論文 98-23-6-16

시각암호에 의한 개인 인증 방식

준회원 김 미 라* 정회원 박 지 환*

A Human Identification Scheme Using Visual Cryptography

Mi-Ra Kim*, Ji-Hwan Park* *Regular Members*

※본 논문은 과학재단의 핵심전문 연구과제(과제번호 971-0905-030-1) 연구비에 의해 연구되었음.

요 약

본 논문에서는 복잡한 암호학적 연산없이 숨겨진 화상을 복원할 수 있는 시각암호를 이용한 개인 인증 방식에 대하여 고찰한다. Katoh와 Imai는 1개의 표시화상에 인증을 위한 2개의 질문 화상을 숨길 수 있는 방식을 제안하였다. 이 방식을 확장시켜 복수개의 질문화상을 숨길 수 있는 일반화 구성법을 제시한다. 나아가, Droste방식을 적용시켜 모든 슬라이드의 조합에 따라 서로 다른 비밀화상을 숨길 수 있는 방식을 제안한다.

ABSTRACT

In this paper, we investigate a human identification scheme using visual cryptography, which can decode concealed images without any cryptographic computations. T.Katoh & H.Imai proposed a secret sharing scheme which can conceal two query images into one displayed image for the identification. The generalized construction of the share matrix is proposed to conceal the multiple query images by stacking user slides on the displayed image. Furthermore, an extended method is proposed in which group of slides can conceal an independent secret image as well as the pairs of slides can.

Ⅰ. 서 론

정보통신의 발달로 인하여 각종 전자 상거래(electronic commerce)와 정보 서비스 제공의 기회가 급증하고 있는 가운데 서비스를 제공받고자 하는 사용자가 정당한지를 확인하는 방법이 요구 된다. 이를 위하여 정당한 사용자임을 확인할 수 있는 여러 가지 개인 인증 방식이 연구되어 오고 있다. 현재 가장 널리 사용되고 있는 패스워드 방식은 사용자와 단말기 사이에 미리 비밀 정보(패스워드)를 설정해 두고 입력된 패스워드가 정당한 사용자의 것인지를 검사하는 방식으로 구성이 간단하고 사용자가 손쉽게 이용할 수 있는 장점이 있다. 그러나, 도청이나 엿보기 공격(peeping attack)에 약하다는 등이 많은 문제점을 노출시키고 있다. 이러한 문제점을 극복하기 위하여 고안된 대화형 개인 인증 방식[1]은 미리 사용자와 단말기 사이에 비밀정보를 정하여 패스워드 방식을 수행하지만, 단말기로부터 제시된 질문에 대하여 사용자는 비밀정보를 이용하여 간단한 연산을 한 후, 그 결과를

* 부경대학교 전자계산학과
論文番號:97264-0731
接受日字:1997年 7月 31日

입력하여 정당성을 대화적으로 검증하는 방식이다. 이 방식은 외부 기록매체나 복잡한 계산을 수반하지 않으며, 비밀정보가 부분적으로 누설되어도 단순 패스워드 방식에 비하여 엿보기 공격에 강한 특징을 갖는다. 여러 가지 형태의 엿보기 공격에 대한 안전성은 균등 사상을 이용한 이론적 해석이 이루어져 있다[2].

T.Katoh와 H.Imai는 대화형 개인 인증 방식에 있어서 단말기로부터 사용자에게 제시되는 질문을 시각암호[3]에 의해 생성되는 슬라이드를 이용하는 방식을 제안하였다[4]. 이 방식은 사용자에게 미리 약속된 슬라이드가 배포되어 있으며, 인증 하고자 할 때 단말기의 화면상에 표시되는 질문용 슬라이드와 사용자 슬라이드를 겹침으로서 나타나는 메시지를 읽어 들여 인증을 하기 때문에 사용자가 이용하려는 단말기 자체가 위조 단말인지를 패스워드를 입력하기 전에 알아 낼 수 있는 이점을 갖는다. 또한, 사용자에게 복수개의 슬라이드를 배포하여 겹치는 슬라이드에 따라 다른 서비스를 받을 수도 있다. 즉, 1장의 표시화상에 대하여 어떤 슬라이드를 겹치느냐에 따라 질문화상이 다르게 나타나는 방식이다. 이를 위한 슬라이드의 구성은 복원화상의 해상도를 높이기 위하여 share크기를 작게 하여야 하며, 슬라이드의 모든 조합에 대하여 질문화상을 형성할 수 있는 것이 바람직하다.

