Journal of Imaging Science and Technology® 52(6): 060508–060508-12, 2008.

Secret Image Sharing: DPVCS A Two-in-One Combination of (D)eterministic and (P)robabilistic (V)isual (C)ryptography (S)chemes

Ching-Nung Yang, An-Guo Peng and Tse-Shih Chen
Computer Science and Information Engineering Department, National Dong Hwa University, #1, Sec. 2, Da Hsueh Rd., Hualien, Taiwan
E-mail: cnyang@mail.ndhu.edu.tw

Abstract. *Visual cryptography scheme (VCS) is a secure method that encrypts a secret image by breaking it into shadow images. Due to the nature of encryption there are two types of VCS: one is the deterministic VCS (DVCS), and the other is the probabilistic VCS (PVCS). For the DVCS, we use m (known as the pixel expansion) subpixels to represent a secret pixel. The PVCS uses only one subpixel to represent a secret pixel, while the quality of reconstructed image is degraded. It is evident that one can combine both VCSs simultaneously over shadow images to develop their specialities: the DVCS retains the resolution and the PVCS considerably reduces the shadow size. This article has two main contributions: (1) the authors prove that this two-in-one VCS still satisfies the contrast and security conditions of VCS; (2) the authors show how to arrange subpixels with two different pixel expansions to retain the visual quality of reconstructed image. © 2008 Society for Imaging Science and Technology.*
[DOI: 10.2352/J.ImagingSci.Technol.(2008)52:6(060508)]

INTRODUCTION

For the (k,n)-threshold visual cryptography scheme (VCS), a secret image is encrypted into n shadow images (shadows) by expanding each secret pixel into m (known as the pixel expansion) subpixels. Any k participants may print shadows on transparencies and stack them on the overhead projector. Finally, one can visually decode the secret by the human visual system (HVS) without the help of hardware and computation. However, stacking $k-1$ or fewer shadows will not gain any information. This distinctive property of easy decoding can be used to securely and cheaply share the printed-text secret image, e.g., the password, where no computer assistance is available or desirable. The first VCS strategy was to encrypt the black-and-white secret image into noise-like shadows.[1] The authors used the whiteness (the number of white subpixels in a m-subpixel block) to distinguish the black color from white color, i.e., "$m-h$" B "h" W (respectively, "$m-l$" B "l" W) represents a white (respectively, black), where $h>l$. Afterwards, size-reduced VCSs schemes were proposed.[2–7] Some of them even had no pixel expansion (i.e., $m=1$); these schemes are known as the probabilistic VCS (PVCS).[5–7] The PVCS adopts the probabilistic strategy which uses different frequencies of whiteness in black and white areas to distinguish the color. The secret image can be reconstructed although the edge is blurred. The conventional VCS with the fixed m (>1), unlike the PVCS, is called the deterministic VCS (DVCS).

Generally, for processing gray or color secret images, a trivial solution is to convert the secret image into a binary image by the halftoning technique, and then process it using the black-and-white VCS.[8,9] Other VCSs for sharing the gray and chromatic secret images were subsequently proposed.[10–14] Lukac and Plataniotis introduced simple operations in the bit-plane for sharing the secret image without affecting its quality.[15,16] Other secret image sharing frameworks based on $(k-1)$-degree polynomials were proposed to reconstruct the original secret image.[17,18] However, they need complex computation, the Lagrange polynomial, to recover the secret. Lin and Tsai[19] embedded the shared bits and authentication bit in a 4-pixel block to achieve steganography and authentication simultaneously. Afterwards, Yang et al.[20] solved the authentication weakness in Ref. 19 to address the dishonest participant problem. Recently, Chang et al.[21] further enhanced this authentication ability by application of the Chinese remainder theorem. By using a specific dithering transformation, Jin, Yan, and Kankanhalli[22] designed a two-in-one VCS which has two decoding options. The first is stacking to get a vague reconstructed image like VCS, and the second is to reconstruct the perfect secret image by a dithering look-up table. However, the pixel expansion is $9m$. Lin and Lin[23] and Yang and Chen[24] combined VCS and polynomial-based secret sharing to design new two-in-one VCSs with the small pixel expansion. Due to the uniqueness of VCS (direct decoding by HVS) and more visual data in the modern visual communication, we believe that there will be more and more intended applications of VCS in the future. Up to now, the VSS technology has been adopted in many applications such as digital image indexing, watermarking, securing display, and embedding private information.[25–30]

Most researches on VCS are dedicated to find the minimum m and simultaneously maintain the contrast of the reconstructed image. DVCS and PVCS have their respective

Received Jan. 28, 2008; accepted for publication Jul. 14, 2008; published online Dec. 10, 2008.
1062-3701/2008/52(6)/060508/12/$20.00.

abilities. The DVCS provides good contrast for the reconstructed image, while the PVCS has a small shadow size. This article introduces the DPVCS by combining the DVCS and the PVCS to trade contrast for shadow size.

PRELIMINARIES

DVCS and PVCS

Our new scheme is a hybrid of DVCS and PVCS. Two VCSs are properly combined to develop their specialties and overcome their drawbacks. In this subsection we briefly describe these two elements of our new DPVCS.

The (k,n)-Threshold DVCS[1]

A black-and-white (k,n)-threshold DVCS can be designed using two black and white $n\times m$ base matrices, B_B and B_W, with elements "1" and "0" denoting black and white subpixels. When sharing a black (respectively, white) secret pixel, the dealer randomly chooses one row of the matrix in the set C_B (respectively, C_W) including all matrices obtained by permuting the columns in B_B (respectively, B_W) to a relative shadow. Let $\mathrm{OR}(B_B|r)$ (respectively, $\mathrm{OR}(B_W|r)$) denote the "OR"-ed r rows in B_B (respectively, B_W), and $H(\cdot)$ be the Hamming weight function. Then, a (k,n)-threshold DVCS should satisfy the following contrast and security conditions:

$$(\mathrm{D}-1)H(\mathrm{OR}\ (B_B|r)) \geqslant (m-l) \text{ and } H(\ \mathrm{OR}(B_W|r)) \leqslant (m-h)) \text{ for } r \geqslant k, \text{ where } 0 \leqslant l < h \leqslant m.$$

$$(\mathrm{D}-2)H(\mathrm{OR}\ (B_B|r)) = H(\mathrm{OR}(B_W|r)) \text{ for } r \leqslant (k-1).$$

