An Optimization Model for Visual Cryptography Schemes with Unexpanded Shares

Ching-Sheng Hsu[1], Shu-Fen Tu[2], and Young-Chang Hou[3]

[1] Department of Information Management, Ming Chuan University
No. 5, De-Ming Rd., Gui Shan Township, Taoyuan County 333, Taiwan, R.O.C.
cshsu@mcu.edu.tw
[2] Department of Information Management, Chinese Culture University
No. 55, Huagang Rd., Shihlin District, Taipei City 111, Taiwan, R.O.C.
dsf3@faculty.pccu.edu.tw
[3] Department of Information Management, Tamkang University
No. 151, Ying-Chuan Road, Tamshui, Taipei County 251, Taiwan, R.O.C.
ychou@mail.im.tku.edu.tw

Abstract. Visual cryptography schemes encrypt a secret image into n shares so that any qualified set of shares enables one to visually decrypt the hidden secret; whereas any forbidden set of shares cannot leak out any secret information. In the study of visual cryptography, pixel expansion and contrast are two important issues. Since pixel-expansion based methods encode a pixel to many pixels on each share, the size of the share is larger than that of the secret image. Therefore, they result in distortion of shares and consume more storage space. In this paper, we propose a method to reach better contrast without pixel expansion. The concept of probability is used to construct an optimization model for general access structures, and the solution space is searched by genetic algorithms. Experimental result shows that the proposed method can reach better contrast and blackness of black pixels in comparison with Ateniese et al.'s.

1 Introduction

Visual cryptography schemes (VCSs) were first proposed by Naor and Shamir in 1995 [1]. The difference between visual cryptography and traditional ones is the decryption process. Traditional cryptographic methods decrypt secrets by computers; while visual cryptography schemes can decrypt secrets only with human eyes. Therefore, VCSs are practical methods to share secrets when computers are not available. The (k, n)-threshold visual cryptography scheme is a method to encrypt a binary secret image into n shadow images called shares, so that any k or more shares enable the "visual" recovery of the secret image when they are stacked together. However, one cannot gain any secret information by gathering less than k shares. Ateniese et al. [2] extended the (k, n)-threshold access structure to general access structures in the form of (Γ_{Qual}, Γ_{Forb}, m), where Γ_{Qual} denotes a set of qualified sets, Γ_{Forb} denotes a set of forbidden sets, and m is the pixel expansion parameter. Any qualified set $Q \in \Gamma_{Qual}$ is able to recover the secret image, whereas any forbidden set $F \in \Gamma_{Forb}$ cannot leak out any secret information. In the study of visual cryptography, pixel expansion and contrast are two primary issues [3]. Since pixel-expansion based

F. Esposito et al. (Eds.): ISMIS 2006, LNAI 4203, pp. 58 – 67, 2006.

methods encode a pixel to many pixels on each share, the size of the share is larger than that of the secret image [1-6]. Therefore, such schemes not only result in distortion of shares but also consume more storage space.

In this paper, a method using genetic algorithms is proposed to cope with the problems of pixel expansion. Based on the requirements of security and contrast, the basic idea uses the concept of probability to construct an optimization model for general access structures, and the solution space is searched by genetic algorithms. The result shows that, in comparison with Ateniese et al.'s method, the proposed method can reach better contrast and blackness of black pixels in the case with four shares.

2 The Proposed Scheme

2.1 Access Structures

Let $N = \{1, \ldots, n\}$ be a set of n shares, and let 2^N denote the set of all subsets of N. Let $\Gamma_{Qual} \subseteq 2^N$ and $\Gamma_{Forb} \subseteq 2^N$, where $\Gamma_{Qual} \cup \Gamma_{Forb} = \emptyset$. We refer to members of Γ_{Qual} as qualified sets and members of Γ_{Forb} as forbidden sets. Any qualified set $Q \in \Gamma_{Qual}$ of shares can recover the secret image, whereas any forbidden set $F \in \Gamma_{Forb}$ of shares cannot leak out any secret information. The pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is called the access structure on N. For $A \subseteq 2^N$, we say that A is monotone increasing if for any $B \in A$ and any $C \subseteq N$ such that $B \cup C = \emptyset$, we have $B \cup C \in A$. That is, any superset of the set belonging to A is also in A. We say that A is monotone decreasing if for any $B \in A$ and any $C \subseteq B$ we have that $B \backslash C \in A$. That is, any subset of the set belonging to A is also in A. In the case where Γ_{Qual} is monotone increasing, Γ_{Forb} is monotone decreasing, and $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^N$, we say the access structure is strong. In this paper, we assume that access structures are strong.

