通信情報保護學會論文誌
第 7 卷 第 4 號, 1997. 12

시각암호에 의한 비밀 분산법

김 미 라*, 박 지 환*, 박 상 우**, 김 광 조**

Secret Sharing Scheme Using Visual Cryptography

Mi-Ra Kim*, Ji-Hwan Park*, Sang-Woo Park**, Kwang-Jo Kim**

요 약

시각암호는 기존의 비밀 분산법이 비밀을 분산/복호시의 방대한 연산량을 수반하는 것과는 달리 인간의 시각에 의해 직접 복호되기 때문에 복잡한 연산이 필요 없는 방식이다. 본 논문에서는 중첩하는 슬라이드의 매수에 따라 복수의 비밀화상이 복원되는 시각암호에 대해 알아보고, 그 안전성을 검증한다. 분산하고자 하는 비밀화상의 수가 증가함에 따라 share 크기가 기하 급수적으로 커지기 때문에 복원화상의 인식이 어렵게 된다. 따라서, 고정 가중치 부호의 해밍 거리를 조정하여 줄임으로써 복원화상의 해상도를 개선하는 방법을 제안한다.

Abstract

A secret sharing scheme is required a vast computation when share or decode a secret information, whereas the visual cryptography scheme has no need of complex computation because of directly decodable by the human visual system. In this paper, we investigate the visual cryptography scheme which can decode the multiple secret images according as the number of stacked slides and verify its security. It is hard to recognize the decoded image, because of the share size increase exponentially when the number of secret image increase. In order to overcome, we propose a method that can improve the resolution of decoded secret image by reducing the share size using constant weight code.

1. 서 론

중요한 정보를 안전하게 관리하기 위해서 정보를 여러 개로 분산하여 임의의 개수 이상이 결합되면 비밀정보에 접근할 수 있지만, 그 미만이 결합되면 결코 비밀정보에 접근할 수 없는 비밀 관리 체계인 (k, n)문턱치 비밀 분산법이 A.Shamir에 의해 제안[1]된 이후, 비밀

* 부경대학교 전자계산학과
** 한국전자통신연구원

정보로서 화상을 이용하여 복잡한 암호학적 연산 없이도 비밀을 복원할 수 있는 시각암호가 M.Naor & A.Shamir에 의해 제안되었다[2]. 이 방식에 의해 분산된 비밀화상은 슬라이드와 같은 물리적 중첩이 가능한 곳에 인쇄되는 경우를 가정한다. (k, n)비밀 분산법에서처럼 그룹 내 n명에게 배포된 슬라이드 중 임의의 k명 이상의 슬라이드를 겹치면 비밀화상을 복원할 수 있지만, k-1명 이하의 슬라이드를 겹치는 경우에는 비밀화상을 복원할 수 없어 안전성이 유지된다.

시각암호의 확장 방식으로서 겹친 슬라이드의 매수에 따라 서로 다른 비밀화상을 복원할 수 있는 복수 화상용 시각암호가 T.Katoh & H.Imai에 의해서 제안되었다[3,4]. 그러나, Katoh & Imai의 복수 화상용 시각암호는 비밀화상의 수가 증가할수록 share 크기가 기하급수적으로 커져 복원된 비밀화상의 인식이 어렵다는 문제점을 가지고 있다.

본 논문에서는 이러한 문제점을 해결하기 위하여 고정 가중치 부호[5]를 이용하여 share 크기를 줄이는 방식을 제안하고, 비밀화상들 사이에서 시각적 안전성은 보장되지만 첫번째 비밀화상을 복원한 사용자의 결탁공격에 대한 안전성은 보장되지 않는다는 것을 보인다. 2장에서는 M.Naor & A.Shamir에 의해 제안된 시각암호의 개념을 소개하고, 3장에서는 T.Katoh & H.Imai에 의해 제안된 복수 화상용 시각암호와 그 안전성을 검증하며, 4장에서는 두 개의 비밀화상을 세 장의 슬라이드에 분산시킬 때 고정 가중치 부호의 해밍거리를 조정하여 share 크기를 줄이는 방식을 제안한 후, 그 성능을 컴퓨터 시뮬레이션을 통하여 평가한다. 마지막으로 5장에서는 결론 및 향후 연구과제를 도출한다.

2. Naor & Shamir의 시각암호

2.1 기본 모델

시각암호에 의한 비밀 분산 문제의 가장 간단한 형태는 흑과 백의 화소(pixel)로 구성된 이진화상(binary image)에 적용하는 것이다. 이때, 각 화소는 따로 조작될 수 있다고 가정한다. 비밀화상의 각 화소는 n장의 슬라이드에 각각 m개의 부화소(subpixel)로 분산되며, 이것을 share라 부른다.

이 구조는 비밀화상의 각 화소가 $n \times m$ 부울행렬 $S = [s_{ij}]$ 로 표현될 수 있으며, 이때 s_{ij}의 값은 i번째 share 중 j번째 부화소가 흑인 경우에 1을, 백인 경우에 0을 나타낸다.

Share들을 정확하게 일치하도록 겹쳤을 때, 행렬 S의 행들의 불리언 "or"로 표현되는 결합 share를 볼 수 있다. 결합 share의 grey단계는 "or"연산을 한 m차 벡터 V의 해밍 가중치 $H(V)$에 비례한다. 이 grey단계는 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 $n \times m$부울행렬들의 두 집합 C_0, C_1으로 구성된다. 백의 화소를 분산하기 위해서 C_0의 행렬 중 하나를 임의로 선택하고, 흑의 화소를 분산하기 위해서 C_1의 행렬 중 하나를 임의로 선택한다. 선택된 행렬의 각 행은 한 개의 share에 대응하고 행의 각 요소가 1이면 흑을, 0이면 백을 나타낸다. 아래의 세 가지 조건을 만족하면 (k, n)시각 비밀 분산법의 해가 유효하게 된다.