본 논문에서는 1개의 표시화상에 2개의 질문화상을 숨길 수 있는 Katoh & Imai 방식의 구성법을 복수개 숨길 수 있도록 일반화하고, Droste 방식[5]을 적용시켜 개인 인증에 응용할 수 있는 새로운 방식을 제안한다. 2장에서는 M.Naor & A.Shamir에 의해 제안된 시각암호의 기본 모델을 소개하고, 3장에서는 시각암호를 개인 인증 방식에 응용하는 Katoh & Imai에 의해 제안된 방식을 알아본 후, 1개의 표시화상에 복수개의 질문화상을 숨길 수 있는 일반화 구성법을 제시한다. 나아가, 그 확장으로서 모든 사용자 슬라이드를 표시화상에 겹쳤을 때도 또 다른 질문화상이 나타나도록 Droste 방식에 기초한 새로운 구성법을 제안한다. 마지막으로 4장에서는 결론 및 향후 연구과제를 도출한다.

Ⅱ. 시각암호의 기본 모델

시각암호에 의한 비밀 분산 문제의 가장 간단한 형태는 흑화소와 백화소로 구성된 비밀화상에 적용하는 것이다. 이때, 각 화소는 따로 조작될 수 있다고 가정한다. 비밀화상의 각 화소는 n장의 슬라이드에 각각 m개의 부분화소로 분산되며, 이것을 share라 부른다. 따라서, 비밀화상의 한 화소는 m배 확대되어 n장으로 분산된다.

이 구조는 비밀화상의 각 화소가 $n \times m$부울 행렬 $S = [s_{ij}]$로 표현될 수 있으며, 이때 s_{ij}의 값은 i번째 share 중 j번째 부분화소가 흑인 경우에 1을, 백인 경우에 0을 나타낸다. Share들을 정확하게 일치하도록 겹쳤을 때, 행렬 S의 행들의 논리 "or"로 표현되는 결합 share를 시각적으로 인식할 수 있다. 이 결합 share의 계조(grey level)는 "or"연산을 한 m차 벡터 V의 해밍 가중치 $H(V)$에 비례하며, 어떤 고정된 문턱치 $1 \le d \le m$와 상대적인 차 $\alpha > 0$에 대해서 $H(V) \ge d$이면 흑으로, $H(V) \le d - \alpha m$이면 백으로 인식된다.

◆정의 (k, n) 시각 비밀 분산법은 $n \times m$ 부울 행렬들의 두 집합 C_0, C_1으로 구성된다. 백 화소를 분산하기 위하여 C_0의 행렬들 중 임의로 하나를 선택하고, 흑화소를 분산하기 위하여 C_1의 행렬들 중 임의로 하나를 선택한다. 선택된 행렬의 각 행은 한 개의 share에 대응하고, 행의 각 요소가 1이면 흑을, 0이면 백을 나타낸다. 다음 세 가지 조건을 만족하면 (k, n) 시각 비밀 분산법의 해가 유효하게 된다.

(1) C_0의 임의의 S에 대하여, n행중 임의의 k행의 "or" 연산을 한 m차 벡터 V의 해밍 가중치는 $H(V) \le d - \alpha m$을 만족한다.

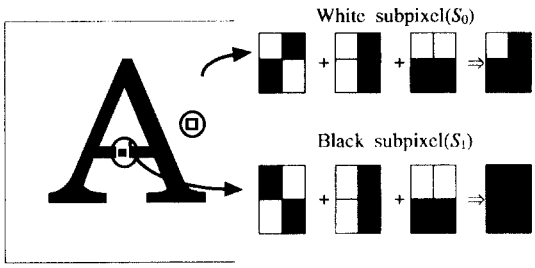
(2) C_1의 임의의 S에 대하여, n행중 임의의 k행의 "or" 연산을 한 m차 벡터 V의 해밍 가중치는 $H(V) \ge d$를 만족한다.

(3) $q < k$인 $\{1, 2, \cdots, n\}$의 임의의 부분집합 $\{i_1, i_2, \cdots, i_q\}$에 대하여, $C_t\,(t \in \{0, 1\})$의 각 $n \times m$ 행렬을 행 $i_1, i_2, \cdots, i_q$로 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 화상의 휘도(contrast)를 나타내고, 조건3은 k장 미만의 share를 겹쳤을 때 분산된 화소가 흑인지 백인지를 구분할 수

없는 안전성(security)을 나타낸다. 그림 1에 $(3,3)$ 시각 비밀 분산법의 일 예를 나타낸다. 이때, 문턱치 d와 상대적인 차 α는 각각 4와 1/4이 된다.

$$S_0=\begin{pmatrix}0110\\0101\\0011\end{pmatrix},\quad S_1=\begin{pmatrix}1001\\0101\\0011\end{pmatrix}$$