The (k,n)-Threshold PVCS with No Pixel Expansion[6]

A black-and-white (k,n)-threshold PVCS can be designed using the black set C'_B and white set C'_W, including $n\times 1$ column Boolean matrices. When sharing a black (respectively, white) pixel, the dealer first randomly chooses one column matrix in C'_B (respectively, C'_W), and then selects the row of this column matrix to a relative shadow. Let $\mathrm{OR}(C'_B|r)$ (respectively, $\mathrm{OR}(C'_W|r)$) denote the sets of the OR-ed r rows in the column matrices of C'_B (respectively, C'_W), and $P(\cdot)$ be the appearance probabilities of the 0 (whiteness). The (k,n)-threshold PVCS is considered valid if the following contrast and security conditions are met: $(\mathrm{P}\text{-}1)P(\mathrm{OR}(C'_B|r)) \leqslant (p_{\mathrm{TH}}-\alpha)$ and $P(\mathrm{OR}(C'_W|r)) \geqslant p_{\mathrm{TH}}$ for $r \geqslant k$, where p_{TH} is a threshold probability and α is a relative difference.

$(\mathrm{P}\text{-}2)P(\mathrm{OR}(C'_B|r)) = P(\mathrm{OR}(C'_W|r))$ for $r \leqslant (k-1)$.

Example 1: Construct the (2, 2) DVCS and the (2, 2) PVCS, respectively. The secret is a printed-text image NDHU (National Dong Hwa University).

The (2, 2) DVCS of $(m,h,l)=(2,1,0)$ can be constructed using $B_1=\left[\begin{smallmatrix}10\\01\end{smallmatrix}\right]$ and $B_0=\left[\begin{smallmatrix}10\\10\end{smallmatrix}\right]$. It is observed that $H(\mathrm{OR}(B_B|2))=2$ and $H(\mathrm{OR}(B_W|2))=1$. So, the black color is 2B and the white color is 1B1W (or 1W1B) in the reconstructed image. Each shadow contains 1B1W or 1W1B with the same frequencies since $H(\mathrm{OR}(B_B|1))=H(\mathrm{OR}(B_W|1))=1$, and so that one cannot see anything from his own shadow.

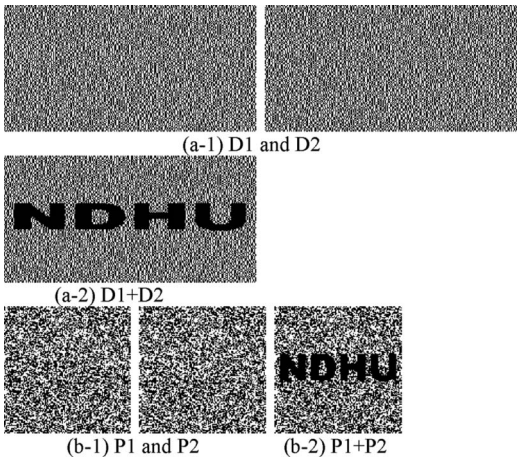

Figure 1. (2, 2) DVCS and (2, 2) PVCS; the secret image is a printed-text NDHU: (a) the DVCS: two shadows D1, D2 and the reconstructed image D1+D2, (b) the PVCS: two shadows P1, P2 and the reconstructed image P1+P2.

The (2, 2) PVCS of $p_{\mathrm{TH}}=0.5$ and $\alpha=0.5$ can be constructed using $C'_B=\{\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right],\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]\}$ and $C'_W=\{\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right],\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\}$. It is evident that $P(\mathrm{OR}(C'_B|2))=0$ and $P(\mathrm{OR}(C'_W|2))=0.5$ satisfy the contrast condition, and $P(\mathrm{OR}(C'_B|1))=P(\mathrm{OR}(C'_W|1))=0.5$ satisfies the security condition. Two shadows (D1 and D2) of DVCS and the reconstructed image (D1+D2) are shown in Figure 1(a). Figure 1(b) shows two shadows (P1 and P2) and the reconstructed image (P1+P2) for the PVCS. PVCS has no pixel expansion, i.e., the sizes of the shadow image and the secret image are the same, while the shadow size of DVCS doubles that of PVCS. However, the contrast of Fig. 1(b-2) is not compared with that of Fig. 1(a-2). The detailed edge of NDHU text in Fig. 1(b-2) is blurred.

The (k,n)-Threshold PVCS with Adjustable Pixel Expansion[7]

The PVCS in Ref. 6 has no pixel expansion, i.e., a single secret pixel is represented by a single subpixel. Cimato et al.[7] randomly choose $m' \in [1,m]$ columns to form the sets C''_B and C''_W. This strategy can adjust the pixel expansion between 1 to m for trading the shadow size with the contrast. Cimato et al.'s PVCS with m' is also a PVCS (see below and in Ref. 7).

Example 2: Construct Cimato et al.'s (2, 3) PVCS with adjustable $m' \in [1,3]$ using the base matrices

$$B_B=\begin{bmatrix}100\\010\\001\end{bmatrix} \quad \text{and} \quad B_W=\begin{bmatrix}100\\100\\100\end{bmatrix}$$

where $(m,h,l)=(3,2,1)$.