1. C_0의 임의의 S에 대해서, n행 중 임의의 k행의 "or" 연산을 한 m차 벡터 V의 해밍 가중치는 $H(V) \leq d - \alpha m$을 만족한다.
2. C_1의 임의의 S에 대해서, n행 중 임의의 k행의 "or" 연산을 한 m차 벡터 V의 해밍 가중치는 $H(V) \geq d$를 만족한다.
3. $q < k$인 $\{1, 2, \cdot, n\}$의 임의의 부분집합 $\{i_1, i_2, \cdot, i_q\}$에 대해서, $C_t(t \in \{0, 1\})$의 각 $n \times m$행렬을 $i_1, i_2, \cdot, i_q$행으로 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 화상에서의 휘도(contrast)를 나타내고, 조건3은 k장 미만의 share를 겹쳤을 때 분산된 화소가 흑인지 백인지를 구분할 수 없는 안전성(security)을 나타낸다. 시각 비밀 분산법에 사용되는 파라미터들은 다음과 같다.

- m : share를 구성하는 화소의 수를 나타내며, 원화상과 분산된 화상과의 해상도 손실에 영향을 미치므로 가능한 한 작아야 한다.
- α : 원화상의 백과 흑의 화소로부터 생성된 결합 share들간의 가중치의 상대적인 차로서 휘도의 손실을 나타내므로 가능한 한 커야 한다.
- r : 집합 C_0, C_1의 크기이며, $\log r$은 share들을 나타내기 위해 필요한 임의의 비트 수로 화질에는 영향을 주지 않는다.

2.2 (k, k)시각 비밀 분산법

(k, k)시각 비밀 분산법을 구성하기 위하여 k개의 원소를 갖는 전체 집합 $W = \{e_1, e_2, \cdot, e_k\}$와 원소의 개수가 짝수인 부분집합 리스트 $\pi_1, \pi_2, \cdot, \pi_{2^{k-1}}$, 원소의 개수가 홀수인 부분집합 리스트 $\sigma_1, \sigma_2, \cdot, \sigma_{2^{k-1}}$을 고려하자.

$1 \leq i \leq k$와 $1 \leq j \leq 2^{k-1}$에 대하여, S_0와 S_1은 $e_i \in \pi_j$일 때 $S_0[i, j] = 1$, $e_i \in \sigma_j$일 때 $S_1[i, j] = 1$로 정의되는 $k \times 2^{k-1}$행렬이다. C_0와 C_1은 S_0와 S_1의 열들을 교환해서 만든 행렬의 집합을 나타낸다.

$C_0 = \{S_0$의 열들을 교환해서 만든 모든 행렬들$\}$
$C_1 = \{S_1$의 열들을 교환해서 만든 모든 행렬들$\}$

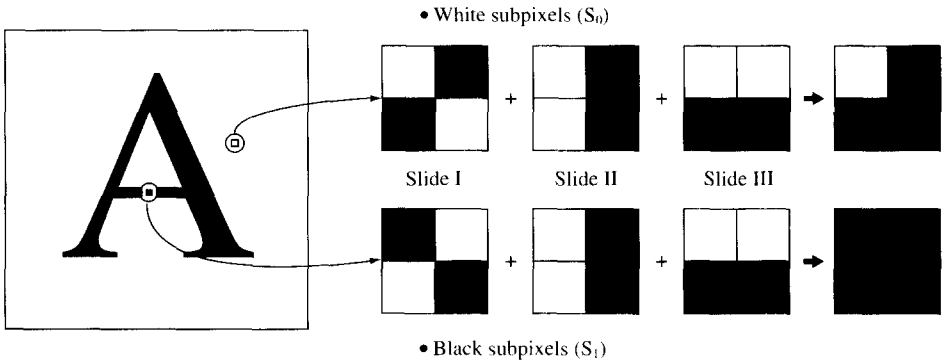
그리고, (k, k)시각 비밀 분산법은 $m = 2^{k-1}$, $\alpha = \frac{1}{2^{k-1}}$, $r = 2^{k-1}!$을 갖는다. 예를 들어, $k = 3$일 때

$W = \{e_1, e_2, e_3\}$
$\pi_1 = \{\ \}$, $\pi_2 = \{e_1, e_2\}$, $\pi_3 = \{e_1, e_3\}$, $\pi_4 = \{e_2, e_3\}$
$\sigma_1 = \{e_1\}$, $\sigma_2 = \{e_2\}$, $\sigma_3 = \{e_3\}$, $\sigma_4 = \{e_1, e_2, e_3\}$

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

로 된다. 따라서, $S_0[S_1]$의 한 행으로 이루어지는 백[흑]의 화소는 k행 겹쳤을 때 $\frac{1}{2^{k-1}}$만큼 휘도 차가 나지만, k행 미만일 때는 해밍 가중치가 같아 흑과 백을 구별할 수 없으므로 안전성이 보장된다. 즉, 그림1은 (3, 3) 비밀 분산법의 일 예이며, 원화상의 백[흑]의 화소는 행렬 $S_0[S_1]$의 각 행에 대응하는 부화소(subpixel)로 각각의 슬라이드에 분산된다. 복원시 문턱치인 $k = 3$장을 중첩하면 흑화소의 경우는 완전히 검게되고, 백화소의 경우는 3/4만큼 검게되어 $\alpha = \frac{1}{4}$을 유지하여 시각적으로 흑과 백을 구별할 수 있게 된다.