(a)원화상 (b)화소의 분산

그림 1. (3, 3)시각 비밀 분산법
Fig. 1 Visual (3, 3) secret sharing scheme

Ⅲ. 시각암호를 이용한 개인 인증 방식

대화형 개인 인증 방식[1]은 사용자가 단말기에 패스워드와 같은 비밀정보를 직접 입력하는 것이 아니라, 단말기와 공유하는 비밀정보를 이용하여 단말기가 제시한 질문에 대한 해답을 입력한다. 이 방식은 비밀정보를 직접 입력하는 것이 아니기 때문에 엿보기 공격에 강한 장점을 갖는다. 시각암호를 개인 인증에 응용한 방식으로 1개의 표시화상에 2개의 질문화상을 숨길 수 있는 방식이 Katoh & Imai에 의해 제안되었다[4]. 즉, 사용자는 제공받고자 하는 서비스에 따라 미리 배포된 슬라이드 중 어느 것을 표시화상에 겹치는가에 따라 다른 질문화상이 나타나는 방식이다. 이 방식의 특징은 단말기가 사용자를 인증할 뿐만 아니라 사용자도 단말기가 정당한지를 인증할 수 있게 된다. 대화형 인증을 위한 절차의 개요를 아래에 간략히 나타낸다.

[인증 절차]

1. 사용자와 단말기는 식별정보(ID)와 비밀정보를 공유하고, 사용자는 각각의 슬라이드를 배포 받는다. 이때 슬라이드는 시각 복호형 $(2,2)$비밀 분산법에서 생성된 share 생성 행렬로 구성된다.
2. 서비스를 이용하기 위하여 사용자는 자신의 식별정보를 입력한다.
3. 단말기는 식별정보에 대응한 사용자 슬라이드를 겹침으로써 어떤 메시지가 나타나도록 화면에 표시화상을 제시한다.
4. 사용자는 미리 배포된 슬라이드를 표시화상에 겹쳐 복원되는 메시지와 자신의 비밀정보를 이용하여 약정된 간단한 연산을 수행한 결과를 응답으로써 입력한다.

따라서, 시각암호에 의한 비밀 분산법을 이용한 개인 인증은 슬라이드만으로 사용자와 단말기를 상호 인증 할 수 있게 된다.

3.1 일반화 구성법

여기서는 Katoh & Imai 방식을 확장시켜 1개의 표시화상에 복수개의 질문화상을 숨길 수 있는 일반화 구성을 제시한다. 먼저, 사용자 슬라이드를 생성하기 위한 share 생성 행렬은 다음과 같이 얻어진다.

- I: $n\times n$의 단위 행렬
- Z: $n\times n$의 영행렬(모든 요소가 0인 행렬)
- IZ: I와 Z의 연결, $n\times 2n$의 사용자 share 생성 행렬
- C:행렬 IZ의 열을 교환하여 만든 사용자 share 생성 행렬의 집합

예를 들어, $n=3$의 경우 사용자 share 생성 행렬의 집합 C는

$$C=\left\{\begin{pmatrix}100000\\010000\\001000\end{pmatrix}\text{의 열을 교환하여 만든 모든 행렬}\right\}$$

로 된다. 사용자 슬라이드를 구성하기 위하여 share 생성 행렬의 집합 C에서 임의의 한 행렬을 선택한다. 첫번째 행은 사용자 슬라이드1, 두번째 행은 사용자 슬라이드2, 그리고 세번째 행은 사용자 슬라이드3을 위하여 이용된다.