Cimato et al.'s (2, 3) PVCSs with $m'=1$ and 3 are the PVCS in Ref. 6 and the DVCS in Ref. 1, respectively. We could choose any two columns from B_B and B_W to construct C''_B and C''_W for Cimato et al.'s (2, 3) PVCS with $m'=2$ as follows:

$$C_B'' = \left\{ \begin{bmatrix} 10 \\ 01 \\ 00 \end{bmatrix}, \begin{bmatrix} 10 \\ 00 \\ 01 \end{bmatrix}, \begin{bmatrix} 00 \\ 10 \\ 01 \end{bmatrix} \right\}$$

and

$$C_W'' = \left\{ \begin{bmatrix} 10 \\ 10 \\ 10 \end{bmatrix}, \begin{bmatrix} 10 \\ 10 \\ 10 \end{bmatrix}, \begin{bmatrix} 00 \\ 00 \\ 00 \end{bmatrix} \right\}.$$

It can be easily verified that, $P(\mathrm{OR}(C_W''|2)) = 2/3 > P(\mathrm{OR}(C_B''|2)) = 1/3$ satisfy the contrast condition, and $P(\mathrm{OR}(C_B''|1)) = P(\mathrm{OR}(C_W''|1)) = 1/2$ satisfy the security condition. Cimato et al.'s (2, 3) PVCSs with $m' = 2$ is a compromise of the (2, 3) DVCS of $m = 3$ and (2, 3) PVCS of $m = 1$.

Motivation and Contribution

The goodness of a VCS is often measured in terms of the pixel expansion and the contrast. However, DVCS and PVCS have the opposite characteristics. DVCS achieves the high resolution of the reconstructed image but causes a large shadow size. Although PVCS has a small shadow, it yields a vagueness in visual quality in the reconstructed image. To make VCS more suitable for applications, it is reasonable to design a VCS with the capability that trades the contrast for the shadow size. There are two previous VCSs with this trading ability. One is Cimato et al.'s PVCS[7] (see above), and the other is the size-adjustable VCS (Ref. 31) which is a fusion of DVCS and the PVCS, described in Ref. 6. However, Cimato et al.'s PVCS loses the deterministic feature that a secret pixel is represented by the actual representation (all m subpixels of the original DVCS). The size-adjustable VCS proposed by Yang and Chen is suited only to the (k,k) and the soft-threshold $(k_L \sim k_U, n)$ VCSs. The soft-threshold scheme means that k-out-of-n may or may not reveal the secret when $k_L \leqslant k < k_U$, but the image is always recovered when $k \geqslant k_U$; no information is gained when $k < k_U$.

In this article, we also study the trading ability of VCS to provide for a trade-off between. By combining the DVCS and Cimato et al.'s PVCS in shadow images simultaneously, we design a hybrid DPVCS. Our scheme has better contrast than Cimato et al.'s PVCS, and is a general (k,n) scheme overcoming the weakness of size-adjustable VCS.

More in detail, our main contributions are summarized as follows.

- First, we propose a methodology that combines DVCS and PVCS.
- Second, we theoretically prove that the DPVCS satisfy (P-1) and (P-2) (contrast and security conditions) of PVCS. So our DPVCS still holds the property of VCS.
- Third, we give a contrast measurement when combing DVCS and PVCS.

THE PROPOSED (k,n)-THRESHOLD DPVCS

Design Concept

The different types of VCSs result in distinct characteristics. The pixel expansion of DVCS is fixed and large enough to represent the detail of secret image, while the pixel expansion of Cimato et al.'s PVCS is adjustable for reducing the shadow size. When combining DVCS and PVCS to deign our DPVCS, we should carefully consider the problem. *How to combine DVCS and PVCS?* Notice that the size-adjustable VCS in Ref. 31 also uses DVCS and PVCS. However, it is only a soft (k,n) VCS because it combines them by a hierarchical way. From this observation, we need to combine both VCSs in the shadow image simultaneously. At this time, the combination of DVCS and PVCS presents another problem: how to arrange the subpixels for DVCS and PVCS in shadows such that they perform the appropriate roles, i.e., the DVCS improves the contrast and the PVCS reduces the shadow size.

Let the pixel expansions of the DVCS and PVCS be m and m', respectively. To make sure these subpixels with different m and m' can be arranged properly in shadow image, we define the following arrangements. Let the symbolic notation $\boxed{\mathrm{D}}$ (respectively, $\boxed{\mathrm{P}}$) represent the operation that encrypts m' (respectively, m) secret pixels by the DVCS (respectively, PVCS). For convenience, we also use the notations $\boxed{\mathrm{D}}$ and $\boxed{\mathrm{P}}$ to indicate the areas including subpixels. Then, proceed $\boxed{\mathrm{D}}$ and $\boxed{\mathrm{P}}$ alternately in the interlaced pattern (Figure 2(a-1)) or the regular pattern (Fig. 2(a-2)). Finally, there are $(100 \times m')/(m+m')\%$ secret pixels encrypted by the DVCS and $(100 \times m)/(m+m')\%$ secret pixels encrypted by the PVCS, respectively. Because $\boxed{\mathrm{D}}$ and $\boxed{\mathrm{P}}$ are all $(m \times m')$ subpixels, the corresponding locations of subpixels and the secret pixels can be matched exactly. Another arrangement for these subpixels with different m and m' uses the DVCS and the PVCS 50/50 in a shadow image. Notations $\boxed{\mathrm{D}_1}$ and $\boxed{\mathrm{P}_1}$ are alike, except encrypting a single secret pixels. Then, the interlaced and regular patterns for the operations of $\boxed{\mathrm{D}_1}$ and $\boxed{\mathrm{P}_1}$ are shown in Figs. 2(b-1) and (b-2). Also, $\boxed{\mathrm{D}_1}\boxed{\mathrm{P}_1}$ and $\boxed{\mathrm{P}_1}\boxed{\mathrm{D}_1}$ have $(m+m')$ subpixels, and then the arrangement can retain the co-locations between secret pixel and the subpixels.

It is evident that the average pixel expansion is $m \times m'/(m+m') + m' \times m/(m+m') = 2m'm/(m+m')$ when using $\boxed{\mathrm{D}}$ and $\boxed{\mathrm{P}}$. On the other hand, the average pixel expansion is $m \times 1/2 + m' \times 1/2 = (m+m')/2$ when using $\boxed{\mathrm{D}_1}$ and $\boxed{\mathrm{P}_1}$. All these patterns have the following features: (1) the DVCS operations $\boxed{\mathrm{D}}$ and $\boxed{\mathrm{D}_1}$ are located alternately or continuously in every row and every column; (2) these subpixels with two different pixel expansions are arranged in orderly fashion over the entire shadow; and (3) there are $(100 \times m)/(m+m')\%$ and 50% for $\boxed{\mathrm{P}}$ and $\boxed{\mathrm{P}_1}$, respectively. The first feature lets the DVCS can retain the actual representation (all m subpixels) in each direction. The second feature achieves a more relative position between the secret pixels and subpixels to avoid distortion. Both features enable the proposed DPVCS to provide high contrast. The latter feature reduces the shadow size.