행렬	모두 0인 열의 수	k-1 행의 "or"	k 행의 "or"
S_0	1	$(2^{k-1}-1)$개의 1	$(2^{k-1}-1)$개의 1
S_1	0	$(2^{k-1}-1)$개의 1	$2^{k-1}-1$개의 1



〈그림1〉 화소의 분산

3. Katoh & Imai의 시각암호

3.1 구성법

비밀화상의 각 화소를 n개의 share로 분산하기 위하여 n개의 행과 i(i = 0, 1, · · · , n)개의 1을 갖는 열로 구성되는 $n \times {}_nC_i$행렬 $M_{n,i}$를 고려한다. 이때, 1의 수가 짝수인 열로 구성된 $M_{n,i}$을 연결시킨 행렬 S_0가 백화소를 표현하는 share 생성 행렬이고, 1의 수가 홀수인 열로 구성된 행렬을 연결시킨 행렬 S_1이 흑화소를 표현하는 share 생성 행렬이다. 예를 들어, n = 3의 경우

$$M_{3,0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \; M_{3,1} = \begin{pmatrix} 100 \\ 010 \\ 001 \end{pmatrix},$$

$$M_{3,2} = \begin{pmatrix} 011 \\ 101 \\ 110 \end{pmatrix}, \; M_{3,3} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$S_0 = M_{3,0}M_{3,2} = \begin{pmatrix} 0011 \\ 0101 \\ 0110 \end{pmatrix},$$

$$S_1 = M_{3,1}M_{3,3} = \begin{pmatrix} 1001 \\ 0101 \\ 0011 \end{pmatrix}$$

로 된다.

이 행렬에 의해서 생성된 share를 한 개씩 겹쳤을 때 share에 포함된 흑화소의 수는 표1과 같다. 실제로 행렬 S_0, S_1 각각의 열 교환으로 만들어진 모든 행렬의 집합 C_0, C_1을 이용하여 (n, n)시각 비밀 분산법을 구성하게 된다.

3.2 복수화상용 비밀 분산법

Naor & Shamir 방식은 하나의 비밀화상을 n장의 슬라이드에 분산하고, 정해진 매수 이상의 슬라이드를 겹치기만 하면 한 개의 비밀화상이 복원되는 방식이었다. 이 절에서는 이 방식을 확장하여 두 개 이상의 비밀화상을 분산

〈표1〉 겹친 share의 개수와 흑화소의 수

	1매	2매	3매		1매	2매	3매
$M_{3,0}$	0	0	0				
$M_{3,1}$	1	2	3	S_0	2	3	3
$M_{3,2}$	2	3	3	S_1	2	3	4
$M_{3,3}$	1	1	1				

시키는 Katoh & Imai 방식에 대하여 검토한다. 예를 들면, 세 장의 슬라이드에 두 개의 비밀화상을 분산할 때 각 슬라이드는 랜덤한 화상으로 보이지만, 임의의 두 장을 겹치면 첫번째 비밀화상이, 세 장 모두 겹치면 두번째 비밀화상이 복원되는 방식이다. 이때, 첫번째 비밀화상이 복원되는 단계에서는 두번째 비밀화상을, 두번째 비밀화상이 복원되는 단계에서는 첫번째 비밀화상을 추정할 수 없으므로 시각적 안전성은 보장된다.

3.1절에서 제시된 S_0, S_1의 행렬을 구성하기 위하여 행렬 $M_{3,j}$에서 생성된 각각의 share를 겹쳤을 때, 겹친 개수에 대응하는 흑화소 수의 천이를 열 벡터로 하는 행렬 T_3을 구한다. 단, 모든 요소가 0인 행렬 $M_{3,0}$은 흑화소 수의 천이에 영향을 미치지 않으므로 제거한다.

$$T_3 = \begin{matrix} M_{3,1} & M_{3,2} & M_{3,3} \\ \end{matrix}$$
$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 1 \\ 3 & 3 & 1 \end{pmatrix} \begin{matrix} 1\text{매} \\ 2\text{매} \\ 3\text{매} \end{matrix}$$

그리고, share 생성 행렬 S을 구성하기 위해서 필요한 행렬 $M_{3,j}(i = 1, 2, 3)$의 개수 x_i를 요소로 하는 벡터를 $X_3 = (x_1, x_2, x_3)^T$, 구성된 행렬에 의해서 생성된 share를 $j(j = 1, 2, 3)$개를 겹쳤을 때 share에 포함된 흑화소의 수 y_i를 요소로 하는 벡터를 $Y_3 = (y_1, y_2, y_3)^T$라 하면, T_3, X_3, Y_3는 다음과 같은 관계식

$$Y_3 = T_3 X_3 \quad (1)$$
$$X_3 = T_3^{-1} Y_3 \quad (2)$$

이 성립된다.

Share 생성 행렬을 구성하기 위해 필요한 흑화소 수의 천이의 상대적 오차를 구하기 위해서 벡터 Y_3을 화소값 조합에 따라 $Y_{WW} = (y_{ww1}, y_{ww2}, y_{ww3})^T$, $Y_{BW} = (y_{bw1}, y_{bw2}, y_{bw3})^T$, $Y_{WB} = (y_{wb1}, y_{wb2}, y_{wb3})^T$, $Y_{BB} = (y_{bb1}, y_{bb2}, y_{bb3})^T$로 나누면 표2와 같은 관계가 성립한다.

〈표2〉 겹친 share의 개수와 흑화소의 수

	1매	2매	3매
Y_{WW}	y_{ww1}	y_{ww2}	y_{ww3}
Y_{BW}	y_{wb1}	$y_{ww2}+1$	y_{ww3}
Y_{WB}	y_{wb1}	y_{ww2}	$y_{ww3}+1$
Y_{BB}	y_{ww1}	$y_{ww2}+1$	$y_{ww3}+1$

따라서, 화소값 조합에 따라 share 생성 행렬을 구성하기 위하여 필요한 행렬 $M_{3,i}$의 개수를 요소로 하는 벡터를 $X_{WW} = (x_{ww1}, x_{ww2}, x_{ww3})^T$, $X_{WB} = (x_{wb1}, x_{wb2}, x_{wb3})^T$, $X_{BW} = (x_{bw1}, x_{bw2}, x_{bw3})^T$, $X_{BB} = (x_{bb1}, x_{bb2}, x_{bb3})^T$라 할 때, 이 벡터들은 식(2)에 의해 m을 최소로 하는 X_{WW}, X_{WB}, X_{BW} 및 X_{BB}을 구할 수 있다.

