A Probabilistic Model of (t, n) Visual Cryptography Scheme With Dynamic Group

Sian-Jheng Lin and Wei-Ho Chung, *Member, IEEE*

***Abstract*—The (t, n) visual cryptography (VC) is a secret sharing scheme where a secret image is encoded into n transparencies, and the stacking of any t out of n transparencies reveals the secret image. The stacking of $t-1$ or fewer transparencies is unable to extract any information about the secret. We discuss the additions and deletions of users in a dynamic user group. To reduce the overhead of generating and distributing transparencies in user changes, this paper proposes a (t, n) VC scheme with unlimited n based on the probabilistic model. The proposed scheme allows n to change dynamically in order to include new transparencies without regenerating and redistributing the original transparencies. Specifically, an extended VC scheme based on basis matrices and a probabilistic model is proposed. An equation is derived from the fundamental definitions of the (t, n) VC scheme, and then the (t, ∞) VC scheme achieving maximal contrast can be designed by using the derived equation. The maximal contrasts with $t = 2$ to 6 are explicitly solved in this paper.**

***Index Terms*—Contrast, random grids (RGs), secret sharing, visual cryptography (VC).**

I. Introduction

VISUAL cryptography (VC) is a branch of secret sharing. In the VC scheme, a secret image is encoded into n transparencies, and the content of each transparency is noise-like so that the secret information cannot be retrieved from any one transparency via human visual observation or signal analysis techniques. In general, a (t, n)-threshold VC scheme has the following properties: The stacking of any t out of those VC generated n transparencies can reveal the secret by visual perception, but the stacking of any $t-1$ or fewer number of transparencies cannot retrieve any information other than the size of the secret image. Naor and Shamir [1] proposed a (t, n)-threshold VC scheme based on basis matrices, and the model had been further studied and extended. The related works include the VC schemes based on probabilistic models [2]–[4], general access structures [5], [6], VC over halftone images [7], [8], VC for color images [9], cheating in VC [10], [11], the general formula of VC schemes [12], and region incrementing VC [13].

Contrast is one of the important performance metrics for VC schemes. Generally, the stacking revelation of the secret with higher contrast represents the better visual quality, and therefore the stacking secret with high contrast is the goal of pursuit in VC designs. Naor and Shamir [1] define a contrast formula which has been widely used in many studies. Based on the definition of contrast, there are studies attempting to achieve the contrast bound of (t, n) VC scheme [4], [14]–[20]. For instance, Blundo *et al.* [17] give the optimal contrast of $(2, n)$ VC schemes. Hofmeister *et al.* [19] provide a linear program which is able to compute exactly the optimal contrast for (t, n) VC schemes. Krause and Simon [20] provide the upper bound and lower bound of the optimal contrast for (t, n) VC schemes. Moreover, there exist VC related researches using differential definitions of contrast [21]–[23]. Another important metric is the pixel expansion denoting the number of subpixels in transparency used to encode a secret pixel. The minimization of pixel expansions has been investigated in previous studies [24], [25].

The probabilistic model of the VC scheme was first introduced by Ito *et al.* [2], where the scheme is based on the basis matrices, but only one column of the matrices is chosen to encode a binary secret pixel, rather than the traditional VC scheme utilizing the whole basis matrices. The size of the generated transparencies is identical to the secret image. Yang [31] also proposed a probabilistic model of (t, n) VC scheme, and the two cases $(2, n)$ and (n, n) are explicitly constructed to achieve the optimal contrast. Based on Yang [31], Cimato *et al.* [32] proposed a generalized VC scheme in which the pixel expansion is between the probabilistic model of VC scheme and the traditional VC scheme.

Encrypting an image by random grids (RGs) was first introduced by Kafri and Keren [26] in 1987. A binary secret image is encoded into two noise-like transparencies with the same size of the original secret image, and stacking of the two transparencies reveals the content of the secret. Comparing RGs with basis matrices, one of the major advantages is that the size of generated transparencies is unexpanded. The RG scheme is similar to the probabilistic model of the VC scheme, but the RG scheme is not based on the basis matrices. The recent studies include the RG for color image [27], $(2, n)$ RG, and (n, n) RG schemes [28], [29]. We also compare the proposed method with $(2, n)$ RG [29] in Section IV.

We consider the scenario of a dynamic user group, where n'' new participants are to join the user group with n' original participants; and the transparencies need to accommodate the new $n = n' + n''$ users. If the transparencies are to be generated with the traditional (t, n') VC scheme, the n' original transparencies need to be discarded, and the $n' + n''$ new transparencies need to be generated with the traditional $(t, n' + n'')$ VC scheme. The regeneration and redistribution of the whole transparencies consume computing and communication resources and may lead to

Manuscript received May 09, 2011; revised August 15, 2011; accepted August 17, 2011. Date of publication September 06, 2011; date of current version January 13, 2012. This work was supported by the National Science Council of Taiwan, under Grant NSC 100-2221-E-001-004. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Carlo Blundo.

The authors are with the Research Center for Information Technology Innovation, Academia Sinica, Nankang, Taipei 115, Taiwan (e-mail: whc@citi.sinica.edu.tw).

Digital Object Identifier 10.1109/TIFS.2011.2167229

the potential security vulnerability. The addition and deletion of users are further discussed in Section IV-A.

In this paper, we propose a probabilistic model of (t, n) VC scheme with unlimited n. The major contribution is that the proposed scheme accommodates dynamic changes of users in the group sharing a VC secret. The proposed scheme allows changes of users without regeneration and redistribution of VC transparencies, which reduce the computing and communication resources in accommodating user changes. The scheme is capable of generating an arbitrary number of transparencies and the explicit algorithms are proposed to generate the transparencies. For a group with n' initial users, the proposed Algorithm 1 explicitly generates the required n' transparencies. For n'' newly joining participants, the n'' new transparencies can be explicitly generated through Algorithm 2, and the n'' new transparencies can be distributed to the n'' new participants without the need to update the original transparencies. The secondary contribution is that this paper designs an implementation of (t, ∞) VC based on the probabilistic model, and the proposed scheme allows the unlimited number of users. For the conventional (t, n) VC scheme to implement the case $n \to \infty$, the mathematical manipulations of infinite size of basis matrices and variables are often required, which is computationally prohibitive. Our approach designs an implementation scheme which is capable of producing a finite subset of the complete infinite transparencies through the proposed Algorithms 1 and 2, with computationally feasible operations. We also derive an optimization problem $L(t)$ to solve the maximal contrast of the proposed (t, ∞) VC scheme.

Notations

t	The threshold of a (t, n) VC scheme.
n	The number of generated transparencies of a (t, n) VC scheme.
m	The number of subpixels to encode a secret pixel; i.e., the width of the basis matrices.
$\oplus$	Stacking operation, equivalent to the bitwise operation "OR."
C_0 and C_1	Two collections of $n \times m$ Boolean matrices.
$H(v)$	The number of ones in a vector v.
α	The contrast of the VC scheme based on basis matrices.
B_0 and B_1	Two $n \times m$ Boolean matrices where $B_0 \in C_0$ and $B_1 \in C_1$.
$A_{j,n}$	A $n \times \binom{n}{j}$ Boolean matrix containing all possible combinations of j zeros and $(n - j)$ ones as the columns.
H_0 and H_1	Two vectors to represent the multiplicities of A_j in B_0 and B_1.
α'	The contrast of the probabilistic model of VC scheme.
b_0, b_1	A column randomly selected from B_0 and B_1.
$h(v)$	The frequency probability of appearing ones in a vector v.
P_0, P_1	The discrete probability distribution of all columns in B_0 and B_1.
$E(\bullet)$	A memoryless binary sequence with values of elements as 0 or 1, where the probability of assigning each element e to 0 is $\bullet$.
ΔP	A vector $\Delta P = P_0 - P_1$.
X, Y	Two vectors to record the nonzero terms in ΔP.
$L(t)$	An optimization problem to find the optimal contrast of $(t, n \to \infty)$ VC scheme.
S	A binary secret image.
s	A ready-to-process pixel taken from S.
T_i	The ith generated transparency.
t_i	A pixel at T_i, and the position corresponds to the position of s.
n' and n''	n' is the number of original participants in the user group initially, and n'' is the number of new participants to join the user group.
Z	An index table where $Z[w, h]$ is the index of the used memoryless sequence $E(x_{Z[w,h]})$ to encode the secret pixel $s[w, h]$.
$P(\bullet)$	The probability of the event $\bullet$.
$G(\bullet)$	A group which contains all columns of the matrix $\bullet$ as the elements.