Encoding Procedure of DPVCS

Encoding procedure of the (k,n)-threshold DPVCS is described as follows. Some notations are defined as:

I: The secret image with size $|I|$;

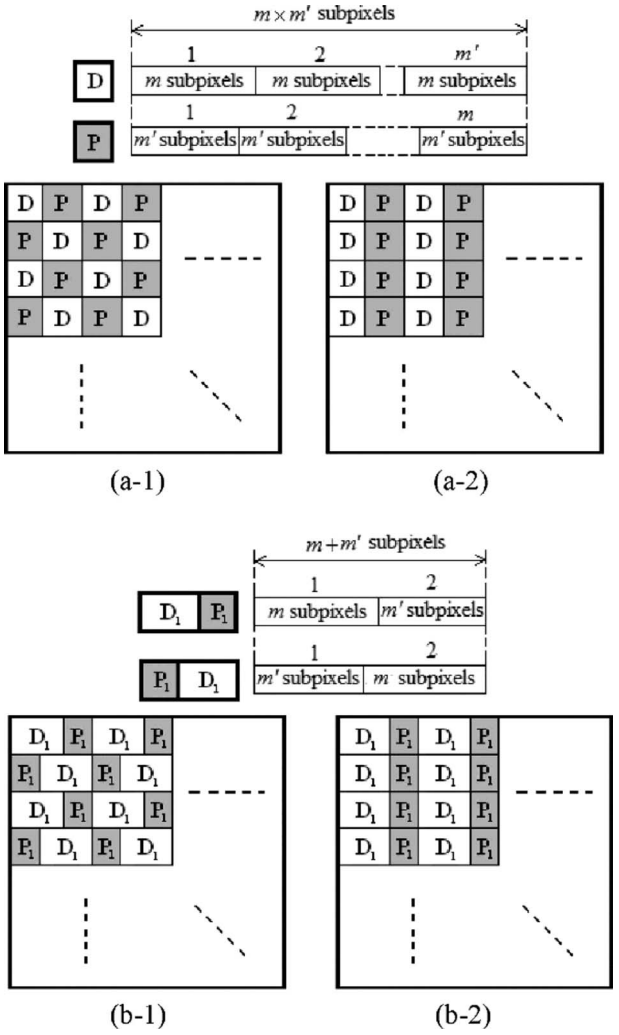

Figure 2. Arrange the subpixels generated from the DVCS and the PVCS alternately according: (a-1, b-1) the interlaced pattern, (a-2, b-2) the regular pattern.

IP: Use the interlaced pattern in Fig. 2(a-1) and apply the operations D and P;

RP: Use the regular pattern in Fig. 2(a-2) and apply the operations D and P;

IP_1: Use the interlaced pattern in Fig. 2(b-1) and apply the operations D_1 and P_1;

RP_1: Use the regular pattern in Fig. 2(b-2) and apply the operations D_1 and P_1;

S_i: The n output shadows with size $(2mm'/(m+m') \times |I|)$ when using IP and RP, or

$((m+m')/2 \times |I|)$ when using IP_1 and RP_1, $i \in [1,n]$.

Encoding Procedure

Input: I, m and m'.

Note that m' can be chosen from 1 to m; however, when choosing $m'=m$ DPVCS is reduced to DVCS.

Output: S_i, $i \in [1,n]$.

Step1: Choose one of the pattern: IP, RP, IP_1, or RP_1.

Step2: According the chosen pattern, encode the secret pixels by the operations D, P, D_1, and P_1.

Step3: Output S_i, $i \in [1,n]$.

Theorem: The proposed (k,n) DPVCS from the encoding procedure is a (k,n)-threshold VCS.

Proof: Our DPVCS scheme is a hybrid of the DVCS with m and Cimato's VCS with m' $(1 \leq m' \leq m)$. Because the DVCS is also Cimato's schemes with $m'=m$, the DPVCS can be considered as the combination of two Cimato's schemes with two different m'. Therefore, we only prove the DPVCS to satisfy the contrast and security conditions (P-1) and (P-2).

We first prove (P-1). When stacking r $(\geq k)$ shadows, we have $H(\mathrm{OR}(B_B|r)) \geq (m-l)$ and $H(\mathrm{OR}(B_W|r)) \leq (m-h)$ in the areas D and D_1. Then, the whiteness probabilities of the black color is calculated as

$$P(\mathrm{OR}(C_B|r)) = (m - H(\mathrm{OR}(B_B|r)))/m \leq (m-(m-l))/m = l/m. \quad (1a)$$

By the same approach, we have

$$P(\mathrm{OR}(C_W|r)) = (m - H(\mathrm{OR}(B_w|r)))/m \geq h/m. \quad (1b)$$

On the other hand, consider the areas P and P_1. Since Cimato's VCS with m' comes from DVCS with $H(\mathrm{OR}(B_B|r)) \geq (m-l)$ and $H(\mathrm{OR}(B_W|r)) \leq (m-h)$ by randomly choosing any m' columns. Therefore, a m-tuple vector of OR $(C''_B|r)$ contains $(\leq l)$ white subpixels and $(\geq m-l)$ black subpixels. Suppose a sample of m' elements is randomly selected from a m-tuple vector of OR $(C''_B|r)$. Let the random variable denote the number of whiteness is chosen in the sample. Then this random variable is a hypergeometric random variable with the probability density function $f(x) = \binom{l}{x}\binom{m-l}{m'-x} / \binom{m}{m'}$. Therefore, the whiteness probability of the black color can be determined as

$$\begin{aligned} P(\mathrm{OR}(C''_B|r)) &\leq \sum_{x=1}^{m'} (x/m') \times f(x) \\ &= \sum_{x=1}^{m'} (x/m') \times \binom{l}{x}\binom{m-l}{m'-x} \Big/ \binom{m}{m'} \\ &= 1/m' \times \sum_{x=1}^{m'} x \binom{l}{x}\binom{m-l}{m'-x} \Big/ \binom{m}{m'} \\ &= 1/m' \times (m' \times l/m) = l/m. \end{aligned} \quad (2a)$$

(Note: $\sum_{x=1}^{m'} x\binom{l}{x}\binom{m-l}{m'-x} / \binom{m}{m'} = (m' \times l/m)$ is the mean of the hypergeometric distribution).