벡터 X_{WW}, X_{WB}, X_{BW}, X_{BB}에 따라 share 생성 행렬을 구성했을 때, 백화소의 share 생성 행렬의 열의 수가 흑화소의 share 생성 행렬의 열의 수보다 적은 경우가 발생하면 행렬 $M_{3,0}$을 부족한 만큼 더하여 조절한다.

$$\begin{cases} X_{WW} = (1, 1, 3) \\ X_{BW} = (0, 3, 0) \\ X_{WB} = (2, 0, 4) \\ X_{BB} = (1, 2, 1) \end{cases}$$

$$S_{WW} = M_{3,0}M_{3,1}M_{3,2}M_{3,3}^4 = \begin{pmatrix} 01000011111 \\ 00101011111 \\ 00011101111 \end{pmatrix}$$

$$S_{BW} = M_{3,0}M_{3,2}^3 = \begin{pmatrix} 01101101100 \\ 01011011101 \\ 00110110111 \end{pmatrix}$$

$$S_{WB} = M_{3,1}^2M_{3,3}^4 = \begin{pmatrix} 10010011111 \\ 01001011111 \\ 00100111111 \end{pmatrix}$$

$$S_{BB} = M_{3,1}M_{3,2}^2M_{3,3} = \begin{pmatrix} 10011011011 \\ 01010110111 \\ 00101101111 \end{pmatrix}$$

단, $M_{n,i}^p$는 행렬 $M_{n,i}$의 p개의 연결을 나타낸다.

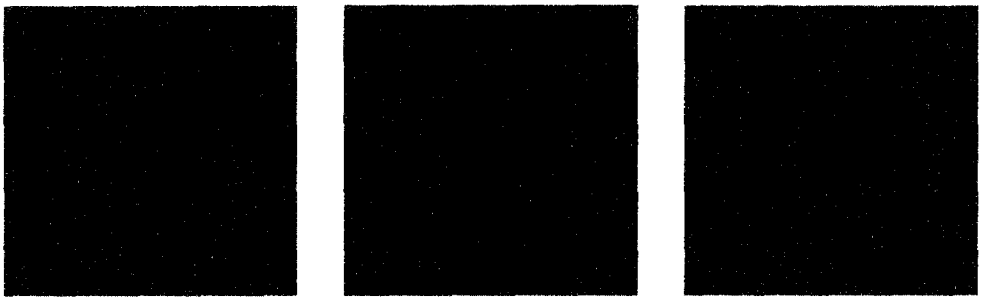
벡터 Y_c (c ∈ {WW, BW, WB, BB})는 식(2)에 대입하여 얻을 수 있는 벡터 X_i에 의해서 구성된 행렬 S_{WW}, S_{BW}, S_{WB}, S_{BB}에 대응한다. 따라서, X_{WW}는 share를 두 개 또는 세 개를 겹쳤을 때 모두 백화소를 생성하는 행렬 S_{WW}, X_{BW}는 share를 두 개 겹쳤을 때는 흑화소를 세 개를 겹쳤을 때는 백화소를 생성하는 행렬 S_{BW}, X_{WB}는 share를 두 개 겹쳤을 때는 백화소를 세 개 겹쳤을 때는 흑화소를 생성하는 행렬 S_{WB}, X_{BB}는 share를 두 개 또는 세 개 겹쳤을 때 모두 흑화소를 생성하는 행렬 S_{BB}을 각각 구성하기 위해 필요한 행렬 $M_{3,i}(i = 1, 2, 3)$의 개수를 요소로 갖는 벡터이다. 이 행렬에 의해서 생성된 share는 10개의 화소로 구성되지만, 종횡비를 맞추기 위해 각 share에 6개의 화소를 군더더기로 추가해야 한다. 단, 추가하는 화소의 색은 모든 share에서 동일해야하며, 흑/백의 제한은 없다.

그림2는 50 × 50화소로 구성되는 비밀화상 Ⅰ과 Ⅱ를 나타내고, 그림3은 Katoh & Imai에 의해 제안된 복수 화상용 시각암호로 구성된 share 생성 행렬에 '1'만 갖는 행렬을 6개 추가하여 종횡비를 맞추어 시뮬레이션한 결과이다. 각 슬라이드를 나타내는 (a), (b) 및 (c)는 그 내용을 알아 볼 수 없는 랜덤한 화상이다. 그러나, (d), (e)와 (f)는 임의의 두 장을 겹쳤을 때 첫번째 비밀화상을, (g)는 슬라이드 세 장을 모두 겹쳤을 때 두번째 비밀화상이 복원된 결과이다. 이때, 각 share는 가로와 세로 방향으로 각각 $\sqrt{m} = 4$배로 확대되어 각 슬라이드는 200 × 200화소의 크기로 된다. 또한, 첫번째 비밀화상과 두번째 비밀화상 사이에는 서로 시각적 추정이 불가능함을 알 수 있다.