II. Extended Version Based on Basis Matrices and Probabilistic Model

A. Basis Matrices

The basis matrices of (t, n) VC scheme were first introduced by Naor and Shamir [1]. In this paper, a white-and-black secret image or pixel is also described as a binary image or pixel. In the basis matrices, to encode a binary secret image S, each secret pixel $s \in \{\text{white}, \text{black}\}$ will be turned into n blocks at the corresponding position of n transparencies $T_1, T_2, \ldots, T_n$, respectively. Each block consists of m subpixels and each subpixel is opaque or transparent. Throughout this paper, we use 0 to indicate a transparent subpixel and 1 to indicate an opaque subpixel. If any two subpixels are stacked with matching positions, the representation of a stacked pixel may be transparent, when the two corresponding pixels are both transparent. Otherwise, the stacked pixel is opaque. Let $\oplus$ denote the stacking operation, defined as

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1,\ 1 \oplus 0 = 1,\ 1 \oplus 1 = 1.$$

Actually, $\oplus$ can be treated as the bitwise operation "OR." It is noted that we use the notation $T_i \oplus T_j$ to indicate the stacking of the two transparencies T_i and T_j, since T_i and T_j can be treated as two Boolean matrices.

For the basis matrices, two collections of $n \times m$ Boolean matrices C_0 and C_1 are constructed to encode the binary pixel s, respectively. Each row of the matrix in C_0 and C_1 corresponds to an encoded block, and the elements represent the subpixels. Before describing the definitions of C_0 and C_1, we first explain how to encode s. For s being white, the dealer randomly chooses a matrix from C_0 with uniform distribution and then sends all the rows to each T_i, respectively. For s being black, the dealer randomly chooses a matrix from C_1 with uniform distribution and then sends all the rows to each T_i, respectively. The C_0 and C_1 are required to meet the conditions described in Definition 1. Let $H(v)$ denote the hamming weight of a $(0-1)$-vector v (i.e., the number of ones in v).

Definition 1: A (t, n) VC scheme with m subpixels and contrast $\alpha > 0$ can be represented as two collections of $n \times m$ Boolean matrices C_0 and C_1. Let d be a constant integer. A valid VC scheme is required to meet the following conditions [1]:

1) For any matrix in C_0, the stacked v of any t out of the n rows in the matrix satisfies $H(v) \leq d - \alpha m$.
2) For any matrix in C_1, the stacked v of any t out of the n rows in the matrix satisfies $H(v) \geq d$.
3) For any k-element subset $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ and $k < t$, the two collections of $k \times m$ matrices obtained by restricting each matrix in C_0 and C_1, to rows $i_1, i_2, \ldots, i_k$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The first and the second conditions represent the contrast requirements. In general, with larger α, the stacking result is more visually distinguishable. The third condition represents the security requirement. A valid VC must be able to prevent the secret pixels from being revealed by analyzing the patterns or probability distributions from k transparencies for $k < t$.

If we find an $n \times m$ Boolean matrix $B_0 \in C_0$ and an $n \times m$ Boolean matrix $B_1 \in C_1$, we can construct C_0 and C_1 by permuting all columns of B_0 and B_1 [1], expressed as

$$\begin{aligned} C_0 = &\{\text{All the matrices obtained} \\ &\quad \text{by permuting all columns of } B_0\}, \\ C_1 = &\{\text{All the matrices obtained} \\ &\quad \text{by permuting all columns of } B_1\}. \end{aligned}$$

If two $n \times m$ Boolean matrices B_i' and B_i'' can be adjusted to become the same matrix with reordering columns, B_i' and B_i'' are equivalent in terms of generating C_i. Therefore, the orders of columns of B_0 and B_1 are technically insignificant.

The previous studies indicated that the "totally symmetric" scheme [19] (also called the canonical form [15]) is only considered for constructing B_0 and B_1, since the studies [15] and [19] proved that the "totally symmetric" schemes cover the (t, n) VC schemes with optimal contrast. Let $A_{j,n}$ denote an $n \times \binom{n}{j}$ Boolean matrix consisting of all possible combinations of j zeros and $(n-j)$ ones as columns of $A_{j,n}$. A matrix B_i is called "totally symmetric" if B_i can be divided into some $A_{j,n}$, $j \in \{0, 1, \ldots, n\}$ with horizontal concatenation. Thus, the B_0 and B_1 of a "totally symmetric" VC scheme can be presented as two vectors $H_0 = (h_{0,0}, h_{1,0}, \ldots, h_{n,0})$ and $H_1 = (h_{0,1}, h_{1,1}, \ldots, h_{n,1})$ in which $h_{j,i}$ is the multiplicity of $A_{j,n}$ in B_i. The relation between m and $h_{j,i}$ is

$$m = \sum_{j=0}^{n} \binom{n}{j} h_{j,i}. \tag{1}$$

Example 1: An example of a (3, 4) VC scheme is

$$B_0 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$\text{and} \quad B_1 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The $A_{j,n}$ are

$$A_{0,4} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \; A_{1,4} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix},$$

$$A_{2,4} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \; A_{3,4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$A_{4,4} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Thus, B_0 is represented as $H_0 = (0, 1, 0, 0, 2)$, and B_1 is represented as $H_1 = (2, 0, 0, 1, 0)$. ■

B. Probabilistic Model of VC Scheme

In the scenario where n is very large, i.e., $n \to \infty$, to construct B_i is impractical. Thus, the proposal of a new VC scheme is required in order to overcome the above problem. The probabilistic model of VC is first introduced by Ito *et al.* [2]. Instead of the basis matrices expanding a secret pixel into a block with m subpixels in transparencies, the probabilistic model of VC only uses one subpixel to represent one secret pixel. The idea is briefly described as follows.

To encode the secret image S, the probabilistic model of VC constructs two basis matrices B_0 and B_1. For the secret pixel s being white, the dealer randomly chooses a column b_0 from B_0 with uniform distribution and sends each element t_i to T_i, respectively. For s being black, the dealer randomly chooses a column b_1 from B_1 with uniform distribution and sends each element t_i to T_i, respectively. To decode S, any t out of the n transparencies $T_{i_1}, T_{i_2}, \ldots, T_{i_t}$ are stacked $T_{i_1} \oplus T_{i_2} \oplus \cdots \oplus T_{i_t}$. Then the region $\{s = \text{white} | s \in S\}$ is probabilistically *more likely* to appear white than the region $\{s = \text{black} | s \in S\}$ is. Thus, we have

$$\begin{aligned} &P(t_{i_1} \oplus t_{i_2} \oplus \cdots \oplus t_{i_t} = 0 | s = \text{white}) \\ &\qquad > P(t_{i_1} \oplus t_{i_2} \oplus \cdots \oplus t_{i_t} = 0 | s = \text{black}) \end{aligned} \tag{2}$$

where $P(\bullet)$ is the probability of the event $\bullet$, and $t_{i_j} \in T_{i_j}$ is a binary value taken from b_0 (if s is white) or b_1 (if s is black). The notation $\{t_{i_j}, t_{i_j}, \ldots, t_{i_t}\} \subseteq b_i$ means that $\{t_{i_j}, t_{i_j}, \ldots, t_{i_t}\}$ are

any t elements in b_i. As a result, S can be interpreted by visual perception since the human visual system can be treated as a low pass filter. On the other hand, to protect S, in the case where the number of stacked transparencies k is smaller than t, the region corresponding to the white pixels in S is probabilistically *identical*, in terms of appearing black or white, to the region corresponding to the black secret pixels. In other words, the regions $\{s = \text{white}|s \in S\}$ are probabilistically indistinguishable to the regions $\{s = \text{black}|s \in S\}$ on the stacking result. The property is expressed as

$$P(t_{i_1} \oplus t_{i_2} \oplus \cdots \oplus t_{i_k} = 0|s = \text{white}) > P(t_{i_1} \oplus t_{i_2} \oplus \cdots \oplus t_{i_k} = 0|s = \text{black}), \quad \text{for } k < t. \quad (3)$$

For the contrast condition described in probability model [2], the contrast between white and black pixels is calculated from the differential "probability" of appearing zero and not the differential "frequency" used in basis matrices. The contrast is defined as

$$\alpha' = P(t_{i_1} \oplus t_{i_2} \oplus \cdots \oplus t_{i_t} = 0|s = \text{white}) - P(t_{i_1} \oplus t_{i_2} \oplus \cdots \oplus t_{i_t} = 0|s = \text{black}) \quad (4)$$

to distinguish α used in Definition 1. Let $h(v) = H(v)/m$ denote the frequency probability of appearing ones in v. The definition of (t, n) Probabilistic VC scheme based on B_0 and B_1 is given as follows.

Definition 2: A (t, n) Probabilistic VC scheme with contrast $\alpha' > 0$ can be represented as two $n \times m$ Boolean matrices B_0 and B_1. Let d' be a constant integer; a valid Probabilistic VC must satisfy the following conditions:

1) The stacked v of any t out of the n rows in B_0 satisfies $h(v) \leq d' - \alpha'$.
2) The stacked v of any t out of the n rows in B_1 satisfies $h(v) \geq d'$.
3) For any k-element subset $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ and $k < t$, the two $k \times m$ matrices obtained by restricting each matrix in B_0 and B_1, to rows $i_1, i_2, \ldots, i_k$ are the identical.