By the same approach, we have

$$P(\mathrm{OR}(C''_W|r)) \geq h/m. \quad (2b)$$

From Eqs. (1a), (1b), (2a), and (2b), our DPVCS has the whiteness probabilities in the black area (respectively, white area) $\leq l/m$ (respectively, $\geq h/m$). Set $p_{\mathrm{TH}} = l/m$ and $\alpha = 0$, then the whiteness probabilities in DPVCS satisfy (P-1) when stacking r $(\geq k)$ shadows.

Next, we prove (P-2). In D and D_1. Suppose $H(\mathrm{OR}(B_B|r))=H(\mathrm{OR}(B_W|r))=(m-w)$ when stacking r ($\leqslant k-1$) shadows. Then, the whiteness probabilities $P(\mathrm{OR}(C_B|r))$ and $P(\mathrm{OR}(C_W|r))$ are calculated as

$$P(\mathrm{OR}(C_B|r)) = (m - H(\mathrm{OR}(B_B|r)))/m = (m-(m-w))/m = w/m, \quad (3a)$$

$$P(\mathrm{OR}(C_W|r)) = (m - H(\mathrm{OR}(B_W|r)))/m = w/m. \quad (3b)$$

Consider the areas P and P_1. Use the same approach of obtaining Eqs. (2a) and (2b); for the case the probability density function $f'(x)=\binom{w}{x}\binom{m-w}{m'-x}/\binom{m}{m'}$, and then the value of $P(\mathrm{OR}(C''_B|r))$ is calculated as

$$\begin{aligned} P(\mathrm{OR}(C''_B|r)) &= \sum_{x=1}^{m'} (x/m') \times f'(x) \\ &= \sum_{x=1}^{m'} (x/m') \times \binom{w}{s}\binom{m-w}{m'-x} \Big/ \binom{m}{m'} \\ &= 1/m' \times \sum_{x=1}^{m'} x\binom{w}{x}\binom{m-w}{m'-x} \Big/ \binom{m}{m'} \\ &= 1/m' \times (m' \times w/m) = w/m. \end{aligned} \quad (4a)$$

Since $H(\mathrm{OR}(B_W|r))=H(\mathrm{OR}(B_B|r))$, we also have

$$P(\mathrm{OR}(C''_W|r)) = (w/m). \quad (4b)$$

From Eqs. (3a), (3b), (4a), and (4b), our DPVCS has the same whiteness probabilities in the black and white areas when stacking r ($\leqslant k-1$) shadows. So the condition (P-2) is proved.

EXPERIMENT AND COMPARISON

Experimental Results

Three experiments are conducted to evaluate the performance of DPVCS. Experiment A shows the (2, 3)-threshold DPVCS using $(m,h,l)=(3,2,1)$ and four arrangement patterns IP, RP, IP_1, RP_1. Experiment B employs the (2, 3)-threshold DPVCS using $(m,h,l)=(3,1,0)$ to demonstrate the effects for different h, l, and m. The tested image in experiments A and B is a simple black/white printed-text NDHU. In experiment C we use a natural gray image *House* to test the proposed DPVCS. From these experimental results, we can also evaluate our ability to trade off between contrast and shadow size.

In the above experiments, we adopt the printer/print setting of 600 dpi, which is a common default setting for commercial laser printers. We photocopy each pattern on a separate transparency. Afterwards, we align them carefully, and project the result with an overhead projector to decrypt the secret message. We do not need to use the overhead projector in the decoding phase, as the secret image can still be visually revealed by directly stacking transparencies. The overhead projector is merely used to enhance the luminance for easy visualization. All experiments we do can be reproduced correctly when using the above approach. However, to speed up the viewing process, one can use a GIMP image editing tool instead of overhead projector to superimpose shadows, and visually decode the secret on screen. For simplicity, most papers on VCS have adopted the latter approach to show their experimental results.

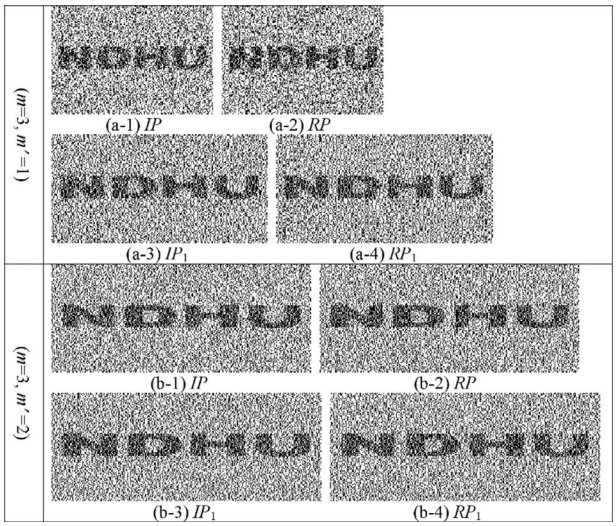

Figure 3. Reconstructed images of the (2, 3)-threshold DPVCS using $(m,h,l)=(3,2,1)$; four patterns, IP, RP, IP_1, RP_1, are tested; the secret image is a printed-text NDHU: (a-1, a-2) pixel expansion=1.5, (a-3, a-4) pixel expansion=2, (b-1, b-2) pixel expansion=2.4, (b-3, b-4) pixel expansion=2.5.

Experiment A: Construct the (2, 3)-threshold DPVCS using the base matrices

$$B_B = \begin{bmatrix} 100 \\ 010 \\ 001 \end{bmatrix} \quad \text{and} \quad B_W = \begin{bmatrix} 100 \\ 100 \\ 100 \end{bmatrix},$$

where $(m,h,l)=(3,2,1)$. Four patterns, IP, RP, IP_1, RP_1, are tested.