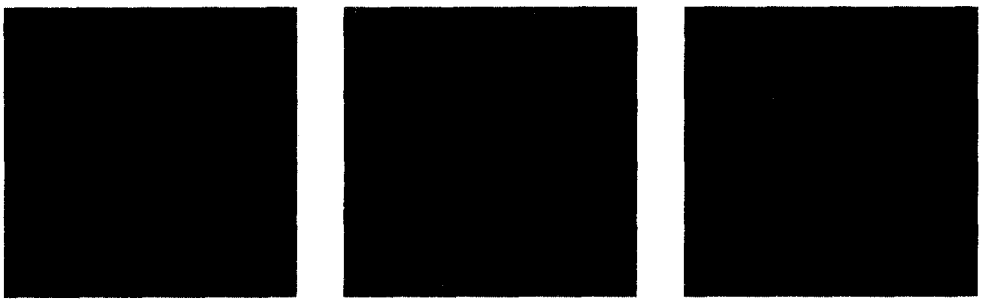
(a) 비밀화상 Ⅰ

(b) 비밀화상 Ⅱ

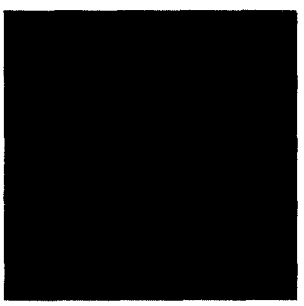
〈그림2〉 2개의 비밀화상



(a) 슬라이드 I (b) 슬라이드 II (c) 슬라이드 III



(d) 슬라이드 I 과 II 를 겹침 (e) 슬라이드 I 과 III 을 겹침 (f) 슬라이드 II 와 III 을 겹침



(g) 슬라이드 I, II, III 의 겹침

〈그림3〉 세 장의 슬라이드에 두 개의 비밀화상을 분산(Katoh & Imai 방식)

3.3 안전성 검증

Katoh & Imai의 복수 화상용 시각암호의 안전성을 검증한다. 그림3의 (a), (b) 및 (c)는 은닉된 정보가 무엇인지 전혀 알 수 없으며, 한 개의 비밀화상을 숨기는 방식과 동일한 안전성이 보장된다. 즉, 모든 share 생성 행렬의 각 행이 같은 해밍 가중치를 가지기 때문에 슬라이드 I, II 와 III 에 분산된 화소가 흑인지 백인지 구별할 수 없다. 따라서, 그림3의 (a), (b) 및 (c)에서는 비밀화상 I 과 비밀화상 II 를 모두 추정할 수 없다.

다음으로 복원된 비밀화상Ⅰ로부터 비밀화상Ⅱ에 대한 안전성을 검증하여 보자. 그림3의 (d), (e), (f) 및 (g)로부터 비밀화상Ⅰ과 비밀화상Ⅱ의 시각적 안전성이 보장된다는 것을 알 수 있다. 그러나, 만약 비밀화상Ⅰ을 복원할 수 있는 정당한 사용자 2명이 비밀화상Ⅱ를 복원하려고 결탁한다면 안전성은 보장될 수 없다. 즉, 결탁공격에 대한 안전성은 보장되지 않는다. 복원된 비밀화상에서 시각적으로 인식 가능한 흑과 백의 휘도비 α가 $1/36(=1/m)$정도로 제한되고, 비밀화상Ⅰ을 복원한 두 장의 슬라이드의 share의 흑화소의 수가 같기 때문에 share 크기 m을 간단하게 찾을 수 있다. 또한, m을 알면 복원된 비밀화상Ⅰ에서 흑화소 수의 천이의 상대적 오차도 구할 수 있으므로 $3 \times m$ share 생성 행렬의 3행 중 2행을 구성할 수 있다. 복원된 비밀화상Ⅰ에 겹쳤을 때 의미가 있는 정보가 나타나도록 흑화소 수의 천이의 상대적 오차를 1씩 증가시켜 가면서 나머지 행을 구성하면 된다.

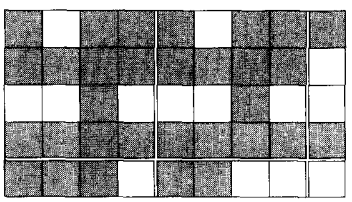
예를 들어, 정당한 사용자 A, B 그리고 C가 그림3의 슬라이드Ⅰ, Ⅱ, Ⅲ을 가지고 있으며, 첫번째 비밀화상을 복원할 수 있는 정당한 사용자 A와 B가 결탁하여 두번째 비밀화상을 복원하려 한다고 가정하자. 사용자 슬라이드는 share에서 같은 수의 흑화소를 가지므로 share 크기 m을 알아내기 위해서 4, 9, 16 · · · 로 증가시키면서 흑화소의 수를 비교한다. 그림4 (a)와 (b)에서 $m = 4$와 $m = 9$일 때 흑화소의 수는 다르지만, $m = 16$ 일 때 흑화소의 수는 12로 같으므로 share 크기 m은 16으로 결정된다.

그림4 (c)에서 복원된 첫번째 비밀화상의 백과 흑을 나타내는 흑화소의 수가 14와 15 이므로 두 행의 "or" 연산시 해밍 가중치가 14와 15로 되는 행렬을 다음과 같이 구하게 된다.

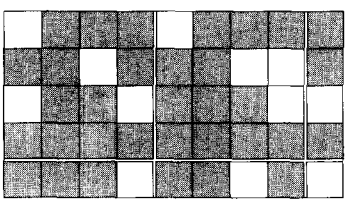
$$\begin{pmatrix} 1011111100101111 \\ 0111110101101111 \end{pmatrix}, H(V) = 14$$

$$\begin{pmatrix} 1011111100101111 \\ 0111110011101111 \end{pmatrix}, H(V) = 15$$

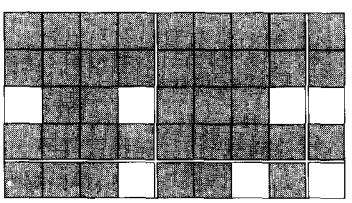
Share 크기 m, share를 구성하는 흑화소의 수와 흑과 백의 상대적 오차를 알 수 있으므로 두번째 비밀화상의 화소값에 따라 나머지 share 생성 행렬을 구할 수 있다. 따라서, 첫번째 비밀화상을 복원할 수 있는 두 장의 슬라이드로부터 두번째 비밀화상을 복원하는 것은 가능하게 된다.