Example 1: Let $N = \{1, 2, 3, 4\}$ be the set of shares. Suppose that sets $\{1, 4\}$, $\{3, 4\}$, $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 3, 4\}$, $\{2, 3, 4\}$, and $\{1, 2, 3, 4\}$ can decrypt the secret image. However, other sets must not leak out any secret information. This access structure can be represented as $\Gamma_{Qual} = \{\{1, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$ and $\Gamma_{Forb} = 2^N - \Gamma_{Qual}$.

2.2 Probability and Blackness

From the perspective of digital image halftoning, in a region of a binary image, the higher the density of evenly distributed black pixels is, the darker that region is. Thus, by adjusting the density of evenly distributed black pixels, one can create various degrees of blackness, which range from 0% (pure white) to 100% (pure black). For example, if 70 pixels of a 10×10 image block are randomly selected and colored black, then this block will be interpreted as an area with 70% blackness by human eyes. In other words, if the probability that a pixel is colored black in a binary image block is 0.7, then the blackness of this block will be 70%. Since visual cryptography is characterized by the "visual" decryption process, the secret can be successfully recovered as long as human eyes can distinguish the difference between black and

white regions. Therefore, by controlling the probability of black pixels in an image region, we can realize a visual cryptography scheme without pixel expansion.

To encrypt a secret image without pixel expansion, one can encrypt each secret pixel to a black or a white pixel on each share. Therefore, for n shares, we have 2^n encryption rules to encrypt a secret pixel. Take the (2, 2)-threshold access structure for example; that is, $N = \{1, 2\}$, $\Gamma_{\text{Qual}} = \{\{1, 2\}\}$, and $\Gamma_{\text{Forb}} = \{\{1\}, \{2\}\}$. The four encryption rules for each secret pixel will be "white-white", "white-black", "black-white", and "black-black" at the corresponding positions on the share S1 and the share S2. The corresponding colors of the stacked share (S1 + S2) are "white", "black", "black", and "black", respectively (see Table 1). The key point is how to determine the probability values of the corresponding encryption rules on the premise that security is assured and that contrast is optimized. To ensure security, we should guarantee that the probability values of the encryption rules for white pixels and that for black pixels should be identical. Suppose that P_w (resp. P_b) denotes the probability that a white (resp. black) pixel is encrypted and stacked as a black pixel on the stacked share of a forbidden set $F \in \Gamma_{\text{Forb}}$. Based on the monotone assumption, it is trivial to prove that perfect secrecy is ensured if P_w equals to P_b for every forbidden set. From the contrast point of view, the secret image can be reconstructed by the stacked share of a qualified set $Q \in \Gamma_{\text{Qual}}$.only if the difference between P_w and P_b is large enough so that human eyes can distinguish between black and white regions.

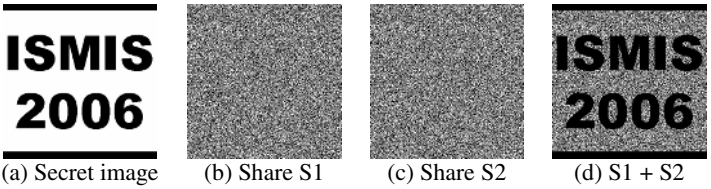
Table 1. Encryption rules of the (2, 2)-threshold VCS

Pixels	ShareS1	Share S2	Stacked share (S1 + S2)	Probability
□	□	□	□	?
	□	■	■	?
	■	□	■	?
	■	■	■	?
■	□	□	□	?
	□	■	■	?
	■	□	■	?
	■	■	■	?