Since $m=3$ and $m' \in [1,3]$ if we choose $m'=3$ the DPVCS is reduce to the DVCS with $m=3$. Two combinations of pixel expansions are used: ($m=3$, $m'=1$) and ($m=3$, $m'=2$). Figures 3(a-1) and (a-2) show the reconstructed images using ($m=3$, $m'=1$) for the patterns IP and RP, respectively. The secret pixels encrypted by the DVCS and PVCS are $(100\times m')/(m+m')\%=25\%$ and $(100\times m)/(m+m')\%=75\%$. The average pixel expansion is 1.5 ($=3\times 25\%+1\times 75\%$). Figures 3(a-3) and (a-4) are the results for the patterns IP_1 and RP_1; there are half and half secret pixels encrypted by the DVCS and the PVCS and the average pixel expansion is 2 ($=3\times 50\%+1\times 50\%$). The reconstructed images using ($m=3$, $m'=2$) for these four arrangement patters are shown in Fig. 3(b). The pixel expansions are 2.4 (using IP and RP) and 2.5 (using IP_1 and RP_1). From experimental results, it is observed that the larger shadow has the clearer reconstructed image. Our DPVCS is provided with the trading capability.

Experiment B: Construct the (2, 3)-threshold DPVCS using the base matrices

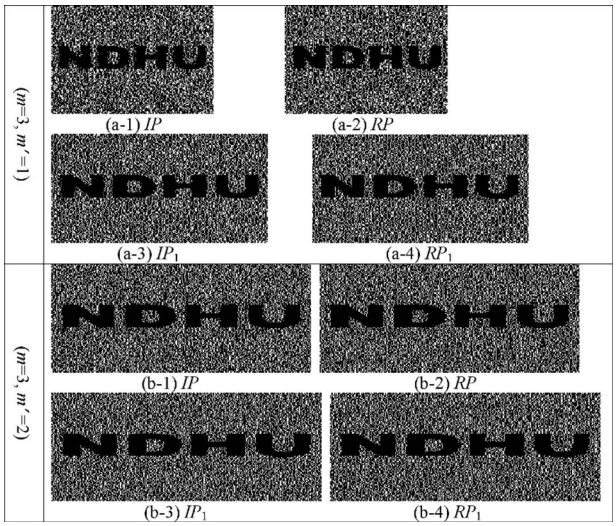

Figure 4. Reconstructed images of the (2, 3)-threshold DPVCS using $(m,h,l)=(3,1,0)$; four patterns, IP, RP, IP_1, RP_1, are tested; the secret image is a printed-text NDHU: (a-1, a-2) pixel expansion=1.5, (a-3, a-4) pixel expansion=12, (b-1, b-2) pixel expansion=2.4, (b-3, b-4) pixel expansion=2.5.

$$B_B=\begin{bmatrix}110\\011\\101\end{bmatrix} \quad \text{and} \quad B_W=\begin{bmatrix}110\\110\\110\end{bmatrix},$$

where $(m,h,l)=(3,1,0)$. Do the same test in experiment A.

Experiment B has the same pixel expansion as experiment A and achieves better contrast, owing to the whiteness "$l=0$" in experiment B, i.e., the black secret pixels are all represented as black subpixels. Here, we give a more in-depth discussion regarding the contrast. By the previous theoretical contrast definition $(h-l)/m$ in Ref. 1, the contrasts for the DVCS with $(m,h,l)=(3,1,0)$ and the DVCS with $(m,h,l)=(3,2,1)$ are all 1/3 (Figure 4). Subsequently, Eisen and Stinson[32] demonstrated that the definition in Ref. 1 is inadequate and gave a new one, $(h-l)/(m+l)$. According this new definition, the DVCS of $(m,h,l)=(3,1,0)$ has contrast 1/3, better than 1/4 of $(m,h,l)=(3,2,1)$. The inconsistency between these two definitions occurs due to personal, subjective opinion. However the case $l=0$, i.e., all black color, is more sensitive by HVS. Therefore, the definition $(h-l)/(m+l)$ is more suited to the real situation. The proposed DVPVCS is constructed from the DVCS and Cimato's PVCS which also comes from the DVCS. Therefore, the contrast for the DVCS of $(m,h,l)=(3,1,0)$ is better than for the DVCS of $(m,h,l)=(3,2,1)$, and it implies that the DPVCS in experiment B will have the better contrast than experiment A.

Experiment C: Use the natural image *House* to test both (2, 3)-threshold DPVCSs in experiments A and B.

Figures 5(a-1), 5(a-2), 5(b-1), 5(b-2) use the DPVCS $(m=3,\ h=2,\ l=1,\ m'=1)$ but Figs. 5(a-3), 5(a-4), 5(b-3), 5(b-4) use the DPVCS $(m=3,\ h=1,\ l=0,\ m'=1)$. Figures 5(c) and 5(d) are similar to Figs. 5(a) and 5(b), respectively, but use $m'=2$. It is observed that the DPVCS in experiment