(a) 그림3 (a)의 일부분 확대



(b) 그림3 (b)의 일부분 확대



(c) 그림3 (d)의 일부분 확대

〈그림4〉 그림3의 슬라이드를 일부 확대

4. 고정 가중치 부호에 의한 개선

4.1 Share 크기 축소

복수 화상을 숨기는 Katoh & Imai 방식의 경우 이론적으로는 많은 비밀화상을 분산시킬 수 있지만, 실제로 시각에 의해 인식 가능한 흑/백의 휘도비 α는 1/25에서 1/36정도로 제한되기 때문에 비밀화상의 수는 표3에서 알 수 있듯이 기껏해야 두 개 또는 세 개로 제한된다. 따라서, 더 많은 비밀화상을 분산시키기 위해서는 share 크기 m을 가능한 한 작게 해야 한다.

〈표3〉 비밀화상의 수에 따른 share 크기

슬라이드 수	비밀화상 수	share 크기
3	2	10
4	3	36
5	4	116
6	5	358

이상과 같은 문제점을 해결하기 위한 방법으로 세 장의 슬라이드에 두 개의 비밀화상을 분산시키는 경우에 고정 가중치 부호[5]를 이용하여 share 크기를 줄이는 방법을 보인다[6]. 먼저, 구성 방식에 사용되는 파라미터를

- m : 부호어의 길이($\sum_{i=0}^{2} {}_3C_i$)
- w : 부호어의 해밍 가중치:

  $M_{3,0}, M_{3,1}, M_{3,2}, M_{3,3}$를 연결했을 때 생성되는 행렬$M_3$ 의 행의 해밍 가중치

$$M_3 = \begin{pmatrix} 01001101 \\ 00101011 \\ 00010111 \end{pmatrix}, \ w = 4$$

- d : 두 부호어 간의 해밍 거리로 정의한다.

두 비밀화상의 화소값 조합 WW, WB, BW, BB에 대응하는 share 생성 행렬을 구성하기 위하여

- M_3에서 결정된 $d = 4$를 만족하는 두 부호어의 해밍 가중치
  = 첫번째 비밀화상의 화소값이 백일 때 해밍 가중치 (3)
- $H_1(W) + 1 = H_2(W), H_1(B)$
  $H_1(B) + 1 = H_2(B)$ (4)
  $H_2(W) + 1 = H_2(B)$

단, $H_1(B(W))$:첫번째 비밀화상의 화소값이 흑(백)일 때 해밍 가중치
$H_2(B(W))$:두번째 비밀화상의 화소값이 흑(백)일 때 해밍 가중치라 하자.

Share 생성 행렬 구성 알고리즘

첫번째 비밀화상의 화소값이 백(W)인 경우,

[Step 1] $d = 4$인 부호어 집합을 구한다.

Step 1.1. 세 개의 부호어를 임의로 뽑아내어 해밍 가중치 조사.

Step1.2. (3), (4)식에 의해서,
만약 $H_1(W) = 6, H_2(W) = 7$ 그리고 $H_2(B) = 8$을 만족하면 두 비밀화상의 화소값 조합 WW, WB에 대응하는 share 생성 행렬을 구성하고 exit.
그렇지 않으면 step1.1과 step1.2 반복 수행.

첫번째 비밀화상의 화소값이 흑(B)인 경우,

[Step 2] : (4)식에 의해서 $d = 6(H_1(B) = 7)$인 부호어 집합을 구한다.

Step 2.1. 세 개의 부호어를 임의로 뽑아내어 해밍 가중치 조사.

Step2.2. (4)식에 의해서,
만약 $H_1(B) = 7, H_2(W) = 7$ 그리

고 $H_2(B) = 8$을 만족하면 두 비밀화상의 화소값 조합 BW, BB에 대응하는 share 생성 행렬을 구성하고 exit.

그렇지 않으면 Step2.3.

Step2.3. 해밍 거리 $d = 2$인 부호어를 $d = 6$인 부호어 집합에 더하여 세 개의 부호어를 임의로 뽑아 내어 해밍 가중치 조사.

Step2.4. $H_2(W) = 7$와 $H_2(B) = 8$를 만족하고, $H_1(B) = 7$ 또는 반전을 위해서 $H_1(W) = 6$보다 작은 해밍 가중치를 가지는 부호어를 찾아서 share 생성 행렬 구성

겹친 share의 개수에 따른 흑화소 수의 천이를 표4에 나타낸다. 표4에서 기준이 되는 화소값 조합 WW의 흑화소 수는 행렬 M_3에서 임의의 두 행을 "or" 연산했을 때 해밍 가중치 $H_2(V) = 6$과 세 행 모두 "or" 연산했을 때 해밍 가중치 $H_3(V) = 7$에 각각 대응한다. 나머지 화소값 조합(WB, BW, BB)에 대한 흑화소 수는 겹친 share의 개수에 따라 비밀화상의 화소값이 백화소(W)이면 WW의 흑화소 수와 같고, 비밀화상의 화소값이 흑화소(B)이면 WW의 흑화소 수에 1을 더한 값이 되어야 한다.

〈표4〉 겹친 share에 따른 흑화소 수의 천이

두 비밀화상의 화소값 조합	2개의 share를 겹쳤을 때 흑화소 수	3개의 share를 겹쳤을 때 흑화소 수
WW	$6 \cdots H_1(W)$	$7 \cdots H_2(W)$
WB	$6 \cdots H_1(W)$	$8 \cdots H_2(B)$
BW	$7(7, 7, 5) \cdots H_1(B)$	$7 \cdots H_2(W)$
BB	$7(7, 7, 5) \cdots H_1(B)$	$8 \cdots H_2(B)$

$m = 8$, $w = 4$일 때 두 행을 "or" 연산시 해밍 가중치가 6이 되기 위하여 $d = 4$로 결정된다. m과 w의 조건을 만족하면서 $d = 4$인 부호어를 뽑아 내면 두 행의 해밍 가중치는 모두 6이 되고, 세 행의 해밍 가중치는 7 또는 8이 된다. 따라서, 표4의 화소값 조합 WW, WB의 해밍 가중치를 만족시키는 share 생성 행렬을 쉽게 구할 수 있다.