Table 2 shows the probability setting of the encryption rules for the (2, 2)-threshold VCS and their effects on security and contrast. In table 2, (s_{j1}, s_{j2}) denotes the j-th encryption rule on the share S1 and the share S2, and s_{j3} denotes the result of "OR"ing s_{j1} and s_{j2}, where 0 denotes a white pixel and 1 denotes a black pixel. Let c_{0j} (resp. c_{1j}) be the probability that a white (resp. black) pixel is encrypted by the j-th encryption rule. Table 2 shows that, on S1, the probability that a white pixel is encrypted as a black pixel is $FC_{01} = s_{11} \times c_{01} + s_{21} \times c_{02} + s_{31} \times c_{03} + s_{41} \times c_{04} = 0.5$, and the probability that a black pixel is encrypted as a black pixel is also 0.5. Since $FC_{01} = FC_{11} = 0.5$ and $FC_{02} = FC_{12} = 0.5$, security is ensured. On the stacked share (S1 + S2), the probability that a white pixel is encrypted and stacked as a black pixel is $QC_{01} = s_{13} \times c_{01} + s_{23} \times c_{02} + s_{33} \times c_{03} + s_{43} \times c_{04} = 0.5$, and the probability that a black pixel is encrypted and stacked as a black pixel is $QC_{11} = 1$. Since $QC_{11} > QC_{01}$, one can recognize the secret information from (S1 + S2) with eyes (see Fig. 1).

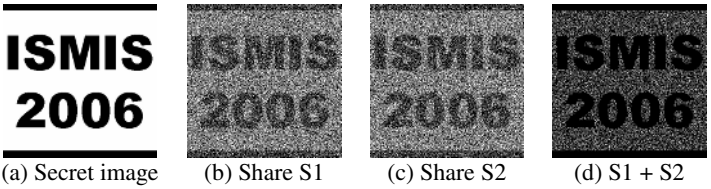
Table 2. An example of the probability setting with good security and good contrast

Pixels	Share S1	Share S2	Stacked share (S1 + S2)	Probability	Probability of being black		
					S1	S2	(S1+S2)
0	$s_{11} = 0$	$s_{12} = 0$	$s_{13} = 0$	$c_{01} = 0.5$	$FC_{01} = 0.5$	$FC_{02} = 0.5$	$QC_{01} = 0.5$
	$s_{21} = 0$	$s_{22} = 1$	$s_{23} = 1$	$c_{02} = 0.0$			
	$s_{31} = 1$	$s_{32} = 0$	$s_{33} = 1$	$c_{03} = 0.0$			
	$s_{41} = 1$	$s_{42} = 1$	$s_{43} = 1$	$c_{04} = 0.5$			
1	$s_{11} = 0$	$s_{12} = 0$	$s_{13} = 0$	$c_{11} = 0.0$	$FC_{11} = 0.5$	$FC_{12} = 0.5$	$QC_{11} = 1.0$
	$s_{21} = 0$	$s_{22} = 1$	$s_{23} = 1$	$c_{12} = 0.5$			
	$s_{31} = 1$	$s_{32} = 0$	$s_{33} = 1$	$c_{13} = 0.5$			
	$s_{41} = 1$	$s_{42} = 1$	$s_{43} = 1$	$c_{14} = 0.0$			



(a) Secret image (b) Share S1 (c) Share S2 (d) S1 + S2

Fig. 1. An example of good security and good contrast



(a) Secret image (b) Share S1 (c) Share S2 (d) S1 + S2

Fig. 2. An example of poor security and moderate contrast

If we change the probability setting of encryption rules in Table 2 to (0.25, 0.25, 0.25, 0.25, 0.00, 0.25, 0.25, 0.50), even though the new probability setting can also make difference between black and white regions on the stacked share (S1 + S2), i.e., QC_{01} (0.75) < QC_{11} (1.00), the probabilities corresponding to white and black pixels on the share S1 and S2 are not identical, i.e., FC_{01} (0.50) < FC_{11} (0.75) and FC_{02} (0.50) < FC_{12} (0.75). Thus, the security this access structure cannot be ensured (see Fig. 2). Our objective is to find a proper probability setting (c_{0j}, c_{1j}) so that the contrast of the stacked share is optimized and the security is ensured as well.