단말기의 화면에 제시될 표시화상용 슬라이드를 생성하기 위하여 사용자 share 생성 행렬 IZ를 단위

행렬 I 부분과 영행렬 Z 부분으로 나누어 고려한다. 단위 행렬 I 부분은 질문화상의 화소값이 백(W)이면 그 질문화상에 대응하는 행벡터들을 논리 "or"하고, 모두 흑(B)인 경우만 논리 "and" 연산한다. 예를 들어, 질문화상1, 질문화상2와 질문화상3의 화소값이 모두 백(WWW)이면 I의 1행, 2행 및 3행의 행벡터를 논리 "or"한 (111)을 얻게 된다. 한편, 영행렬 Z 부분은 질문화상의 화소값 조합에서 흑의 화소값의 개수 B_k만큼 "0"을 "1"로 바꾼다. 따라서, n C_{B_k}개의 경우의 수가 존재한다. $n=3$일 때의 표시화상을 위한 행벡터의 구성 예를 표 1에, 사용자 share와 표시화상이 겹쳐지는 모습을 그림 2에 나타낸다. 즉, 3가지 질문화상의 화소값 조합에 따라 표 1에서 구해진 표시화상용 행렬을 이용하여 질문 화상의 각 화소(B/W)를 복원 하는 과정을 나타낸다. C의 각 행에 해당하는 사용자 share들과 화소값 조합이 BWB일 때의 표시화상용 행렬(010011)을 겹치면 복원 화상의 화소가 BWB로 인식됨을 나타내고 있다. 사용자 슬라이드 3장을 번갈아 표시화상에 겹치면 3가지 질문화상이 차례로 복원되며, 백으로 인식되는 share의 해밍 가중치는 그림 2에서 처럼 3으로, 흑으로 인식되는 share의 해밍 가중치는 4로 된다. 즉, 복원된 질문화상에서 백으로 인식되는 share의 해밍 가중치는 n, 흑으로 인식되는 share의 해밍 가중치는 $n+1$이고 흑과 백의 상대적인 차 α는 $1/2n$으로 된다. 또한, share의 크기를 나타내는 m은 질문화상의 수 n의 2배로 된다.

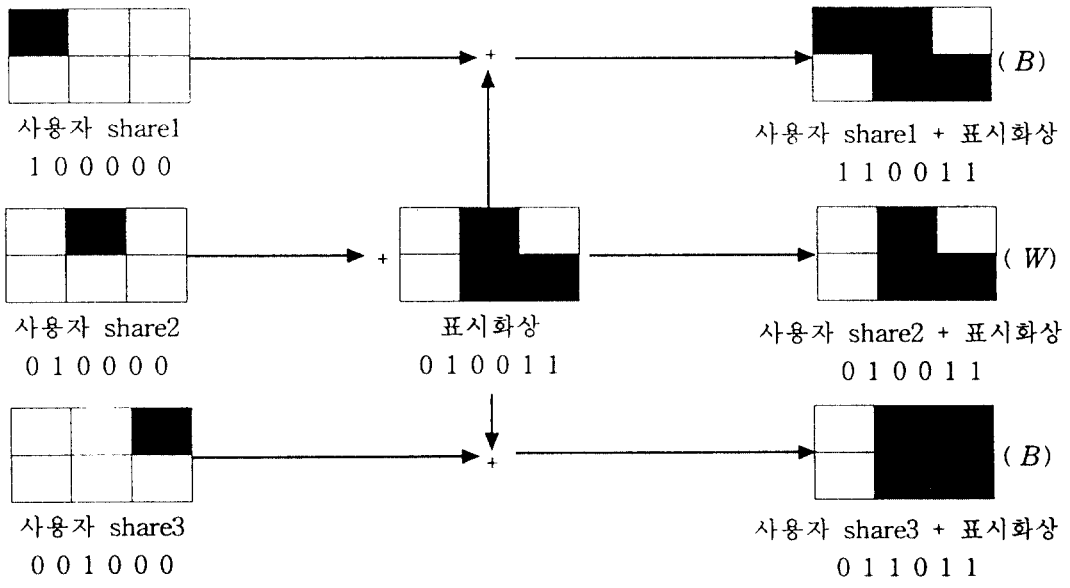


그림 2. 사용자 share와 표시화상이 겹쳐지는 모습
Fig. 2 Stacking the user share on the displayed image

표 1. 표시화상을 위한 행벡터(n=3)
Table 1. Row vectors for the display image

화소값 조합			표시화상용 행렬	
질문화상1	질문화상2	질문화상3	단위행렬(I)	영행렬(Z)
W	W	W	1 1 1	0 0 0
W	W	B	1 1 0	1 0 0 (0 1 0, 0 0 1)
W	B	W	1 0 1	1 0 0 (0 1 0, 0 0 1)
W	B	B	1 0 0	1 1 0 (1 0 1, 0 1 1)
B	W	W	0 1 1	0 0 1 (0 1 0, 1 0 0)
B	W	B	0 1 0	0 1 1 (1 0 1, 1 1 0)
B	B	W	0 0 1	0 1 1 (1 0 1, 1 1 0)
B	B	B	0 0 0	1 1 1

3.2 Droste 방식

슬라이드의 조합에 따라 복원되는 정보가 달라지는 구성법이 S.Droste에 의해서 제안되었다[5]. 예를 들어, 2장의 슬라이드 1과 2의 조합이 {{1}, {2}, {1,2}}인 경우 각 슬라이드가 서로 다른 정보를 포함하고 있을 뿐만 아니라, 슬라이드 1, 2를 겹쳐도 또 다른 정보가 복원되는 방식이다.