화소값 조합 BW, BB를 위한 share 생성 행렬은 두 행의 해밍 가중치가 7이 되어야 한다. 그러나, d가 4일 때 두 행의 해밍 가중치는 모두 6이 되며, $d = 6$일 때 두 행을 뽑아 내는 세 가지의 모든 경우에 대하여 해밍 가중치 7이 생성되지 않는다.

따라서, $d = 2$인 부호어와 $d = 6$인 부호어를 조합한다. 화소값 조합 BW, BB에 대해서 세 행의 해밍 가중치가 각각 7과 8이면서, 두 행을 뽑는 세 가지 경우 중 한가지만 해밍 거리가 2이고 나머지 두 가지 경우의 해밍 거리가 6인 부호어로 행렬을 구성하면 다음과 같다.

$$S_{WW} = \begin{pmatrix} 11110000 \\ 11001100 \\ 10101010 \end{pmatrix}, S_{WB} = \begin{pmatrix} 11110000 \\ 10101100 \\ 10100011 \end{pmatrix}$$

$$S_{BW} = \begin{pmatrix} 11110000 \\ 10001110 \\ 01111000 \end{pmatrix}, S_{BB} = \begin{pmatrix} 11110000 \\ 10001110 \\ 11100001 \end{pmatrix}$$

행렬 S_{WW}, S_{BB}에서 세 행에 "or" 연산을 한 해밍 가중치는 7과 8로 표4와 동일하지만, 두 행에 대한 "or" 연산의 해밍 가중치는 괄호 속의 값(7, 7, 5)으로 나타난다. 즉, 1행과 2행 및 2행과 3행의 "or" 연산은 해밍 거리 $d = 6$으로 해밍 가중치가 7이 되며, 1행과 3행의 경우는 $d = 2$로 해밍 가중치가 5가 된다.

두 행의 모든 조합에 대해 해밍 가중치 7을 만족하지 않지만, 두 행에 대한 해밍 가중치 5인 부분이 주위의 해밍 가중치 6보다 적어 반전된 형태로 복원되기 때문에 제안된 구성 방식으로 슬라이드를 구성하게 되면 두 장의 슬라이드를 겹치는 세 가지 경우 모두에 대해서 첫번째 비밀화상을 복원할 수 있게 된다.

4.2 시뮬레이션 결과

복원된 비밀화상의 종횡비를 왜곡시키지 않기 위하여 제안방식으로 구성된 share 생성 행렬에 1만 갖는 행렬 $M_{3,3}$을 1개 추가하여 시뮬레이션 하였다. 시뮬레이션에 사용된 비밀화상은 그림2의 (a)와 (b)이며, 크기는 각각 50 × 50 화소이다.

그림5의 (a), (b), (c)는 각각 제안방식으로 구성된 4개의 행렬(S_{WW}, · · · , S_{BB})을 사용 하여 비밀화상을 3 × 3배 확대하여 분산한 것이다. 비밀화상Ⅰ을 나타내고 있는 (d), (e), (f)는 각각 (a)와 (b), (b)와 (c), (a)와 (c)를 겹쳤을 때의 결과이며, (g)는 (a), (b), (c)의 모든 슬라이드를 겹친 결과로 비밀화상Ⅱ를 복원한 것이다.

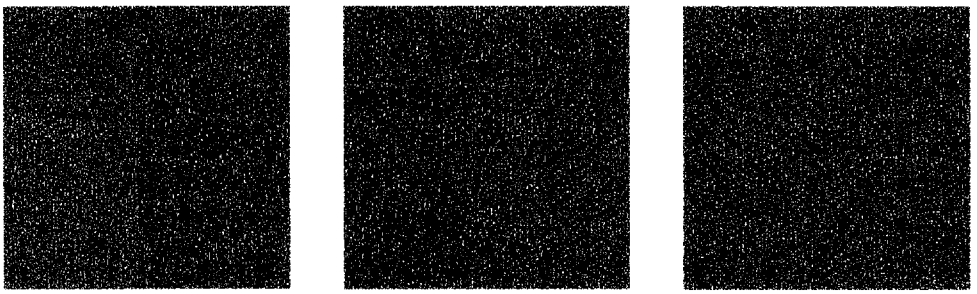
Katoh & Imai 방식의 결과인 그림3과 제안방식의 그림5에서 복원된 비밀화상Ⅰ과 비밀화상Ⅱ를 시각적으로 비교해 보면, 그림5가 훨씬 더 선명하게 복원됨을 알 수 있다. 이것은 그림5에서 사용된 share 생성 행렬의 크기가 그림3에서 사용했던 share 생성 행렬의 크기보다 더 작기 때문이다. 즉, 복원된 화상에서 선명도를 나타내는 흑/백화소 사이의 휘도비 α가 1/9로 더 크게 되었기 때문이다.

마지막으로 그림5에서 (a), (b), (c)는 모두 독립적으로는 아무런 정보도 포함하지 않는 것처럼 보이며, 실제로 이들만으로는 두 비밀화상에 대한 어떤 것도 추정할 수 없다. 그리고 비밀화상Ⅰ과 비밀화상Ⅱ는 서로 시각적으로 추정될 수 없는 안전성을 확보하고 있으나, 3.3절에서 지적한 결탁공격에 대한 안전성이 확보되지 않는 것은 복수 화상용 비밀 분산법의 결점이므로 향후 해결되어야 할 과제이다.