3 The Model for General Access Structures

3.1 Encryption Rule and Probability Matrices

Let $S = [s_{jn}]$ be a $2^n \times n$ Boolean matrix, where $s_{jn} \in \{0, 1\}$. We call S the encryption rule matrix, which represents all of the encryption rules on the set N of n shares. Each

row vector $S_j = [s_{j1}, s_{j2}, \ldots, s_{jn}]$ denotes an encryption rule. In the case of $n = 3$, $S_j = [1, 0, 0]$ indicates that a pixel (either black or white) will be encrypted as a black pixel, a white pixel and a white pixel on the first, the second, and the third share, respectively. Let $C = [c_{ij}]$ be a 2×2^n matrix, where $c_{ij} \in [0, 1]$, and

$$\sum_{j=1}^{2^n} c_{ij} = 1 \tag{1}$$

We call C the probability matrix, where c_{0j} (resp. c_{1j}) denotes the probability that a white (resp. black) pixel is encrypted by the j-th encryption rule. Consider the case of (2, 2)-threshold VCS in Table 2, $c_{01} = 0.5$ means that there is 50% of chance that a white pixel ('0') is encrypted by the first encryption rule [0, 0], and $c_{14} = 0.0$ means that there is no chance that a black pixel ('1') is encrypted by the fourth encryption rule [1, 1].

3.2 Security

Let FC_{0k} (resp. FC_{1k}) be the probability that a white (resp. black) pixel is encrypted and stacked as a black pixel on the stacked share of a forbidden set $F_k \in \Gamma_{\text{Forb}}$. If the security is to be assured, the values of FC_{0k} and FC_{1k} must necessarily be the same for each forbidden set F_k. Otherwise, if $FC_{0k} \neq FC_{1k}$, then the variation of frequency may leak out the secret information; thus, security is not ensured. We denote the security index of each forbidden set F_k as follows:

$$\sigma_k = |FC_{1k} - FC_{0k}|. \tag{2}$$

Since we assume that access structures are monotone, we can ensure the security of an access structure $\Gamma = (\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ as long as $\sigma_k = 0$ for every forbidden set F_k. That is, the probability setting of the encryption rules for black pixels and that for white pixels are identical. In Eq.(2), FC_{ik} can be obtained by the following equation:

$$FC_{ik} = C \times \text{OR}(S, F_k) \tag{3}$$

where $\text{OR}(S, F_k)$ denotes the column vector obtained by "OR"ing those columns in S corresponding to the shares of the forbidden set F_k.

3.3 Contrast

Let QC_{0h} (resp. QC_{1h}) be the probability that a white (resp. black) pixel is encrypted and stacked as a black pixel on the stacked share of a qualified set $Q_h \in \Gamma_{\text{Qual}}$. Then, QC_{ih} can be obtained by the following equation:

$$QC_{ih} = C \times \text{OR}(S, Q_h). \tag{4}$$

We define the contrast index of the stacked share of a qualified set Q_h to be

$$\alpha_h = QC_{1h} - QC_{0h}. \tag{5}$$

The larger the value of the contrast index α_h is, the better the contrast of the stacked share of the qualified set Q_h is; that is, the secret information can be recognized by human eyes more easily.

3.4 The Model

We use the form $\Gamma = (\Gamma_{Qual}, \Gamma_{Forb})$ to denote an arbitrary access structure with q qualified sets and f forbidden sets for a single secret image. The optimization model for VCSs of $\Gamma = (\Gamma_{Qual}, \Gamma_{Forb})$ is formulated as Eq.(6). Since there are 2^n possible encryption rules for each secret pixel, there are totally 2×2^n variables corresponding to all the probability values needed to be solved. Furthermore, each variable is a real number between 0 and 1, and all variables corresponding to the black or white pixels must sum up to be 1. The model also contains f constraint functions with respect to security. Besides, since we need to pursue better contrast of each stacked share of the qualified set $Q \in \Gamma_{Qual}$, there are totally q objective functions to be optimized.

$$\left.\begin{array}{ll} \max & \alpha_h = QC_{1h} - QC_{0h},\ for\ h = 1, 2, ..., q. \\ \text{s.t.} & \sigma_k = \left|FC_{1k} - FC_{0k}\right| = 0,\ for\ k = 1, 2, ..., f, \\ & \sum_{j=1}^{2^n} c_{ij} = 1,\ for\ i = 0, 1, \\ & c_{ij} \in [0, 1],\ for\ i = 0, 1,\ and\ \ j = 1, 2, ..., 2^n. \end{array}\right\} \tag{6}$$