먼저, Droste 방식의 Share 생성 행렬 B^T을 구성하기 위해서 아래의 기호들의 정의한다.

- P:슬라이드의 집합, $P=\{1,2,\cdots,n\}$
- S: P의 공집합이 아닌 부분집합으로 비밀화상을 복원할 수 있는 조합을 그 원소로 가진다.
  즉, $\{i_1,\cdots,i_q\}\in S$일 때 슬라이드 $i_1,\cdots,i_q$를 겹치면 비밀화상이 복원 가능하며, $S\subseteq P(\{1,\cdots,n\})/\{0\}$로 나타낸다.
- T: S의 부분집합($T\subseteq S$); S에 의해서 복원되는 비밀화상의 화소값 조합으로서 $2^{|S|}$종류가 존재하며, $\{i_1,\cdots,i_q\}\in S$에 대해서, $\{i_1,\cdots,i_q\}\in T$일 때 $i_1,\cdots,i_q$에 대응하는 슬라이드를 겹치면 흑, $\{i_1,\cdots,i_q\}\notin T$일 때는 백을 나타낸다.
- $B(T,(i_1,\cdots,i_q)):=\begin{cases} B_0(i_1,\cdots,i_q), & \text{if } \{i_1,\cdots,i_q\}\notin T \\ B_1(i_1,\cdots,i_q), & \text{if } \{i_1,\cdots,i_q\}\in T \end{cases}$

  $\{i_1,\cdots,i_q\}\in S$와 $t\in\{0,1\}$에 대해서, $B_t(i_1,\cdots,i_q)$는 $i_1,\cdots,i_q$에 대응하는 행이 (q,q) 시각 비밀 분산법으로 구성된 share 생성 행렬로 채워지고, 나머지 $n-q$행은 모두 1로 채워지는 $n\times 2^{q-1}$ 크기의 행렬이다.
- B^T:행렬 $B(T,\{i_1,\cdots,i_q\})$의 연결이다.

예를 들어, $P=\{1,2,3\}$일 때 비밀화상을 복원할 수 있는 조합 $S=\{\{1\},\{2,3\},\{1,2,3\}\}$을 임의로 정하면, S는 슬라이드 1만으로, 슬라이드 2와 3을 겹쳤을 때 그리고 슬라이드 1, 2, 3을 모두 겹쳤을 때의 3가지 비밀화상을 복원할 수 있게 된다. 2^3=8가지의 화소값 조합을 나타내는 S의 부분집합 T에 따라 구성되는 share 생성 행렬 B^T는 다음과 같이 구해진다.

$T=\{\{\}\}$일 때 S의 모든 원소가 T의 원소가 아니므로 행렬 $B^{\{\}}$는 $B_0^{\{1\}}$, $B_0^{\{2,3\}}$ 그리고 $B_0^{\{1,2,3\}}$의 연결이다. $B_0^{\{1\}}$은 3행 $2^{1-1}=1$열중 제1행만 0이고 나머지 행들은 모두 1로 구성되고, $B_0^{\{2,3\}}$는 3행 $2^{2-1}=2$열 중 제2행과 제3행만 (2,2)시각 비밀 분산법으로 구성된 행렬로 채워지고 나머지 제1행은 모두 1로 채워진다. $B_0^{\{1,2,3\}}$은 3행 $2^{3-1}=4$열 모두 (3,3)시각 비밀 분산법으로 구성된 행렬로 채워진다. 나머지 부분집합 T에 대해서도 동일한 방법으로 B^T행렬을 구성하면

$$B^{\{\}}=\begin{pmatrix}0|11|0011\\1|01|0101\\1|01|0110\end{pmatrix}$$

$$B^{\{\{1\}\}}=\begin{pmatrix}1|11|0011\\1|01|0101\\1|01|0110\end{pmatrix}$$

$$B^{\{\{2,3\}\}}=\begin{pmatrix}0|11|0011\\1|01|0101\\1|10|0110\end{pmatrix}$$

$$B^{\{\{1,2,3\}\}}=\begin{pmatrix}0|11|1100\\1|01|1010\\1|01|1001\end{pmatrix}$$

$$B^{\{\{1\},\{2,3\}\}}=\begin{pmatrix}1|11|0011\\1|01|0101\\1|10|0110\end{pmatrix}$$

$$B^{\{\{1\},\{1,2,3\}\}} = \begin{pmatrix} 1|11|1100 \\ 1|01|1010 \\ 1|01|1001 \end{pmatrix}$$

$$B^{\{\{2,3\},\{1,2,3\}\}} = \begin{pmatrix} 0|11|1100 \\ 1|01|1010 \\ 1|10|1001 \end{pmatrix}$$

$$B^{\{\{1\},\{2,3\},\{1,2,3\}\}} = \begin{pmatrix} 1|11|1100 \\ 1|01|1010 \\ 1|10|1001 \end{pmatrix}$$

로 된다. 부분집합 T에 S의 원소들이 포함되는 경우와 그렇지 않은 경우에 따라 슬라이드 1장, 2장, 3장을 겹쳤을 때의 해밍 가중치는 각각 4와 5, 5와 6 그리고 6과 7로 되어 흑과 백을 인식할 수 있다.