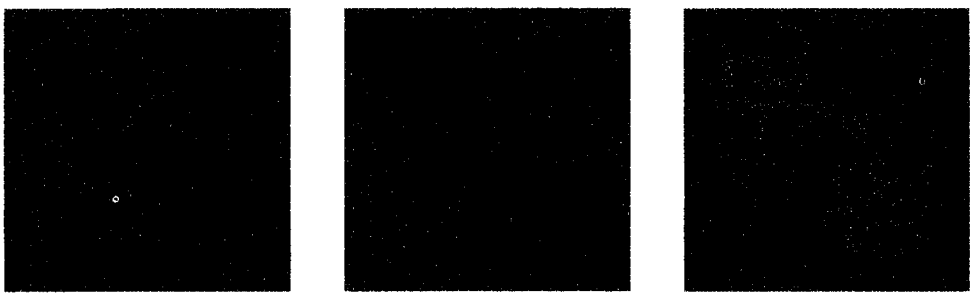
5. 결 론

Naor & Shamir의 시각암호와 Katoh & Imai의 복수 화상용 시각암호에 대하여 고찰하였다. 본 논문에서는 복수 화상용 시각암호의 안전성을 검증하였으며, 분산시키려는 비밀화상의 수의 증가에 따라 share 크기가 기하급수적으로 커지기 때문에 세 장의 슬라이드에 두 개의 비밀화상을 분산시키는 경우, 고정 가중치 부호의 해밍 거리를 조정하여 share 크기를 줄이는 방법을 제안하였다.

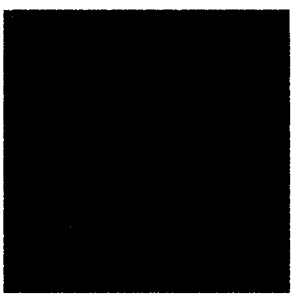
제안방식에 의해 복원되는 비밀화상Ⅰ 중의 하나가 세 장의 슬라이드 중 어떤 두 장을 선택하느냐에 따라 반전된 형태로 복원되지만, Katoh & Imai가 제안한 방식보다 share 크기를 줄이면서 두 개의 비밀화상을 완전히 복원할 수 있으며, 시각적 안전성 또한 보장되었다. 향후, 분석적 안전성에 대한 보완과 제안방식의 일반화에 대한 연구가 필요하다.



(a) 슬라이드 I (b) 슬라이드 II (c) 슬라이드 III



(d) 슬라이드 I 과 II 를 겹침 (e) 슬라이드 II 와 III 을 겹침 (f) 슬라이드 I 과 III 을 겹침



(g) 슬라이드 I, II, III 의 겹침

〈그림5〉 제안 방식으로 구성된 슬라이드

참 고 문 헌

[1] A.Shamir, "How to Share a Secret," Commun. 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, Perugia, Italy, pp.1-12, May 1994.

[3] T.Katoh and H.Imai, "On Extended and Applications of Visual Secret Sharing," ISEC95-19, pp.41-47, September 1995.(in Japanese)

[4] 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)

[5] R.E.Kibler, "Some New Constant Weight Codes," IEEE Trans. Inform. Theory, Vol. IT-26, pp.364-365, May 1980.

[6] 김미라, 박상우, 박지환, "고정 가중치 부호에 의한 복수 화상용 시각암호," 통신정보보호학회 종합학술발표회 논문집, Vol. 6 No. 1, pp.261-271. (1996. 11)

□ 著者紹介

김 미 라(Mi Ra Kim)

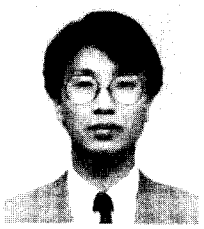
1996년 부산수산대학교 전자계산학과 졸업(이학사)
1996년 ~ 현재 부경대학교 전자계산학과 석사과정 재학중

※ 주관심분야 : 정보이론, 암호학 응용 등

박 지 환(Ji Hwan Park)

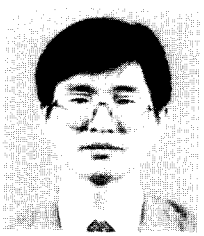
1984년 경희대학교 전자공학과 졸업(공학사)
1987년 日本國立電氣通信大學 情報工學科(工學修士)
1990년 日本橫浜國立大學 電子情報工學科(工學博士)
1990년 ~ 1996년 부산수산대학교 전자계산학과 전강, 조교수, 부교수
1994년 ~ 1995년 日本東京大學生産技術研究所 客員研究員
1996년 ~ 현재 日本東京大學生産技術研究所 協力研究員
현재 부경대학교 전자계산학과 부교수

※ 주관심 분야 : 멀티미디어 압축, 암호학 응용, 오류제어부호 등



박 상 우

1985년 ~ 1989년 고려대학교 사범대학 수학교육학과(이학사)
1989년 ~ 1991년 고려대학교 대학원 수학과(이학석사 : 응용수학 및 확률론)
1991년 ~ 현재 한국전자통신연구소 연구원



김 광 조

1973년 ~ 1980년 연세대학교 전자공학과(학사)
1981년 ~ 1983년 연세대학교 대학원 전자공학과(석사)
1988년 ~ 1991년 요꼬하마 국립대학 대학원 전자정보공학과(박사)
1979년 ~ 1997년 12월 한국전자통신연구원 부호1실장 재직
1997년 12월 ~ 현재 한국정보통신대학원 정보공학부 교수재직
본 학회 암호이론연구회 및 ISO/IEC JTC1 JSC-27 의장,
KIISC, IEICE, IEEE, IACR 각 회원

※ 주관심분야 : 암호학 및 응용 분야, M/W 통신