4 The Application of Genetic Algorithms

Genetic algorithms (GAs), search and optimization procedures, which simulate the natural evolution rules, were proposed by Holland in the 1970s [7]. GAs are composed of a population of chromosomes and several genetic operators. In a population, a chromosome denotes a solution of a specific problem. In addition, GAs use the fitness function to evaluate the goodness of each solution and to guide the direction of search in the solution space. There are three primary operators for GAs: reproduction, crossover and mutation. The reproduction operator is used to choose more survivable chromosomes according to the given fitness function, and then copy these selected chromosomes to the matting pool for further genetic operations. The crossover operator is used to exchange parts of the genes of two chromosomes and then to generate the corresponding offspring. The mutation operator is used sporadically to alter genes randomly; therefore, some important genes that do not present before may appear and some new solutions may be generated from a near converged population. Due to the parallel mechanism for processing a population of chromosomes simultaneously, the power of searching from multiple points makes it very suitable for multi-modal and multi-objective optimization problems.

4.1 Encoding and Decoding

Due to the real number data type of the decision variables in Eq.(6), real parameter encoding method is used; that is, each chromosome is composed of a series of real numbers. The real parameter encoding method is superior in its ability to avoid the

problems of "Hamming cliffs" and loss in precision caused by the binary encoding method [8, 9]; moreover, a real number string is shorter than a binary string. To satisfy the last two constraints in Eq.(6), we pick the $2^n - 1$ real numbers (x_{i1}, x_{i2}, …, $x_{i,2^n-1}$) from the range between 0 and 1 as the partition points. Thus, the range between 0 and 1 is divided into 2^n segments. The length of the j-th segment represents the value of c_{ij}. Therefore, the chromosome is encoded as $\boldsymbol{x} = (x_{01}, x_{02}, \ldots, x_{0,2^n-1}, x_{11}, x_{12}, \ldots, x_{1,2^n-1})$. After ($x_{i1}$, x_{i2}, …, $x_{i,2^n-1}$) is sorted in an ascending order, the $2^n - 1$ partition points are generated. Let (x'_{i1}, x'_{i2}, …, $x'_{i,2^n-1}$) = Sort(x_{i1}, x_{i2}, …, $x_{i,2^n-1}$), $x'_{i0} = 0$, and $x'_{i,2^n} = 1$, where $i = 0, 1$. Using these partition points, we can decode the chromosomes by $c_{ij} = x'_{ij} - x'_{i,j-1}$.

4.2 Fitness Function

Based on the aforementioned chromosome encoding and decoding schemes, we can formulate the contrast functions as $\theta_h(\boldsymbol{x}) = \alpha_h$, *for* $h = 1, 2, \ldots, q$. In addition, to deal with the first constraint in Eq.(6), we use the penalty function $\phi(\boldsymbol{x}) = \sum\sigma_k$, which represents the level of violation of the constraints in the optimization model. Consequently, the fitness functions incorporated with the constraints are written as $\Theta_h(\boldsymbol{x}) = \theta_h(\boldsymbol{x}) - \beta\cdot\phi(\boldsymbol{x})$, where β determines the strength of penalty. To solve this multiple objective optimization problem, we use the weighted-sum approach because of its excellences in efficiency and the ease of implementation. The fitness function under the weight-sum approach is formulated as $\Theta(\boldsymbol{x}) = \sum\Theta_h(\boldsymbol{x})$.

4.3 Reproduction, Crossover and Mutation

To deal with negative fitness values, we use the binary tournament selection method. The procedure is as follows: pick two chromosomes randomly from the population, compare their fitness values, and copy the chromosome with higher fitness value to the matting pool. Besides, we employ the simulated binary crossover (SBX) operator [10], which biases solutions near each parent more favorably than solutions away from the parents, to deal with the crossover operation for the real number strings. The advantage of using the SBX operator is that one can control the search power of GAs by controlling the distribution index η_c. Finally, we mutate a specific gene by the random initialization operation. Let x_i be the i-th gene in the real parameter encoded string, let y_i be the result of mutating x_i, and let $x_i^{(U)}$ and $x_i^{(L)}$ be the upper and lower bounds of x_i, respectively. The random initialization operation is formulated as $y_i = r_i(x_i^{(U)} - x_i^{(L)}) + x_i^{(L)}$, where r_i denotes a random number between 0 and 1. Besides, we assume that the probability of mutation for each gene is uniform.

5 Results and Discussions

We deal with an access structures shown in Example 1. The parameters for GAs are listed in Table 3, and the resultant probability matrix C is as follows.