C. Proposed VC Scheme

The proposed method is based on the basis matrices and the idea of probabilistic model. For a (t, n) VC scheme, the "totally symmetric" form of B_0 and B_1 are both constructed and described as H_0 and H_1, respectively. For a column b_i randomly selected from B_i with uniform distribution, let $p_{j,i}$ be the probability that b_i consists of j zeros and $(n - j)$ ones. The $p_{j,i}$ is expressed by

$$p_{j,i} = P(H(b_i) = n - j|b_i \in G(B_i)) \quad (5)$$

where $G(\bullet)$ outputs a group which contains all columns of the matrix $\bullet$ as the elements, and we have

$$\sum_{j=0}^{n} p_{j,i} = 1 \quad (6)$$

$$p_{j,i} = \binom{n}{j} \frac{h_{j,i}}{m}. \quad (7)$$

Thus, $P_0 = (p_{0,0}, p_{1,0}, \ldots, p_{n,0})$ and $P_1 = (p_{0,1}, p_{1,1}, \ldots, p_{n,1})$ represent the probability distributions by which the columns are selected to encode white and black secret pixels s, and by (7), P_0 and P_1 are homogeneous to H_0 and H_1 for describing B_0 and B_1, respectively. According to the probabilistic model, we randomly choose a column b_i from B_i; since B_i consists of many submatrices $A_{j,n}$, suppose a column is chosen from $A_{j,n}$. This step can be simulated by rearranging a vector consisting of j zeros and $(n - j)$ ones randomly, and all possible combinations are equally likely to be a candidate, since all columns in $A_{j,n}$ have equal chances to be selected. This property reduces the memory requirement to store B_0 and B_1 during encoding. For the case $n \to \infty$, the generated column becomes a (0-1) memoryless sequence $E(j/n)$ where the probability of assigning each element e to 0 is j/n (i.e., $P(e = 0|e \in E(j/n)) = j/n$). In terms of computer programming, $E(j/n)$ can be simulated with a random Boolean generator where the probability of generating 0 is j/n and generating 1 is $(1 - j/n)$. For convenience, in the rest of the paper, the abbreviation (t, ∞) PrVC scheme denotes the probabilistic model of VC with unlimited n.

Lemma 1: For any k elements $t_{i_1}, t_{i_2}, \ldots, t_{i_k}$ generated from the secret pixel s with (t, ∞) PrVC scheme, after the stacking $t_{i_1} \oplus t_{i_2} \oplus \cdots \oplus t_{i_k}$, the probability of the stacking result appearing zero is $P(t_{i_1} \oplus t_{i_2} \oplus \cdots \oplus t_{i_k} = 0|s = \text{white}) = \sum_{j=0}^{n} p_{j,0} \left(\frac{j}{n}\right)^k$ and $P(t_{i_1} \oplus t_{i_2} \oplus \cdots \oplus t_{i_k} = 0|s = \text{black}) = \sum_{j=0}^{n} p_{j,1} \left(\frac{j}{n}\right)^k$.

Proof: To encode the secret pixel s, a candidate in $\{E(j/n)|j = 0, 1, \ldots, n\}$ is chosen, and the generated elements $e_1, e_2, \ldots, e_k$ are assigned to $t_{i_1}, t_{i_2}, \ldots, t_{i_k}$, respectively. The probability of generating $E(j/n)$ as the candidate is $p_{j,i}$. Suppose $E(j/n)$ is generated to encode the secret pixel. For the case where k transparencies are stacked, the probability of the secret pixel appearing zero is $(j/n)^k$, because the k corresponding elements $e_1, e_2, \ldots, e_k$ at the k transparencies, are required to be all zeros, and we have

$$P\left(e_1 \oplus e_2 \oplus \cdots \oplus e_k = 0|\{e_1, e_2, \ldots, e_k\} \subseteq E\left(\frac{j}{n}\right)\right) = \prod_{j=1}^{k} P(e_j = 0) = \left(\frac{j}{n}\right)^k.$$

Therefore, the probability of a pixel appearing zero is $\sum_{j=0}^{n} p_{j,i}(j/n)^k$. ■

As stated in the security condition in Definition 2, after stacking any k rows $(k < t)$ in B_0 and B_1 to obtain two vectors v_0 and v_1, we have $h(v_0) = h(v_1)$. Based on the results of Lemma 1, the $t-1$ equations maintaining the security condition are described as

$$\sum_{j=0}^{n} p_{j,0} \left(\frac{j}{n}\right)^k = \sum_{j=0}^{n} p_{j,1} \left(\frac{j}{n}\right)^k \Rightarrow \sum_{j=0}^{n} \Delta p_j \left(\frac{j}{n}\right)^k = 0 \quad \forall k = 1, 2, \ldots, t-1 \quad (8)$$

where $\Delta p_j = p_{j,0} - p_{j,1}$, and $\Delta P = (\Delta p_0, \Delta p_1 \ldots, \Delta p_n) = P_0 - P_1$. On the other hand, by (6), we have

$$\sum_{j=0}^{n} \Delta p_j = \sum_{j=0}^{n} p_{j,0} - \sum_{j=0}^{n} p_{j,1} = 1 - 1 = 0 \quad (9)$$

and α' is described as

$$\alpha' = \sum_{j=0}^{n} p_{j,0}\left(\frac{j}{n}\right)^t - \sum_{j=0}^{n} p_{j,1}\left(\frac{j}{n}\right)^t = \sum_{j=0}^{n} \Delta p_j \left(\frac{j}{n}\right)^t > 0. \quad (10)$$

D. The (t, ∞) PrVC Scheme With Optimal Contrast

In this section, we focus on the construction of the (t, ∞) PrVC scheme with optimal contrast. For convenience, the abbreviation (t, ∞) OptPrVC scheme is used to denote the (t, ∞) PrVC scheme with optimal contrast.

Lemma 2: For P_0 and P_1 of (t, ∞) OptPrVC scheme, if $p_{j,0} > 0$, then $p_{j,1} = 0$; and if $p_{j,1} > 0$, then $p_{j,0} = 0$.

Proof: Suppose $P'_0 = (p'_{0,0}, p'_{1,0}, \ldots, p'_{l,0}, \ldots, p'_{n,0})$ and $P'_1 = (p'_{0,1}, p'_{1,1}, \ldots, p'_{l,1}, \ldots, p'_{n,1})$ are the (t, ∞) OptPrVC scheme with the optimal contrast $\widehat{\alpha}'$ but $\exists l : p'_{l,0} > 0$ and $p'_{l,1} > 0$. Thus, for $i \in \{0, 1\}$, P'_i satisfies (6)(8)(10) which are described as

$$\sum\nolimits_{j=0}^{n} p'_{j,i} = 1 \quad (11)$$

$$\sum\nolimits_{j=0}^{n} (p'_{j,0} - p'_{j,1})\left(\frac{j}{n}\right)^k = 0 \ \forall k = 1, 2, \ldots, t-1 \quad (12)$$

$$\widehat{\alpha}' = \sum\nolimits_{j=0}^{n} (p'_{j,0} - p'_{j,1})\left(\frac{j}{n}\right)^t > 0. \quad (13)$$

Then, a new scheme $P''_i = (p''_{0,i}, p''_{1,i}, \ldots, p''_{n,i})$ with contrast $\widehat{\alpha}''$ is constructed by the following steps. First, calculate $p^{\min} = \min\{p'_{l,0}, p'_{l,1}\}$; second, construct P''_i and each term $p''_{j,i}$ is

$$p''_{j,i} = \begin{cases} \frac{(p'_{l,i} - p^{\min})}{(1-p^{\min})}, & \text{if } j = l \\ \frac{p'_{j,i}}{(1-p^{\min})}, & \text{otherwise.} \end{cases}$$

To verify that P''_i satisfies (6), substituting P''_i in (6), we obtain

$$\sum\nolimits_{j=0}^{n} p''_{j,i} = \frac{p'_{l,i} - p^{\min}}{1-p^{\min}} + \sum\nolimits_{j=0, j\neq l}^{n} \frac{p'_{j,i}}{1-p^{\min}} = \frac{-p^{\min}}{1-p^{\min}} + \frac{\sum_{j=0}^{n} p'_{j,i}}{1-p^{\min}} = 1.$$

To verify the security condition in Definition 2, for $k = 1, 2, \ldots, t-1$, substituting P''_i in (8), we obtain

$$\begin{aligned} &\sum\nolimits_{j=0}^{n} (p''_{j,0} - p''_{j,1})\left(\frac{n}{n}\right)^k \\ &= \left(\frac{p'_{l,0} - p^{\min}}{1-p^{\min}} - \frac{p'_{l,1} - p^{\min}}{1-p^{\min}}\right)\left(\frac{l}{n}\right)^k \\ &\quad + \sum\nolimits_{j=0, j\neq l}^{n} \left(\frac{p'_{j,0}}{1-p^{\min}} - \frac{p'_{j,1}}{1-p^{\min}}\right)\left(\frac{j}{n}\right)^k \\ &= (1-p^{\min})^{-1} \sum\nolimits_{j=0}^{n} (p'_{j,0} - p'_{j,1})\left(\frac{j}{n}\right)^k \\ &= (1-p^{\min})^{-1} \times 0 = 0. \end{aligned} \quad (14)$$