3.3 개인 인증을 위한 Droste 방식의 확장

Katoh & Imai 방식은 사용자 슬라이드 중 어떤 1장의 슬라이드를 표시화상에 겹치느냐에 따라 다른 질문화상이 복원되지만, 사용자 슬라이드 모두를 표시화상에 겹치면 1장씩 겹쳤을 때 복원된 모든 질문화상이 함께 겹쳐진 형태로 나타난다. 이러한 문제점을 해결하기 위하여 3.2절의 Droste 방식[5]을 변형하여 사용자 슬라이드 모두를 표시화상에 겹쳤을 때 또 다른 질문화상이 복원될 수 있는 구성법을 제안한다. 즉, 사용자 슬라이드 중 1장을 표시화상에 겹쳤을 때 서로 다른 질문화상이 복원될 뿐만 아니라 사용자 슬라이드 모두를 표시화상에 겹쳤을 때에도 또 다른 질문화상이 복원될 수 있는 방식이다.

n개의 질문화상을 1개의 표시화상에 숨기기 위한 사용자 share 생성 행렬의 집합 C를 구성하기 위하여 행렬그룹 Ⅰ과 Ⅱ를 정의한다.

◆행렬그룹Ⅰ

- G_{n-1}(Ⅰ): $M_{n-1,i}$의 연결에 의한 행렬, $0 \le i \le n-1$
- $M_{n-1,i}$: $n-1$개의 행을 가지며, i개의 1을 갖는 열을 모두 취한 행렬

예를 들어, $n=3$일 때

$$G_2(\text{Ⅰ}) = \begin{pmatrix} 0011 \\ 0101 \end{pmatrix}.$$

◆행렬그룹Ⅱ

- G_{n-1}(Ⅱ): $M_{n-1,i}$행렬 중에서 $n-2$개의 1을 갖는 모든 열에 모두 1인 열을 ${}_{n-1}C_{n-2}$회 반복하여 연결한 행렬

예를 들어, $n=3$일 때

$$G_2(\text{Ⅱ}) = \begin{pmatrix} 0111 \\ 1011 \end{pmatrix}.$$

사용자 share 생성 행렬의 집합 C는 G_{n-1}(Ⅰ)과 G_{n-1}(Ⅱ)의 연결에 의해

$$C = \left\{ \begin{pmatrix} 00110111 \\ 01011011 \end{pmatrix} \text{의 열을 교환하여 만든 모든 행렬} \right\}$$

로 되며, 3.1절과 동일한 방법으로 사용자 슬라이드를 구성하게 된다.

표시화상을 구성하기 위하여 행렬그룹Ⅰ의 모든 열은 사용자 슬라이드를 모두 겹쳤을 때 나타나는 질문화상1에, 행렬그룹Ⅱ의 각 열은 사용자 슬라이드 각각을 겹쳤을 때 나타나는 질문화상2와 3에 각각 교대로 대응토록 한다. 각 질문화상의 화소값에 따라 백(W)의 경우에는 질문화상에 대응하는 열의 1의 개수가 짝수가 되도록, 흑(B)의 경우에는 열의 1의 개수가 홀수가 되도록 "0"과 "1"을 선택한다. $n=3$일 때의 표시화상을 생성하기 위한 행벡터의 구성 예를 표 2에 나타낸다.