Table 3. Parameters for genetic algorithms

Parameters	Values
Population size	1000
Chromosome length	32
Crossover rate	0.9
Mutation rate	0.01/per gene
Reproduction method	Binary tournament selection
Crossover method	SBX with $\eta_c = 2$
Stop condition	600 generations

$$C = \begin{bmatrix} 0.3 & 0.0 & 0.0 & 0.0 & 0.1 & 0.0 & 0.0 & 0.1 & 0.0 & 0.0 & 0.0 & 0.4 & 0.0 & 0.1 & 0.0 & 0.0 \\ 0.0 & 0.2 & 0.0 & 0.1 & 0.0 & 0.2 & 0.0 & 0.0 & 0.0 & 0.1 & 0.3 & 0.0 & 0.0 & 0.0 & 0.1 & 0.0 \end{bmatrix} \tag{7}$$

Table 4. The security and contrast analysis for Γ

The security index σ_k of the forbidden set F_k		The contrast index α_h of the qualified set Q_h	
$F_1 = \{1\}$	$\sigma_1 = 0$	$Q_1 = \{1, 4\}$	$\alpha_1 = 0.4$ ($QC_{01} = 0.6$, $QC_{11} = 1.0$)
$F_2 = \{2\}$	$\sigma_2 = 0$	$Q_2 = \{3, 4\}$	$\alpha_2 = 0.4$ ($QC_{02} = 0.6$, $QC_{12} = 1.0$)
$F_3 = \{3\}$	$\sigma_3 = 0$	$Q_3 = \{1, 2, 3\}$	$\alpha_3 = 0.1$ ($QC_{03} = 0.7$, $QC_{13} = 0.8$)
$F_4 = \{4\}$	$\sigma_4 = 0$	$Q_4 = \{1, 2, 4\}$	$\alpha_4 = 0.3$ ($QC_{04} = 0.7$, $QC_{14} = 1.0$)
$F_5 = \{1, 2\}$	$\sigma_5 = 0$	$Q_5 = \{1, 3, 4\}$	$\alpha_5 = 0.4$ ($QC_{05} = 0.6$, $QC_{15} = 1.0$)
$F_6 = \{1, 3\}$	$\sigma_6 = 0$	$Q_6 = \{2, 3, 4\}$	$\alpha_6 = 0.3$ ($QC_{06} = 0.7$, $QC_{16} = 1.0$)
$F_7 = \{2, 3\}$	$\sigma_7 = 0$	$Q_7 = \{1, 2, 3, 4\}$	$\alpha_7 = 0.3$ ($QC_{07} = 0.7$, $QC_{17} = 1.0$)
$F_8 = \{2, 4\}$	$\sigma_8 = 0$		