The result of (14) equal to 0 is obtained by the using result of (12). To verify the contrast condition in Definition 2, substituting P''_i in (10), we obtain

$$\begin{aligned} \widehat{\alpha}'' &= \sum\nolimits_{j=0}^{n} (p''_{j,0} - p''_{j,1})\left(\frac{j}{n}\right)^t \\ &= (1-p^{\min})^{-1} \sum\nolimits_{j=0}^{n} (p'_{j,0} - p'_{j,1})\left(\frac{j}{n}\right)^t \\ &> \sum\nolimits_{j=0}^{n} (p'_{j,0} - p'_{j,1})\left(\frac{j}{n}\right)^t = \widehat{\alpha}'. \end{aligned} \quad (15)$$

The contrast $\widehat{\alpha}''$ is larger than $\widehat{\alpha}'$ since $(1-p^{\min})^{-1}$ is larger than 1. Hence we obtain that P''_i has better contrast than P'_i, which incurs contradiction. ■

A similar result of Lemma 2 for finite n had been pointed out by previous work [12]. Lemma 2 gives an immediate mapping from ΔP to P_0 and P_1 which is described as

$$(p_{j,0}, p_{j,1}) = \begin{cases} (\Delta p_j, 0), & \text{if } \Delta p_j > 0 \\ (0, -\Delta p_j), & \text{if } \Delta p_j < 0 \\ (0, 0), & \text{if } \Delta p_j = 0 \end{cases} \quad (16)$$

$$\sum\nolimits_{j=0}^{n} |\Delta p_j| = 2. \quad (17)$$

Lemma 3: For (t, ∞) OptPrVC scheme, there is a ΔP consisting of $t+1$ nonzero values and $n-t$ zeros.

Proof: By (8), (9), (10), and (17), a linear program to achieve the optimal contrast is described as

$$\text{Maximize}: \quad \alpha' = \sum\nolimits_{j=0}^{n} \Delta p_j \left(\frac{j}{n}\right)^t \quad (18)$$

$$\text{Subject to}: \quad \sum\nolimits_{j=0}^{n} |\Delta p_j| = 2 \quad (19)$$

$$\sum\nolimits_{j=0}^{n} \Delta p_j = 0 \quad (20)$$

$$\sum\nolimits_{j=0}^{n} \Delta p_j \left(\frac{j}{n}\right)^k = 0 \quad \forall k = 1, 2, \ldots, t-1. \quad (21)$$

In order to remove the absolute symbols in (19), we divide the feasible region into 2^{n+1} subregions according to the sign of each Δp_j. Then the above linear program is divided into 2^{n+1} subproblems, expressed as

$$\text{Maximize}: \quad \alpha' = \sum\nolimits_{j=0}^{n} \Delta p_j \left(\frac{j}{n}\right)^t \quad (22)$$

$$\text{Subject to}: \sum\nolimits_{j=0}^{n} (g_j \Delta p_j) = 2 \quad (23)$$

$$\sum\nolimits_{j=0}^{n} \Delta p_j = 0 \quad (24)$$

$$\sum\nolimits_{j=0}^{n} \Delta p_j \left(\frac{j}{n}\right)^k = 0 \ \forall k = 1, 2, \ldots, t-1 \quad (25)$$

$$(g_j \Delta p_j) \geq 0 \ \forall j = 0, 1, \ldots, n \quad (26)$$

where $g_j = \pm 1$ is the sign of Δp_j in each subregion. There are one formula (23), one formula (24), and $t-1$ formulas (25)

as the constraints of the linear program, and those formulas are linearly independent as long as the subregion is not empty, and the maximal α' lies at the boundary sets (26). Thus, ΔP consists of $t+1$ nonzero values and $n-t$ zeros. ■

Since the $t+1$ nonzero terms in ΔP represent the critical values, those nonzero terms are recorded by two vectors $X = (x_0, x_1, \ldots, x_t)$ and $Y = (y_0, y_1, \ldots, y_t)$, where $|y_i|$ is the probability of using the memoryless sequence $E(x_i)$ to encode the secret pixel s taken from the secret image S, with $y_i > 0$ for $s =$ white and $y_i < 0$ for $s =$ black. Without loss of generality, X is arranged in increasing order (i.e., $x_i < x_{i+1}$). In other words, the ith nonzero term Δp_j is recorded in x_i and y_i such that $x_i = j/n$ and $y_i = \Delta p_j$. The equations of x_i and y_i are described as

$$0 \le x_0 < x_1 < \cdots < x_t \le 1. \tag{27}$$

Example 2: For $H_0 = (0,1,0,0,2)$ and $H_1 = (2,0,0,1,0)$ obtained from Example 1, the P_0, P_1, ΔP, X, and Y are

$$P_0 = \left(0,\ \frac{1}{3},\ 0,\ 0,\ \frac{2}{3}\right),\ P_1 = \left(\frac{2}{3},\ 0,\ 0,\ \frac{1}{3},\ 0\right)$$
$$\Delta P = \left(-\frac{2}{3},\ \frac{2}{3},\ 0, -\frac{1}{3},\ \frac{1}{3}\right)$$
$$X = \left(\frac{0}{4},\ \frac{1}{4},\ \frac{3}{4},\ \frac{4}{4}\right),\ Y = \left(-\frac{2}{3},\ \frac{2}{3}, -\frac{1}{3},\ \frac{1}{3}\right).$$

■

By (8), (9), and (10), the $(t+1)$ equations substituted with X and Y are expressed as

$$\sum\nolimits_{j=0}^{t} y_j x_j^k = 0 \quad \forall k = 1, 2, \ldots, t-1 \tag{28}$$

$$\sum\nolimits_{j=0}^{t} y_j = 0 \tag{29}$$

$$\alpha' = \sum\nolimits_{j=0}^{t} y_j x_j^t. \tag{30}$$

Then, (28)–(30) are expressed in the matrix form as

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_t \\ \vdots & \vdots & \ddots & \vdots \\ x_0^t & x_1^t & \cdots & x_t^t \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_t \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \alpha' \end{bmatrix}. \tag{31}$$

The $(t+1) \times (t+1)$ matrix M is the transpose of a Vandermonde matrix. By the property of $M^{-1} = ((M^T)^{-1})^{\mathrm{T}}$, we use the inverse Vandermonde matrix to obtain M^{-1}. In fact, the coefficients of inverse Vandermonde matrix can be expressed as Lagrange polynomials[30]. We fill M^{-1} with those coefficients to obtain

$$\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_t \end{bmatrix} = \begin{bmatrix} \bullet & \cdots & \left(\prod_{j=0, j\neq 0}^{t} (x_0 - x_j)\right)^{-1} \\ \bullet & \cdots & \left(\prod_{j=0, j\neq 1}^{t} (x_1 - x_j)\right)^{-1} \\ \vdots & \ddots & \vdots \\ \bullet & \cdots & \left(\prod_{j=0, j\neq t}^{t} (x_t - x_j)\right)^{-1} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \alpha' \end{bmatrix} \tag{32}$$

where $\bullet$ are don't-care terms, since those values will be multiplied by zeros in the later stage. Then y_i is described as

$$y_i = \alpha' \left(\prod\nolimits_{j=0, j\neq i}^{t} (x_i - x_j)\right)^{-1}. \tag{33}$$

Lemma 4: For an (t, ∞) OptPrVC scheme, if $t+i$ is even, then $y_i > 0$; otherwise, if $t+i$ is odd, then $y_i < 0$.

Proof: The result is easily verified by (33). ■

By Lemma 4, all values of y_i are grouped into two sets $\{y_i | t+i \in \text{Even integer}\}$ and $\{y_i | t+i \in \text{Odd integer}\}$; and the sums of all elements in both set are 1 and -1, respectively. By (33), their mathematical formulations are expressed as

$$\sum_{j=0}^{\lfloor t/2 \rfloor} y_{2i} = \alpha' \sum_{i=0}^{\lfloor t/2 \rfloor} \left(\prod_{j=0, j\neq i}^{t} (x_{2i} - x_j) \right)^{-1} = (-1)^t \tag{34}$$

$$\sum_{j=0}^{\lfloor (t-1)/2 \rfloor} y_{2i+1} = \alpha' \sum_{i=0}^{\lfloor (t-1)/2 \rfloor} \left(\prod_{j=0, j\neq i}^{t} (x_{2i+1} - x_j) \right)^{-1} = (-1)^{t+1}. \tag{35}$$

By (34) and (35), α' is expressed as

$$\alpha' = (-1)^t \left[\sum\nolimits_{i=0}^{\lfloor t/2 \rfloor} \left(\prod\nolimits_{j=0, j\neq i}^{t} (x_{2i} - x_j) \right)^{-1} \right]^{-1} = (-1)^{t+1} \left[\sum\nolimits_{i=0}^{\lfloor (t-1)/2 \rfloor} \left(\prod\nolimits_{j=0, j\neq i}^{t} (x_{2i+1} - x_j) \right)^{-1} \right]^{-1}. \tag{36}$$

Lemma 5: For the X of a (t, ∞) OptPrVC scheme, $x_0 = 0$ and $x_t = 1$.