만약, 질문화상1, 2, 3에 대한 화소값 조합 $Q=$

표 2. 제안방식의 표시화상을 위한 행벡터(n=3)
Table 2. Row vectors of the proposed scheme

화소값 조합			표시화상용 행벡터	
			행렬그룹Ⅰ	행렬그룹Ⅱ
질문화상1	질문화상2	질문화상3	0 0 1 1 0 1 0 1	0 1 1 1 1 0 1 1
W	W	W	0 1 1 0	1 1 0 0
W	W	B	0 1 1 0	1 0 0 1
W	B	W	0 1 1 0	0 1 1 0
W	B	B	0 1 1 0	0 0 1 1
B	W	W	1 0 0 1	1 1 0 0
B	W	B	1 0 0 1	1 0 0 1
B	B	W	1 0 0 1	0 1 1 0
B	B	B	1 0 0 1	0 0 1 1

$q_1q_2q_3 = WBW$일 때 표시화상용 행벡터는 "01100110"로 되어 C의 첫번째 행벡터인 "00110111"과의 논리 "or"는 "01110111"이 되며, 두번째 행벡터와의 논리 "or"는 "01111111"로 된다. 따라서, 해밍 가중치가 6인 경우는 "B"로, 7인 경우는 "W"로 되어 반전된 형태로 복원된다. 한편, 모든 슬라이드를 표시화상에 겹치기 위한 C의 모든 행벡터와 "01100110"의 논리 "or"는 "01111111"로 되어, $q_1 = W$일 때는 해밍 가중치가 7, $q_1 = B$일 때는 8로 되므로 흑과 백 화소를 구별할 수 있게 된다.

1장의 사용자 슬라이드와 표시화상을 겹쳤을 때(질문화상2와 3이 생성됨), 백으로 인식되는 share의 해밍 가중치는 $2^{n-1}+2n-3$이고, 흑으로 인식되는 share의 해밍 가중치는 $2^{n-1}+2n-4$로 된다. 또한, 모든 사용자 슬라이드를 표시화상에 겹쳤을 때(질문화상1이 생성됨) 백으로 인식되는 share의 해밍 가중치는 $2^{n-1}+2n-3$이고, 흑으로 인식되는 share의 해밍 가중치는 $2^{n-1}+2n-2$로 된다. 그림 3에 $n=3$