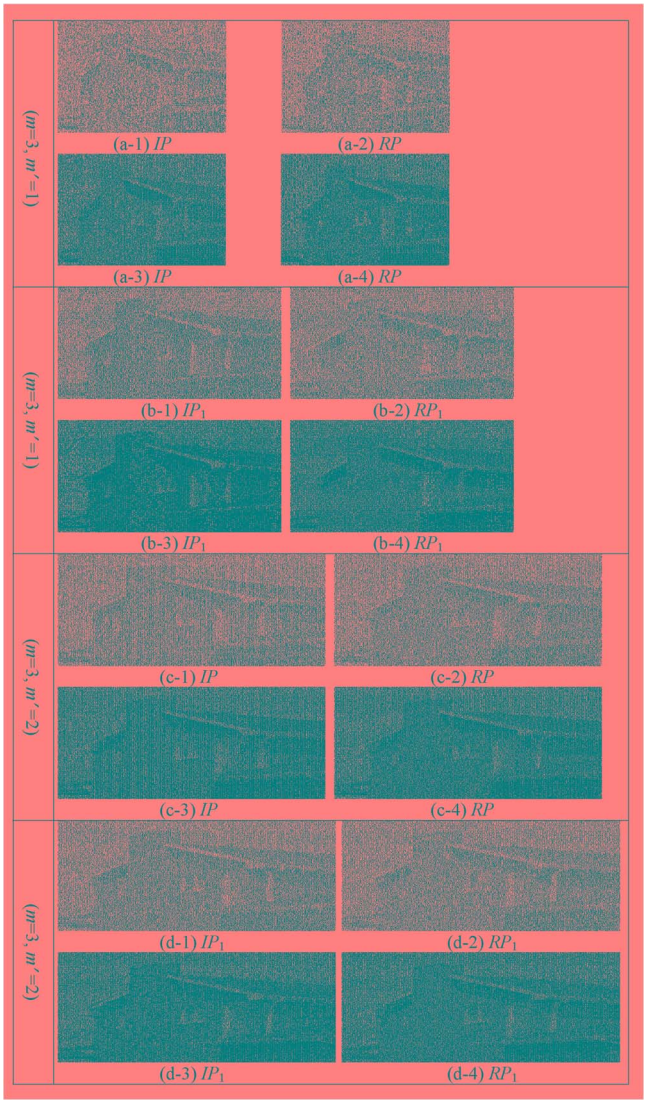

Figure 5. Reconstructed images of the (2, 3)-threshold DPVCS; the secret is a natural image House: (a-1, a-2, b-1, b-2) using $m=3$, $h=2$, $l=1$, $m'=1$, (a-3, a-4, b-3, b-4) using $m=3$, $h=1$, $l=0$, $m'=1$, (c-1, c-2, d-1, d-2) using $m=3$, $h=2$, $l=1$, $m'=2$, (c-3, c-4, d-3, d-4) using $m=3$, $h=1$, $l=0$, $m'=2$.

B ($l=0$) has better contrast than the DPVCS in experiment A ($l=1$). Which pattern is more capable of achieving high contrast is not absolute, e.g., the edges of *House* in Fig. 5(b-1) (using the interlaced pattern) is clearer than Fig. 5(b-2) (using the regular pattern), but Fig. 5(b-2) has more color levels in the shade of eaves. This observation is reasonable. When the shape, pattern, and resolution of the secret image just match the arrangement pattern, the reconstructed image may be clearer.

Comparison

It seems that the size-adjustable VCS in Ref. 31 is the first VCS combining DVCS and PVCS to trade-off between shadow size and contrast. Both VCSs are cascaded by a hierarchical operation $\succ$ which uses the output shadows of the previoius scheme as the input secret of the next scheme. Let $D_{(k_1,n_1)}$ and $P_{(k_2,n_2)}$ be the (k_1,n_1)-threshold DVCS and the (k_2,n_2)-threshold PVCS with the pixel expansion m and 1,

Table I. The pixel expansions for various VCSs for $m=10$ and $1 \leqslant m' \leqslant 10$.

(VCSs\m')	1	2	3	4	5	6	7	8	9	10
DVCS	10	10	10	10	10	10	10	10	10	10
PVCS[a]	1	1	1	1	1	1	1	1	1	1
Cimato *et al.*'s PVCS[b]	1	2	3	4	5	6	7	8	9	10
DPVCS using D and P	1.8	3.3	4.6	5.7	6.7	7.5	8.2	8.9	9.5	10
DPVCS using D_1 and P_1	5.5	6.0	6.5	7.0	7.5	8.0	8.5	9.0	9.5	10

[a]References 6 and 7.
[b]Reference 14.

respectively. A soft-threshold $(k_L \sim k_U, n)$ VCS is constructed by $D_{(k_1,n_1)} \succ P_{(k_2,n_2)}$, where $k_L = k_1 \times k_2, k_U = (k_1-1) \times n_2 + (n_1 - k_1 + 1) \times (k_2 - 1) + 1$ and $n = n_1 \times n_2$ (see Theorem 2 in Ref. 31). This term "soft" means that k-out-of-n may reveal the secret image or not when $k_L \leqslant k < k_U$, but always recovers the image when $k \geqslant k_U$ and no information is gained when $k < k_U$. When $n_2 = k_2$ and $n_1 = k_1$, the soft-threshold $(k_L \sim k_U, n)$ VCS is reduced to the (k,k) VCS where $k = k_1 \times k_2$. For example, $D_{(2,3)} \succ P_{(2,3)}$ and $D_{(2,2)} \succ P_{(3,3)}$ yield the (4–7, 9) VCS and (6, 6) VCS, respectively. This size-adjustable VCS is designed only for some values of k and n, and it is not a general (k,n)-threshold VCS, e.g., the (2, 3) VCS in our experiments cannot be implemented by this size-adjustable VCS. The proposed DPVCS is also a fusion of the DVCS and the PVCS, but we use here the direct combination instead of cascading. Suppose the notation $\perp$ designates direct combining for our DPVCS (described in the encoding procedure). The direct combination $\perp$ is used with the same (k,n) dimensions, i.e., $D_{(k,n)} \perp P_{(k,n)}$ yields the (k,n)-threshold DPVCS. Also, Cimato's PVCS $P_{(k,n)}$ is generated from $D_{(k,n)}$, and thus $D_{(k,n)} \perp P_{(k,n)}$ can construct any (k,n) DPVCS. Finally, we solve the problem of generality for size-adjustable VCS and provide the trade-off capability.

When compared to previous VCSs, we emphasize the most important characteristics of the VCS, the pixel expansion and the contrast, which are also the aims of the proposed DPVCS.