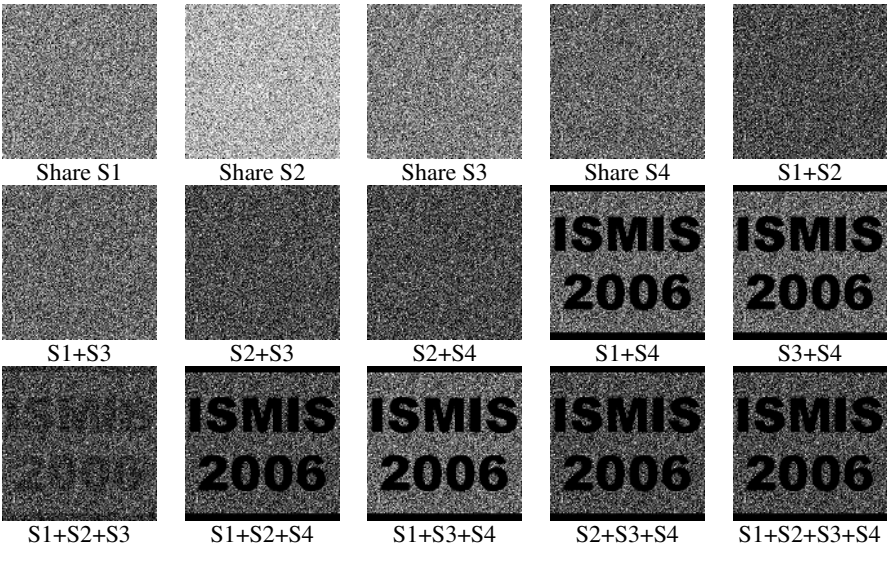


Fig. 3. The experimental result for the access structure Γ

The security and contrast for the resultant probability matrices C are analyzed in Table 4. The shares and stacked results generated according to C are shown in Fig. 3. We can see from Table 4 that the security indices of all the forbidden sets are zero; therefore, C is secure. On the other hand, the contrast indices of the qualified sets Q_1 ~ Q_7 are $\alpha_1 = 0.4$, $\alpha_2 = 0.4$, $\alpha_3 = 0.1$, $\alpha_4 = 0.3$, $\alpha_5 = 0.4$, $\alpha_6 = 0.3$, and $\alpha_7 = 0.3$, respectively. Observing Fig. 3, we can say that one can easily recognize the hidden secret from the stacked shares of the qualified sets. Besides, we can also see from Table 4 that the blackness of black regions of the qualified sets Q_1, Q_2, and Q_4 ~ Q_7 are 100%; therefore, we realized perfect reconstruction of black pixels on the stacked shares of these qualified sets in this experiment.

Ateniese et al. [4] proposed a pixel-expansion-based method to construct basis matrices for the same access structures shown in Example 1, and their basis matrices M_0 for white pixels and M_1 for black pixels with minimum pixel expansion $m^* = 5$ are listed below.

$$M_0 = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \quad M_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{8}$$

Using M_0 and M_1, the contrast indices of the qualified sets Q_1 ~ Q_7 are 0.2, 0.2, 0.2, 0.2, 0.2, 0.2, and 0.4, respectively. Comparing with our results, we found that the average contrast is 37.7% higher than that proposed by Ateniese et al. In addition, we reached perfect reconstruction of black pixels on six qualified sets. However, in Ateniese et al.'s method, only the qualified set {1, 2, 3, 4} has 100% of blackness for black pixels. We can conclude that our method is superior to Ateniese et al.'s in contrast and blackness of black pixels. Moreover, we do not need to expand pixels.

6 Conclusions

Most visual cryptographic methods need to expand pixels so that the size of each share is larger than that of the secret image. Pixel expansion not only results in distortion of the shares but also consumes more storage space. Consequently, it leads to the difficulty in carrying these shares and the requirement of more storage space. This paper proposed a new method without pixel expansion. We used the concept of probability and considered the security and contrast issues to construct an optimization model for general access structures. Then, the solution space is searched by genetic algorithms. In the case of four shares, we found that our method was superior to Ateniese et al.'s in contrast and blackness of black pixels. In the future, we will study the optimization model for sharing multiple secret images among a set of participants.

Acknowledgement

This work was supported in part by a grant from National Science Council of the Republic of China under the project NSC90-2213-E-008-047.

References

1. Naor, M., Shamir, A.: Visual Cryptography, in Advances in Cryptology-EUROCRYPT '94, LNCS 950, Springer-Verlag, (1995) 1-12.
2. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Visual Cryptography for General Access Structures, Information and Computation, 129(2), (1996) 86-106.
3. Blundo, C., De Santis, A.: Visual Cryptography Schemes with Perfect Reconstruction of Black Pixels , Computer & Graphics, 12(4), (1998) 449-455.
4. Ateniese, G., Blundo, C. De Santis, A., Stinson, D.R.: Constructions and Bounds for Visual Cryptography, in 23rd International Colloquium on Automata, Languages and Programming (ICALP '96), LNCS 1099, (1996) 416-428.
5. Hou, Y.C.: Visual Cryptography for Color Images, Pattern Recognition, Vol. 36, No. 7, (2003) 1619-1629.
6. Hou, Y.C., Tu, S.F.: A Visual Cryptographic Technique for Chromatic Images Using Multi-Pixel Encoding Method, Journal of Research and Practice in Information Technology, .Vol. 37, No. 2, (2005) 179-191.
7. Holland, J.H.: Adaptation in Natural and Artificial Systems", Ann Arbor: The University of Michigan Press (1975).
8. Deb, K.: Multi-Objective Optimization using Evolutionary Algorithms, John Wiley & Sons, West Sussex (2001).
9. Srinivas, M., Patnaik, L. M.: Genetic Algorithms: A Survey, Computer, 27(6), (1994) 17-26.
10. Deb, K., Agrawal, R.B.: Simulated Binary Crossover for Continuous Search Space, Complex Systems, 9(2), (1995) 115-148.