므로 1차 식별을 위한 조합을 구성할 수 없다. 다음은 $(2,n)$ VCS에서 한 장의 슬라이드를 사용하여 2단계 식별을 할 수 있는 메카니즘을 나타낸다.

1차 식별은 사용자 슬라이드 Γ_{user}와 슬라이드 $\Gamma_{system1}$의 중첩으로 나타난 메시지와 사용자 개인 정보와의 약정된 연산 결과를 입력하는

[메카니즘1] 1차 식별 절차



대화형 접근법을 취한다. 1차 식별을 위한 시뮬레이션의 결과를 다음에 나타낸다. 그림 2는 사용자의 슬라이드를 디스플레이 화면에 중첩할 때 복원되는 정보이다.

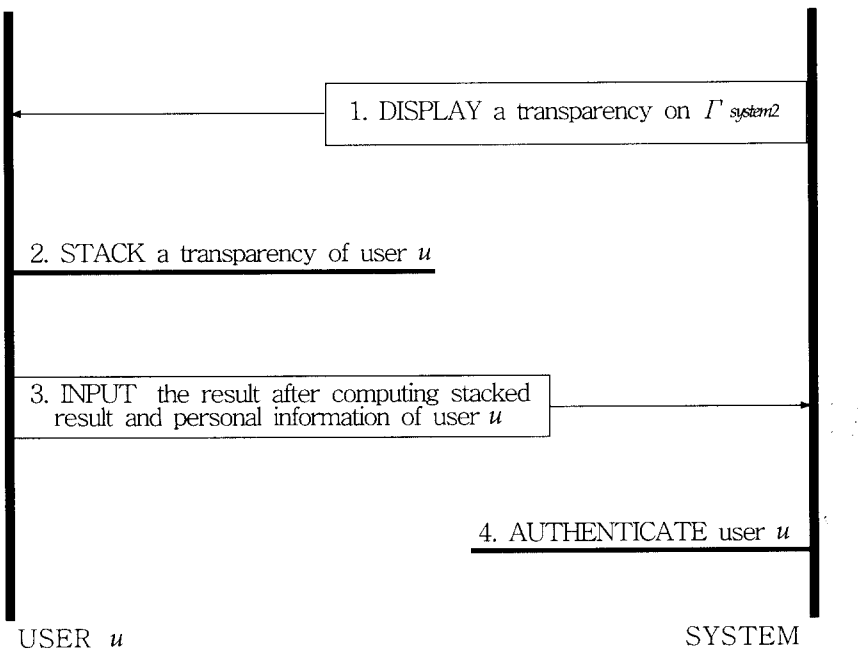


[그림2] 1차 식별을 위한 복원화상
[Fig.2] Reconstructed image for the first identification

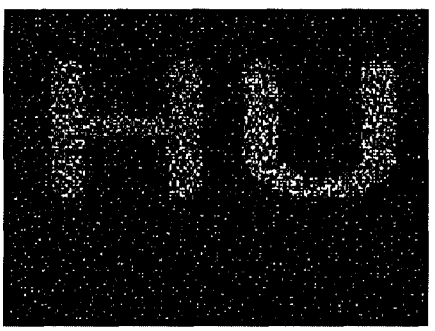
따라서, 2차 식별을 위하여 디스플레이 되는 화면에 사용자의 슬라이드를 중첩하여 나타나는 메시지와 사용자 개인 정보와의 약정된 연산 결과를 입력함으로서 상호 식별 할 수 있다. 그러

1차 식별 절차가 끝난 후 단말은 2차 식별을 위하여 사용자 u에 대한 2차 식별용 슬라이드를 디스플레이 한다. 2차 식별을 위한 메카니즘은 다음과 같다.