Proof: Suppose (X', Y') is a (t, ∞) OptPrVC scheme but $x'_0 > 0$ or $x'_t < 1$. We generate a new (X'', Y'') where each term x''_j in X is

$$x''_j = \begin{cases} 0, & \text{if } j = 0 \\ 1, & \text{if } j = t \\ x'_j, & \text{otherwise.} \end{cases}$$

Then the contrast of (X'', Y'') is better than (X', Y') by substituting X' and X'' in (36). ■

Finally, the optimization problem $L(t)$ is derived by combining (27) and (36) with Lemma 5. The optimization problem $L(t)$ is described as

$$\text{Minimize} : \alpha'^{-1} = (-1)^t \sum_{i=0}^{\lfloor t/2 \rfloor} \left(\prod_{j=0, j\neq i}^{t} (x_{2i} - x_j) \right)^{-1} = (-1)^{t+1} \sum_{i=0}^{\lfloor (t-1)/2 \rfloor} \left(\prod_{j=0, j\neq i}^{t} (x_{2i+1} - x_j) \right)^{-1} \tag{37}$$

$$\text{Subject to} : 0 = x_0 < x_1 < \cdots < x_t = 1. \tag{38}$$

The target function is the reciprocal of α'. Krause and Simon [20] proved that the contrast of (k, n) VC scheme is no less than $4^{-(t-1)}$, so the outcome of $L(t)$ is expected to be $4^{(t-1)}$.

TABLE I
(X, Y) OF SOME (t, ∞) OPTPRVC SCHEMES FOR $2 \le t \le 6$

t	X and Y	α'
2	Y=(1/2, −1,1/2) X=(0,1/2,1)	4^{-1}
3	Y=(−1/3,2/3, −2/3,1/3) X=(0,1/4,3/4,1)	4^{-2}
4	Y=(1/4, −1/2,1/2, −1/2,1/4) X=$(0, (2-\sqrt{2})/4, 1/2, (2+\sqrt{2})/4, 1)$	4^{-3}
5	Y=(−1/5,2/5, −2/5,2/5, −2/5,1/5) $X = (0, (3-\sqrt{5})/8, (5-\sqrt{5})/8,$ $(3+\sqrt{5})/8, (5+\sqrt{5})/8, 1)$	4^{-4}
6	Y=(1/6, −1/3,1/3, −1/3,1/3, −1/3,1/6) X=$(0, (2-\sqrt{3})/4, 1/4, 1/2, 3/4, (2+\sqrt{3})/4, 1)$	4^{-5}

We use Maple to solve $L(t)$ for $2 \le t \le 6$, and the results are listed in Table I.

E. Encoding Algorithm

For a given value of t, the transparencies can be continuously generated with the (t, ∞) OptPrVC scheme. However, practical applications require the algorithm to terminate within finite steps. To meet the requirement, a finite number n' is used to specify the number of transparencies in the algorithm. The algorithm requires (X, Y), obtained by solving $L(t)$ or by looking up Table I. The outputs of Algorithm 1 are n' transparencies $T_1, T_2, \ldots, T'_n$ and an index table Z, where $Z[w, h]$ is the index of the used memoryless sequence $E(x_{Z[w,h]})$ to encode the secret pixel $s[w, h]$.

Algorithm 1. The algorithm of (t, ∞) OptPrVC scheme

Input: A binary secret image S, two positive integers t, n', and two vectors (X, Y).
Output: n' transparencies $T_1, T_2, \ldots, T'_n$; an index table Z.

1 **for** each pixel $s[w, h]$ in S **do**
2 **if** $s[w, h] =$ white **then**
3 Generate an integer $z \in \{t - 2k | k = 0, 1, \ldots, \lfloor t/2 \rfloor\}$ and $P(z = t - 2k) = y_{t-2k}$.
4 **else**
5 Generate an integer $z \in \{t - 1 - 2k | k = 0, 1, \ldots, \lfloor (t-1)/2 \rfloor\}$ and $P(z = t - 1 - 2k) = -y_{t-1-2k}$.
6 **end if**
7 $Z[w, h] = z$.
8 **for** $k = 1$ **to** n' **do**
9 Assign randomly $T_k[w, h]$ to 0 or 1 where $P(T_k[w, h] = 0) = x_z$.
10 **end for**
11 **end for**

In the first round, we use Algorithm 1 to generate n' transparencies and Z. If we need not to generate more transparencies in the future, Z is not required and discarded. Otherwise, Z has to be stored in a safe place, and we can generate more transparencies $T'_1, T'_2, \ldots, T'_{n''}$ by utilizing Z.

Fig. 1. Binary secret image.

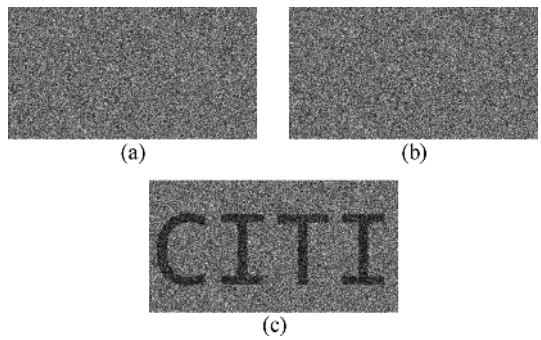

Fig. 2. Results of $(2, \infty)$ OptPrVC scheme. (a) T_1. (b) T_2. (c) $T_1 \oplus T_2$.

Algorithm 2. The algorithm of (t, ∞) OptPrVC scheme by the index table Z

Input: An index table Z, a positive integer n'', and a vector X.
Output: n'' transparencies $T'_1, T'_2, \ldots, T'_{n''}$.

1 **for** each $z[w, h]$ in Z **do**
2 **for** $k = 1$ **to** n'' **do**
3 Assign randomly $T'_k[w, h]$ to 0 or 1 where $P(T'_k[w, h] = 0) = x_z$.
4 **end for**
5 **end for**

III. EXPERIMENTAL RESULTS

Three experiments are performed for $t = 2, 3$, and 4. Fig. 1 shows the binary secret image S. Fig. 2 shows the first experiment for $t = 2$. Fig. 2(a)–(b) shows two generated transparencies T_1 and T_2, and the stacking result $T_1 \oplus T_2$ is shown in Fig. 2(c). We observe that the characters on the stacking result are clear. Based on Lemma 1, we verify the security and contrast of the three experiments. We use $T_{i_1}, T_{i_2}, \ldots, T_{i_k}$ to indicate any k generated transparencies with the proposed scheme, and t_{i_j} is a pixel at T_{i_j} and the position corresponds to the secret pixel s.

For a single transparency T_{i_1}, the probabilities of a white secret pixel appearing zero and a black secret pixel appearing zero are

$$P(t_{i_1} = 0 | s = \text{white}) = 0 \times 1/2 + 1 \times 1/2 = 1/2,$$
$$P(t_{i_1} = 0 | s = \text{black}) = 1 \times 1/2 = 1/2.$$

Therefore, the white pixels and black pixels cannot be distinguished by observing only one transparency. In the case where two transparencies are stacked $T_{i_1} \oplus T_{i_2}$, the contrast

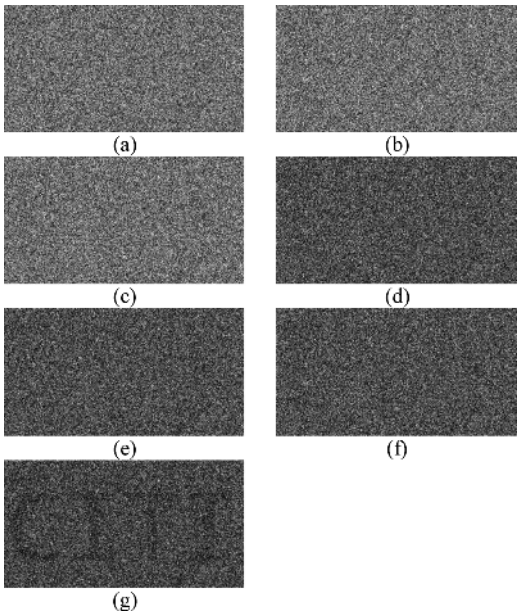

Fig. 3. Results of $(3,\infty)$ OptPrVC scheme. (a) T_1. (b) T_2. (c) T_3. (d) $T_1 \oplus T_2$. (e) $T_1 \oplus T_3$. (f) $T_2 \oplus T_3$. (g) $T_1 \oplus T_2 \oplus T_3$.

verification is

$$P(t_{i_1} \oplus t_{i_2} = 0 | s = \text{white}) = 0 \times (1/2)^2 + 1 \times (1/2)^2 = 1/2,$$
$$P(t_{i_1} \oplus t_{i_2} = 0 | s = \text{black}) = 1 \times (1/2)^2 = 1/4.$$

Thus, the contrast is $\alpha' = 1/2 - 1/4 = 1/4$.