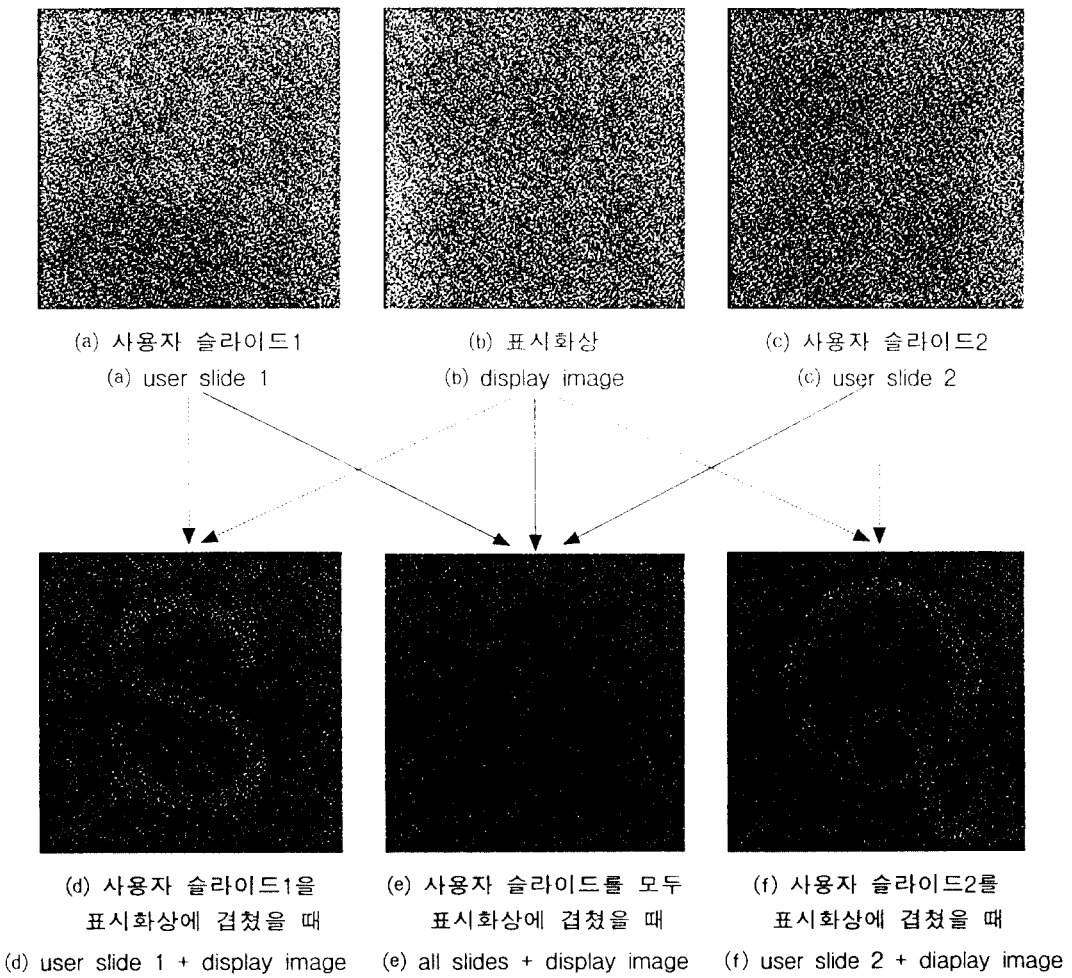


그림 3. 표시화상에 사용자 슬라이드를 모두 겹쳤을 때도 다른 질문화상이 복원되는 제안방식
Fig. 3 Decryption of secret images in the proposed method

일 때의 제안방식을 시뮬레이션한 결과를 나타낸다. (b)의 표시화상에 각 사용자 슬라이드(a)와 (c)를 겹친 (d)와 (f)의 경우는 백의 해밍 가중치가 흑의 해밍 가중치보다 크기 때문에 반전된 형태로 복원된다. 한편, 모든 사용자 슬라이드를 표시화상에 겹친 (e)의 경우는 또 다른 비밀정보를 복원할 수 있는 이점을 가지게 된다.

모든 사용자 슬라이드를 표시화상에 겹쳤을 때 또 다른 질문화상을 나타낼 수 있는 제안방식은 질문화상의 수가 늘어나면 Katoh & Imai의 방식에 비해 share 크기가 표 3과 같이 증가하지만, 질문화상의 수가 많지 않은 실제의 응용에서는 그다지 문제가 되지 않는다.

표 3. 질문화상의 수에 따른 share 크기 변화
Table 3. Share size according to the number of query image

질문 화상수	share 크기	
	Katoh & Imai 방식	제안방식
3	6	8
4	8	14
5	10	24
⋮	⋮	⋮
n	$2n$	$2^{n-1}+2(n-1)$

Ⅳ. 결 론

Naor & Shamir의 시각암호와 Katoh & Imai에 의해 제안된 시각암호를 이용한 개인 인증 방식에 대하여 고찰하였다. 본 논문에서는 시각암호의 개인 인증 방식에의 응용에서 1개의 표시화상에 복수의 질문화상을 숨길 수 있는 일반화 구성법을 제시하였다. 또한, Droste 방식을 변형하여 사용자 슬라이드를 모두 표시화상에 겹쳤을 때도 다른 질문화상이 복원될 수 있는 새로운 방식을 제안하였다. 향후의 과제는 제안방식을 실제의 정보보호 시스템에 적용하기 위한 구현과 인증에 있어서의 다양한 공격에 대한 안전성을 검토할 예정이다.

참 고 문 헌

1. T.Matsumoto, H.Imai, "Human Identification Through Insecure Channel," Advanced in Cryptology-EUROCRYPT'91, pp.409-421, 1991.
2. K.Kobara, H.Imai, "On the Properties of the Security Against Peeping Attacks on Challenge-Response Type Direct Human Identification Scheme Using Uniform Mapping," IEICE Trans., Vol.J79-A, No.8, pp.1352-1359, Aug., 1996(in Japanese).
3. M.Naor and A.Shamir, "Visual Cryptography," Advances in Cryptology-EUROCRYPT'94, pp.1-12, May 1994.
4. T.Katoh and H.Imai, "An Application of Visual Secret Sharing Scheme Concealing Plural Secret Images to Human Identification Scheme," Proc. of SITA'96, pp.661-664, December 1996.(in Japanese)
5. S.Droste, "New Results on Visual Cryptography," Advanced in Cryptology-CRYPTO'96, pp.401-415, Aug. 1996.

김 미 라(Mi-Ra Kim) 준회원
1996년:부산수산대학교 전자계산학과 졸업(이학사)
1998년:부경대학교 전자계산학과 졸업(이학석사)
※주관심분야:정보이론, 암호학 응용 등

박 지 환(Ji-Hwan Park) 정회원
1984년:경희대학교 전자공학과 졸업(공학사)
1987년:日本國立電氣通信大學 情報工學科(工學修士)
1990년:日本橫浜國立大學 電子情報工學科(工學博士)
1990년~1996년:부산수산대학교 전자계산학과 전강, 조교수, 부교수
1994년~1995년:日本東京大學生産技術研究所 客員研究員
1996년~현재:日本東京大學生産技術研究所 協力研究員
현재:부경대학교 전자계산학과 부교수
주관심분야:멀티미디어 압축, 암호학 응용, 오류제어 부호, 화상처리 등
e-mail:jhpark@dolphin.pknu.ac.kr