[메카니즘2] 2차 식별 절차



나, 위조 시스템인 경우는 시스템 자체가 2차 식별을 할 수 있는 $\Gamma_{system2}$의 슬라이드가 없으므로 시스템이 사용자를 그리고 사용자가 시스템을 식별을 할 수 없게 된다. 즉, 1차 식별에서 사용하는 시스템 슬라이드 $\Gamma_{system1}$은 사용자에게도 분배되므로 위조 시스템에 적용하여 1차 식별은 가능하지만, 2차 식별을 위한 그룹 $\Gamma_{system2}$의 슬라이드는 사용자에게 분배되지 않고 시스템만이 가지고 있으므로 2차 식별을 할 수 없다. 임의의 슬라이드를 2차 식별용 디스플레이 화상으로 사용하여도 사용자 슬라이드와 중첩하여 나타난 정보가 의미가 없을 수도 있고, 의미가 있다하더라도 1차 식별시의 복원화상이 나타나지 않기 때문에 사용자도 시스템이 위조인지를 식별을 할 수 있다. 그림3은 2차식별을 위한 복원화상이다.



[그림3] 2차 식별을 위한 복원화상
[Fig.3] Reconstructed image for the second identification

6. 결 론

본 논문에서는 비밀 분산법의 한 형태인 VCS에서 비밀을 계층적 접근구조에 따라 단계적으로 복원 할 수 있는 구성법을 제안하였다. 제안하는 행렬 구성법에서 휘도가 일정한 값을 유지하는 문제점이 있으므로 복원 형태가 반전되는 경우도 성공적으로 간주한 새로운 행렬 구성법을 사용하여 휘도를 개선하는 방법을 제시하였다. 또한, 개선된 행렬 구성법을 사용한 $(2,n)$ VCS를 대화형 개인 식별에 적용하여 한 장의 슬라이드로 2단계 식별을 가능하게 하는 메카니즘을 제안하였다. 향후 연구는 $k\geq 3$에 대하여 그룹 분류 방법의 제안과 복원 가능한 비밀의 수를 확장하는 행렬 구성법의 고안이다.

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, A.Shamir, "Visual Cryptography", Advanced in Cryptology Eurocrypt' 94, pp.1-12, 1994

[3] T.Katoh, H. Imai, "A Study on Visual Multi-secret Threshold Scheme", Proc. of SCIS '96, 6D, 1996 (in Japanese)

[4] G. Ateniese, C. Blundo, A. De Santis

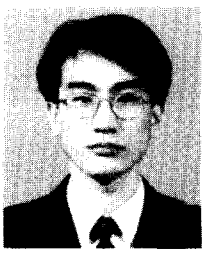
and D. R.. Stinson."Visual Cryptography for General Access Structures", Information and Computation 129, pp.86-106, 1996

[5] 최창근, 박지환, "시각암호의 접근구조에 따른 비밀정보의 계층적 접근과 contrast의 분석", 한국정보처리학회 춘계학술발표대회, 4권 1호, pp.1032-1037, 1997.4

[6] T. Matsumoto, H. Imai, "Human Identification Through Insecure Channel", Advanced in Cryptology-Eurocrypt' 91, pp.409~421, Apr 1991

[7] T. Katoh, H. Imai, "A Human Identification Scheme Against Peeping Attacks Based on Visual Secret Sharing Scheme", Proc. of SCIS' 97, 25C, Feb. 1996. (in Japanese)

□ 著者紹介



최 창 근

1996년 2월: 부산수산대학교 전자계산학과 (이학사)
1998년 2월: 부경대학교 전자계산학과 석사과정 졸업(이학석사)
1998년 4월-현재: 요코하마국립대학 전자정보공학과 박사과정 재학

※ 주관심분야 : 암호학 응용, 비밀 분산법, 이동통신

박 지 환

1984년 2월: 경희대학교 전자공학과 졸업(공학사)
1987년 3월: 전기통신대학 정보공학과 졸업(공학석사)
1990년 3월: 요코하마국립대학 전자정보공학과 졸업(공학박사)
1990년~1996년: 부산수산대학교 전자계산학과 전강, 조교수, 부교수
1994년~1995년: 동경대학 생산기술연구소 객원 연구원
1998년 1월~2월: 전기통신대학 정보시스템학 연구과 방문연구
1996년 4월~현재: 동경대학 생산기술연구소 협력 연구원
1996년 7월~현재: 부경대학교 전자계산학과 부교수

※ 주관심분야 : 멀터미디어 압축, 암호학 응용, 오류제어 부호, 화상처리 등