Fig. 3 shows the second experiment for $t = 3$. Fig. 3(a)–(c) show three generated transparencies T_1, T_2, and T_3, and Fig. 3(d)–(f) show the results of stacking any two transparencies $T_1 \oplus T_2$, $T_1 \oplus T_3$, and $T_2 \oplus T_3$. Fig. 3(g) is the result of stacking the three transparencies $T_1 \oplus T_2 \oplus T_3$, and we can see contours of the secret on stacking result. The verifications of security and contrast are described as follows.

For a single transparency T_{i_1}, the security verification is

$$P(t_{i_1} = 0 | s = \text{white}) = 2/3 \times 1/4 + 1/3 \times 1 = 1/2,$$
$$P(t_{i_1} = 0 | s = \text{black}) = 1/3 \times 0 + 2/3 \times 3/4 = 1/2.$$

In the case where arbitrary two transparencies are stacked $T_{i_1} \oplus T_{i_2}$, the security verification is

$$P(t_{i_1} \oplus t_{i_2} = 0 | s = \text{white}) = 2/3 \times (1/4)^2 + 1/3 \times 1^2 = 3/8,$$
$$P(t_{i_1} \oplus t_{i_2} = 0 | s = \text{black}) = 1/3 \times 0^2 + 2/3 \times (3/4)^2 = 3/8.$$

In the case where arbitrary three transparencies are stacked $T_{i_1} \oplus T_{i_2} \oplus T_{i_3}$, the contrast verification is

$$P(t_{i_1} \oplus t_{i_2} \oplus t_{i_3} = 0 | s = \text{white}) = \frac{2}{3} \times \left(\frac{1}{4}\right)^3 + \frac{1}{3} \times 1^3 = \frac{11}{32},$$
$$P(t_{i_1} \oplus t_{i_2} \oplus t_{i_3} = 0 | s = \text{black}) = \frac{1}{3} \times 0^3 + \frac{2}{3} \times \left(\frac{3}{4}\right)^3 = \frac{9}{32}.$$

Thus, the contrast is $\alpha' = 11/32 - 9/32 = 1/16$.

Fig. 4 shows the third experiment for $t = 4$. Fig. 4(a)–(d) show four generated transparencies T_1, T_2, T_3, and T_4. It is noted that we skip the stacking results of arbitrary two or three transparencies due to the large number of combinations. Fig. 4(e) shows the stacking result $T_1 \oplus T_2 \oplus T_3 \oplus T_4$, where

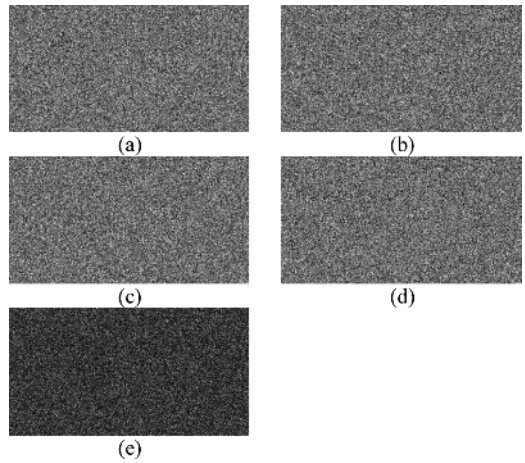

Fig. 4. Results of $(4,\infty)$ OptPrVC scheme. (a) T_1. (b) T_2. (c) T_3. (d) T_4. (e) $T_1 \oplus T_2 \oplus T_3 \oplus T_4$.

the characters on the stacking result are barely visible. The verifications of security and contrast are described as follows.

For a single transparency T_{i_1}, the security verification is

$$P(t_{i_1} = 0 | s = \text{white}) = 0 \times \frac{1}{4} + \frac{1}{2} \times \frac{1}{2} + \frac{1}{4} \times 1 = \frac{1}{2},$$
$$P(t_{i_1} = 0 | s = \text{black}) = \frac{1}{2} \times \frac{(2-\sqrt{2})}{4} + \frac{1}{2} \times \frac{(2+\sqrt{2})}{4} = \frac{1}{2}.$$

In the case where two transparencies are stacked $T_{i_1} \oplus T_{i_2}$, the security verification is

$$P(t_{i_1} \oplus t_{i_2} = 0 | s = \text{white}) = 1/4 \times 0^2 + 1/2 \times (1/2)^2 + 1/4 \times 1^2 = 3/8,$$
$$P(t_{i_1} \oplus t_{i_2} = 0 | s = \text{black}) = 1/2 \times \left((2-\sqrt{2})/4\right)^2 + 1/2 \times \left((2+\sqrt{2})/4\right)^2 = 3/8.$$

In the case where three transparencies are stacked $T_{i_1} \oplus T_{i_2} \oplus T_{i_3}$, the security verification is

$$P(t_{i_1} \oplus t_{i_2} \oplus t_{i_3} = 0 | s = \text{white}) = 1/4 \times 0^3 + 1/2 \times (1/2)^3 + 1/4 \times 1^3 = 5/16,$$
$$P(t_{i_1} \oplus t_{i_2} \oplus t_{i_3} = 0 | s = \text{black}) = 1/2 \times \left((2-\sqrt{2})/4\right)^3 + 1/2 \times \left((2+\sqrt{2})/4\right)^3 = 5/16.$$

In the case where four transparencies are stacked $T_{i_1} \oplus T_{i_2} \oplus T_{i_3} \oplus T_{i_4}$, the contrast verification is

$$P(t_{i_1} \oplus t_{i_2} \oplus t_{i_3} \oplus t_{i_4} = 0 | s = \text{white}) = 1/4 \times 0^4 + 1/2 \times (1/2)^4 + 1/4 \times 1^4 = 9/32,$$
$$P(t_{i_1} \oplus t_{i_2} \oplus t_{i3} \oplus t_{i_4} = 0 | s = \text{black}) = 1/2 \times \left((2-\sqrt{2})/4\right)^4 + 1/2 \times \left((2+\sqrt{2})/4\right)^4 = 17/64.$$

Thus, the contrast is $9/32 - 17/64 = 1/64$.

IV. Discussions and Applications

A. Addition and Deletion of Users in the Dynamic User Group

Since the proposed scheme allows dynamic changes of users in the user group, the operations to add and delete users are elaborated in this section. For the addition of n'' new participants to

TABLE II
OPTIMAL CONTRAST (t, n) VC SCHEMES FOR $2 \leq t \leq 4$

t/n	2	3	4	5	6	7	8	...	50	...	100	...	∞
2	1/2	1/3	1/3	3/10	3/10	2/7	2/7		25/98		25/99		1/4
3		1/4	1/6	1/8	1/10	1/10	2/21		13/196		625/9702		1/16
4			1/8	1/15	1/18	3/70	3/80		1161/65800		425/25608		1/64

the user group with n' original participants, the transparencies need to be able to accommodate the new $n = n' + n''$ users. In the case where the n' original transparencies are produced through the traditional (t, n') VC scheme, the n' original transparencies need to be eliminated, and then the new set of $n' + n''$ transparencies need to be generated through the $(t, n' + n'')$ VC scheme. The frequent regeneration and redistribution of the whole set of transparencies consume huge computing and communication resources for a dynamically changing user group, and may lead to potential security risks if certain original transparencies are not discarded completely. For example in the case of $t = 2$, an original participant holding one of original $(2, n')$ VC transparencies and obtaining one of the new $(2, n' + n'')$ VC transparencies might potentially be able to decode the secret by stacking the two transparencies. In the applications with a known maximal number of participants $n^{\max}$, the better strategy is to apply the $(t, n^{\max})$ VC scheme to generate $n^{\max}$ transparencies; and each authorized participant is assigned a transparency. By applying the $(t, n^{\max})$ VC scheme, the addition and departure of users can be accommodated without frequent regeneration and redistributions of transparencies. However, in many applications, the $n^{\max}$ is unknown and applying a larger number as $n^{\max}$ is a feasible option to avoid the overflow of users over the $n^{\max}$. The proposed (t, ∞) OptPrVC scheme accommodates the addition and departure of users without the problem of user overflow. In addition, with very large $n^{\max}$, the contrast of the (t, ∞) OptPrVC scheme is similar to the $(t, n^{\max})$ VC scheme addressed in Section IV-B.

For the deletion of users, we suppose that n'' out of n' ($n'' < n'$) participants are to leave the user group. If the contrast is to be optimized, the n' original transparencies need to be eliminated, and the new $n' - n''$ transparencies need to be generated through the $(t, n' - n'')$ VC scheme; the process consumes computing and communication resources for a frequently changing user group. Another strategy is to retrieve the transparencies from the departing participants; those retrieved transparencies can be assigned to the new participants. For the proposed (t, ∞) OptPrVC scheme to accommodate the scenarios of departing users, the departing users can simply discard the transparencies, and the new transparencies for new users can simply be generated through Algorithm 2; the retrieval of the transparencies from the departing users is not required. The authentication and security of the retrieved transparencies present a more challenging problem and relevant studies can be found in [11] and [33].

B. Contrast Comparisons of the Proposed Scheme With Traditional (t, n) VC Schemes

In general, the contrast of the (t, ∞) OptPrVC scheme is lower than certain (t, n) VC schemes with a finite value of n. Nevertheless, if n is very large, the (t, ∞) OptPrVC has some advantages over the traditional (t, n) VC scheme. In this case, the contrast of using the (t, n) VC scheme is similar to the (t, ∞) OptPrVC scheme. The (t, n) VC schemes with optimal contrast for $2 \leq t \leq 4$ and various values of n are listed in Table II, which is duplicated for reference from [19], except for $n = \infty$. For $(t, n) = (2, 100)$, the contrast is $25/99 \approx 0.2525$ which is very closes to $1/4 = 0.25$. In addition, For $(t, n) = (3, 100)$, the contrast is $625/9702 \approx 0.064419$ which is also very closes to $1/16 = 0.0625$. Thus, the stacking results of (t, ∞) OptPrVC scheme and (t, n) VC scheme are very close to each other for large n. Fig. 5 is an example of the (2, 100) VC scheme based on probabilistic model with contrast 25/99. We can see similar qualities in Figs. 5(c) and 2(c). However, the traditional (t, n) VC scheme requires larger amounts of computations and memory space to construct basis matrices. A simple analysis is discussed as follows.

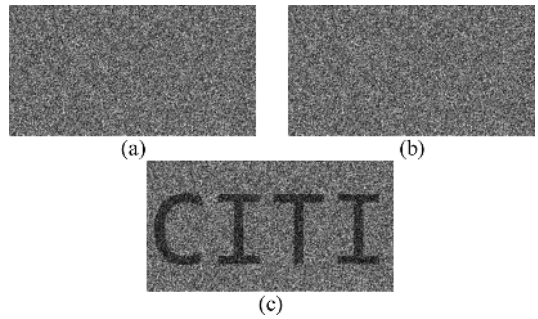

Fig. 5. Experimental result of (2, 100) PrVC. (a) T_1. (b) T_2. (c) $T_1 \oplus T_2$.

For two $n \times m$ basis matrices B_0 and B_1 of the traditional (t, n) VC scheme, the $2mn$ memory space is needed to store B_0 and B_1. To encode a secret pixel, first, the arithmetic sequence $1, 2, \ldots, m$ is permutated to obtain $d_1, d_2, \ldots, d_m$ with $\Theta(m)$ operations; second, each row of B_0 or B_1 is duplicated to the corresponding transparency, and the elements of each row are arranged by following the orders $d_1, d_2, \ldots, d_m$ with $\Theta(nm)$ I/O operations. Thus, the encoding includes $\Theta(m)$ computations and $\Theta(nm)$ I/O operations, and the $\Theta(nm)$ dominates the traditional (t, n) VC scheme due to the essentiality of the duplicating operations during the production of transparencies. It is noted that the encoding complexity is $\Theta(m)$ if the I/O operation is excluded from the complexity measure. On the other hand, the proposed probabilistic (t, n) VC scheme requires the values of two vectors X and Y, whose lengths are both $t + 1$. To encode a secret pixel, an n-element memoryless sequence is generated, which takes $\Theta(n)$ operations. The value of m depends on the construction method of B_0 and B_1. Blundo *et al.* [17] proved that a traditional $(2, n)$ VC scheme with $\alpha > 1/4$ holds the property $m \geq n - 1$. Thus, the space complexity and the time complexity of the $(2, n)$ VC scheme are both $\Theta(n^2)$. On the other hand, the proposed scheme takes $\Theta(t = 2) = \Theta(1)$ space and $\Theta(n)$ operations. Thus, the proposed method substantially reduces the computations and memory space for large n.

C. Comparisons of $L(t)$ With Two Linear Programs

Hofmeister *et al.* [19] provide an elegant linear program to calculate the optimal contrast of (t, n) VC scheme. In addition, the basis matrices can be constructed by the solution of the linear

TABLE III
COMPARISONS OF $L(t)$ WITH OTHER OPTIMIZATION EQUATIONS

	Hofmeister et al. [19]	Bose and Mukerjee [14]	The proposed $L(t)$
Goal	Calculate the optimal contrast of (t, n) VC schemes.	Calculate the optimal contrast of (t, n) VC schemes.	Calculate the optimal contrast of (t, ∞) VC schemes.
The contrast definition	Naor and Shamir [1]	Naor and Shamir [1]	Ito et al. [2]
The model	Basis matrices with the totally symmetric scheme	Basis matrices with the totally symmetric scheme	Probabilistic model
The number of variables	$2n+2$	$n-t$	$t-1$

program. We restate the linear program $M(t, n)$ as follows:

$$\text{Minimize}: \sum_{j=0}^{n-t} \frac{\binom{n-t}{j}}{\binom{n}{j}} \times (p_{j,0} - p_{j,1}) \tag{39}$$

$$\text{Subject to}: p_{j,0}, p_{j,1} \geq 0 \ \ \forall j = 0, 1, \ldots, n \tag{40}$$

$$\sum_{j=0}^{n} p_{j,0} = \sum_{j=0}^{n} p_{j,1} = 1 \tag{41}$$

$$\sum_{j=l}^{n-t+l+1} \frac{\binom{n-t+1}{j-l}}{\binom{n}{j}} \times (p_{j,0} - p_{j,1}) = 0 \ \ \forall l = 0, 1, \ldots, t-1. \tag{42}$$

$M(t, n)$ requires $2n + 2$ variables $\{p_{j,0} | j = 0, 1, \ldots, n\}$ to calculate the optimal contrast of (t, n) VC schemes. Obviously, for $n \to \infty$, (39)–(42) cannot be explicitly formulated due to the infinite terms of the sigma summation, so $M(t, \infty)$ is not computationally feasible. The proposed $L(t)$ is a specialized optimization problem under $n \to \infty$, and (37) and (38) are well formulated capable of solving the $t - 1$ variables $\{x_1, x_2, \ldots, x_{t-1}\}$. On the other hand, for a finite integer of n, $M(t, n)$ is more suitable than $L(t)$.

Moreover, Bose and Mukerjee [14] also provide the L_1-norm optimization equation to calculate the optimal contrast of the (t, ∞) VC scheme; the equation $N(t, n)$ is restated as follows:

$$\delta = \min_{p_n, p_{n-1}, \ldots, p_{t+1}} \left\{ \sum_{j=0}^{n} \left| q(j, n-t) - \sum_{k=0}^{n-t-1} q(j, k) p_{n-k} \right| \right\} \tag{43}$$

where $q(j, k) = (-1)^{j-k} \binom{n}{j} \binom{j}{n-k}$, and the contrast is given as $\alpha' = 2\delta^{-1}$. For $n \to \infty$, (43) also cannot be explicitly formulated due to the infinite terms of the sigma summation. Table III lists the comparisons.

D. Comparisons of the Proposed Method With RG Scheme

Table IV shows the comparisons of the (t, ∞) OptPrVC scheme with RGs [26]–[29]. Rather than the basis matrices, the size of RG's transparencies is identical to the secret image, and this property is similar to the proposed (t, ∞) OptPrVC scheme. It is noted that certain studies [26]–[29] propose various encoding algorithms to achieve various stacking results and contrasts, and therefore, the contrast is not unique. The definition of the contrast follows (4). The proposed (t, ∞) OptPrVC scheme is a generalized scheme for arbitrary t, and the contrast is optimal under the definition of Ito *et al.* [2]. In order to give a detailed comparison, Table V shows the $(2, n)$ RG proposed by Chen and Tsao [29]. As stated in [29], for a white secret pixel $s[w, h] =$ white, we have $P(T_k[w, h] = 0) = 1/2$,

TABLE IV
COMPARISONS OF THE (t, ∞) OPTPRVC SCHEME WITH RGS

Methods	Kafri and Keren [26]	Shyu [27]	Shyu [28]
(t, n)	(2, 2)	(2, 2)	(n, n)
Contrast	2^{-1} or 4^{-1}	2^{-1} or 4^{-1}	2^{1-n}, $(2^n+1)^{-1}$ or 2^{-n}

Methods	Chen and Tsao [29]		The (t, ∞) OptPrVC scheme
(t, n)	(n, n)	$(2, n)$	(t, ∞)
Contrast	2^{1-n},$(2^n+1)^{-1}$ or 2^{-n}	4^{-1}	4^{1-t}

TABLE V
ENCODING ALGORITHM OF $(2, n)$ RG SCHEME PROPOSED BY CHEN AND TSAO [29]

Input: A binary secret image S, and a positive integers n.
Output: n transparencies $T_1, T_2, \ldots, T_n$.

```
Create T1 by assigning each pixel to 0 or 1 and P(T1[w, h]=0)=1/2.
for k=2 to n do
    for each pixel s[w, h] in S do
        if s[w, h] = white then
            Tk[w, h] = Tk-1[w, h].
        end if
        if s[w, h] = black then
            Assign randomly Tk[w, h] to 0 or 1 where P(Tk[w, h]=0)=1/2.
        end if
    end for
end for
```

and $P(T_k[w, h] \oplus T_l[w, h] = 0) = 1/2$, $\forall k \neq l$; and for $s[w, h] =$ black, we have $P(T_k[w, h] = 0) = 1/2$, and $P(T_k[w, h] \oplus T_l[w, h] = 0) = 1/4$, $\forall k \neq l$. The probabilities are identical to Algorithm 1 for $t = 2$. Thus, the $(2, n)$ RG [29] performs the same distribution in generating transparencies through the Algorithm 1 for $t = 2$; and based on the observation, the proposed (t, ∞) OptPrVC scheme is also a generalized version of (t, n) RG for general t and unlimited n.

V. CONCLUSION

We have proposed a (t, n) VC scheme with flexible value of n. From the practical perspective, the proposed scheme accommodates the dynamic changes of users without regenerating and redistributing the transparencies, which reduces computation and communication resources required in managing the dynamically changing user group. From the theoretical perspective, the scheme can be considered as the probabilistic model of (t, n) VC with unlimited n. Initially, the proposed scheme is based on basis matrices, but the basis matrices with infinite size cannot be constructed practically. Therefore, the probabilistic

model is adopted in the scheme. As the results listed in Table I, the proposed scheme also provides the alternate verification for the lower bound proved by Krause and Simon [20]. For $t = 4$, the contrast 4^{-3} is very low so that the secret is visually insignificant. Therefore, in practical applications, the values of 2 or 3 for t are empirically suggested for the proposed scheme.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Advances in Cryptography (EUROCRYPT'94)*, 1995, vol. 950, LNCS, pp. 1–12.

[2] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Trans. Fundam. Electron., Commun., Comput. Sci.*, vol. 82, pp. 2172–2177, Oct. 1999.

[3] C. N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognit. Lett.*, vol. 25, pp. 481–494, Mar. 2004.

[4] S. J. Lin, S. K. Chen, and J. C. Lin, "Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion," *J. Vis. Commun. Image Represent.*, vol. 21, pp. 900–916, Nov. 2010.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Computat.*, vol. 129, no. 2, pp. 86–106, Sep. 1996.

[6] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010.

[7] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," *IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[8] Z. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[9] F. Liu, C. K. Wu, and X. J. Lin, "Colour visual cryptography schemes," *IET Inf. Security*, vol. 2, no. 4, pp. 151–165, Dec. 2008.

[10] G. Horng, T. Chen, and D. S. Tsai, "Cheating in visual cryptography," *Designs, Codes, Cryptography*, vol. 38, no. 2, pp. 219–236, Feb. 2006.

[11] C. M. Hu and W. G. Tzeng, "Cheating prevention in visual cryptography," *IEEE Trans. Image Process.*, vol. 16, no. 1, pp. 36–45, Jan. 2007.

[12] H. Koga, "A general formula of the (t, n)-threshold visual secret sharing scheme," in *Proc. 8th Int. Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology*, Dec. 2002, pp. 328–345.

[13] R. Z. Wang, "Region incrementing visual cryptography," *IEEE Signal Process. Lett.*, vol. 16, no. 8, pp. 659–662, Aug. 2009.

[14] M. Bose and R. Mukerjee, "Optimal (k, n) visual cryptographic schemes for general k," *Designs, Codes, Cryptography*, vol. 55, no. 1, pp. 19–35, Apr. 2010.

[15] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM J. Discrete Math.*, vol. 16, no. 2, pp. 224–261, Feb. 2003.

[16] M. Bose and R. Mukerjee, "Optimal $(2, n)$ visual cryptographic schemes," *Designs, Codes, Cryptography*, vol. 40, no. 3, pp. 255–267, Sep. 2006.

[17] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," *J. Cryptology*, vol. 12, no. 4, pp. 261–289, 1999.

[18] S. Cimato, R. De Prisco, and A. De Santis, "Optimal colored threshold visual cryptography schemes," *Designs, Codes, Cryptography*, vol. 35, no. 3, pp. 311–335, Jun. 2005.

[19] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," *Theoretical Comput. Sci.*, vol. 240, no. 2, pp. 471–485, Jun. 2000.

[20] M. Krause and H. U. Simon, "Determining the optimal contrast for secret sharing schemes in visual cryptography," *Combinatorics, Probability, Comput.*, vol. 12, no. 3, pp. 285–299, May 2003.

[21] E. R. Verheul and H. C. A. Van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," *Designs, Codes, Cryptography*, vol. 11, no. 2, pp. 179–196, May 1997.

[22] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," *Designs, Codes, Cryptography*, vol. 25, no. 1, pp. 15–61, 2002.

[23] F. Liu, C. K. Wu, and X. J. Lin, "A new definition of the contrast of visual cryptography scheme," *Inf. Process. Lett.*, vol. 110, no. 7, pp. 241–246, Mar. 2010.

[24] C. Blundo, S. Cimato, and A. De Santis, "Visual cryptography schemes with optimal pixel expansion," *Theoretical Comput. Sci.*, vol. 369, no. 1, pp. 169–182, Dec. 2006.

[25] H. Hajiabolhassan and A. Cheraghi, "Bounds for visual cryptography schemes," *Discrete Appl. Math.*, vol. 158, no. 6, pp. 659–665, Mar. 2010.

[26] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," *Opt. Lett.*, vol. 12, no. 6, pp. 377–379, Jun. 1987.

[27] S. J. Shyu, "Image encryption by random grids," *Pattern Recognit.*, vol. 40, no. 3, pp. 1014–1031, Mar. 2007.

[28] S. J. Shyu, "Image encryption by multiple random grids," *Pattern Recognit.*, vol. 42, no. 7, pp. 1582–1596, Jul. 2009.

[29] T. H. Chen and K. H. Tsao, "Visual secret sharing by random grids revisited," *Pattern Recognit.*, vol. 42, no. 9, pp. 2203–2217, Sep. 2009.

[30] N. Macon and A. Spitzbart, "Inverses of Vandermonde matrices," *Amer. Math. Monthly*, vol. 65, no. 2, pp. 95–100, Feb. 1958.

[31] C. N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognit. Lett.*, vol. 25, no. 4, pp. 481–494, Mar. 2004.

[32] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic visual cryptography schemes," *Computer J.*, vol. 49, no. 1, pp. 97–107, Jan. 2006.

[33] G. B. Horng, T. G. Chen, and D. S. Tsai, "Cheating in visual cryptography," *Designs, Codes, Cryptography*, vol. 38, no. 2, pp. 219–236, Feb. 2006.

Sian-Jheng Lin was born in Taiwan. He received the B.S., M.S., and Ph.D. degrees in computer science from National Chiao Tung University, in 2004, 2006, and 2010, respectively.

He is currently a postdoctoral fellow with the Research Center for Information Technology Innovation, Academia Sinica. His recent research interests include data hiding, error control coding, and secret sharing.

Wei-Ho Chung (M'11) was born in Kaohsiung, Taiwan, in 1978. He received the B.Sc. and M.Sc. degrees in electrical engineering from National Taiwan University, Taipei City, Taiwan, in 2000 and 2002, respectively, and the Ph.D. degree in the Electrical Engineering Department, University of California, Los Angeles (UCLA), in 2009.

From 2002 to 2005, he was a system engineer at ChungHwa TeleCommunications Company. From 2007 to 2009, he was a Teaching Assistant at UCLA. In 2008, he was a research intern working on CDMA systems in Qualcomm Inc. Since January 2010, he has been a faculty member holding the position of assistant research fellow in the Research Center for Information Technology Innovation, Academia Sinica, Taiwan. His research interests include wireless communications, signal processing, statistical detection and estimation theory, and networks.

Dr. Chung received the Taiwan Merit Scholarship, sponsored by the National Science Council of Taiwan, from 2005 to 2009.