The Pixel Expansion

Let the pixel expansions for the DVCS, the PVCS with no expansion,[5,6] and Cimato's PVCS with adjustable pixel expansion[7] be m_D, m_P, m_C, respectively. Let the average pixel expansions for our DPVCS be $m_H^{(1)}$ and $m_H^{(2)}$ when using the operations (D, P) and (D_1, P_1). All these pixel expansions are: $m_D = m$; $m_P = 1$; $m_C = m'$ $(1 \leqslant m' \leqslant m)$; $m_H^{(1)} = 2m'm/(m+m')$; $m_H^{(2)} = (m+m')/2$. Table I lists these pixel expansions for the case $m=10$ and $1 \leqslant m' \leqslant 10$, and Figure 6 is the corresponding plot. It is observed that the proposed average pixel expansions are between those of the DVCS and the PVCS. This compromise of pixel expansion is used to compromise the contrast. Figure 7 shows the values of $m_H^{(1)}$ and $m_H^{(2)}$ with $m'=1$ and $m'=m/2$, for $1 \leqslant m \leqslant 30$. When $m'=m/2$, there is no large difference between $m_H^{(1)}$ and $m_H^{(2)}$. However, $m_H^{(1)}$ and $m_H^{(2)}$ for $m'=1$ differ from each other for large m. This result implies that when choosing a large m' to construct the DPVCS, all patterns are suitable, while the patterns IP_1 and RP_1 are more suitable than IP and RP when choosing a small m'. Using IP_1 and RP_1 could achieve better contrast but larger shadow. On the contrary, using IP and RP one obtains the opposite characteristics.

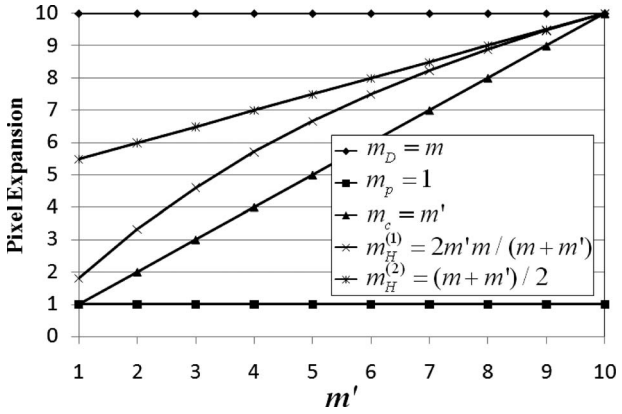

Figure 6. Pixel expansions for all VCSs.

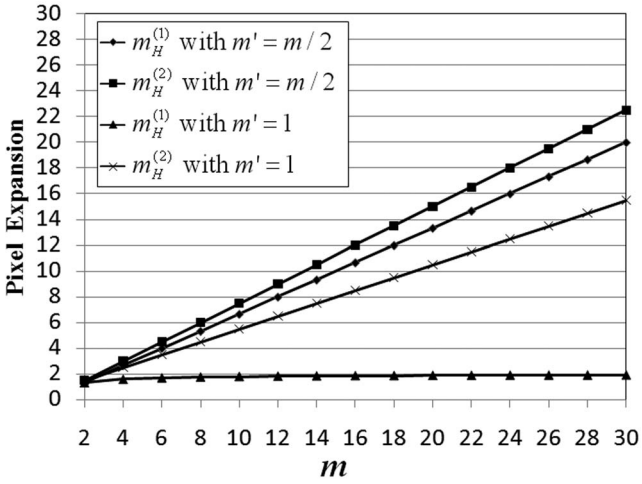

Figure 7. Pixel expansions for the proposed DPVCS.

Contrast

Figure 8 shows reconstructed images for all (2, 3) Cimato PVCSs. The secret is a natural image, *House*. Figures 8(a)

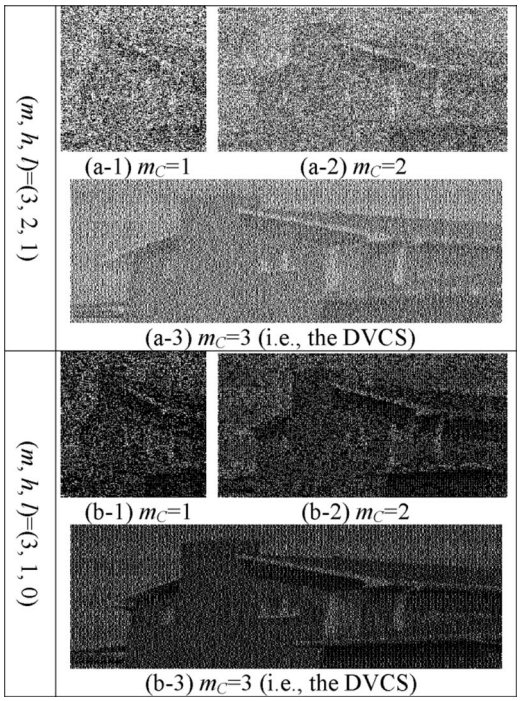

Figure 8. Reconstructed images of the (2, 3) Cimato *et al.*'s PVCS for $m_C=1, 2, 3$; the secret is a natural image House: (a) using $(m,h,l)=(3,2,1)$, (b) using $(m,h,l)=(3,1,0)$.

and 8(b) shows the experimental results when using $(m,h,l)=(3,2,1)$ and $(m,h,l)=(3,1,0)$, respectively. Figures 8(a-1) and 8(b-1) are the results with PVCSs with no pixel expansion, which have poor visual quality and less shadow size. Figures 8(a-3) and 8(b-3) are the DVCSs which have high contrast and large shadow size. Figures 8(a-2) and 8(b-2) (Cimato's PVCS with $m_C=2$) is a compromise between the PVCS with no pixel expansion and the DVCS. To compare our DPVCS with the Cimato PVCS with $m_C=2$, we use Figs. 5(b-2) and 8(a-2) which have the same pixel expansion and are both constructed from the DVCS of $(m,h,l)=(3,2,1)$. Although, the judgment of image contrast by HVS is very subjective, it is evident that the image quality of Fig. 5(b-2) is better than that of Fig. 8(a-2). Figure 8(b-2) has the almost same contrast as Figs. 5(b-3) and 5(b-4), which is due to the using of $l=0$, i.e., fully black.

There are theoretical definitions of contrast for the DVCS proposed in Refs. 1 and 32. However, the contrast of PVCS is difficult to define due to its probabilistic property. The authors in Ref. 7 gave a new measurement, the probabilistic factor β, to measure this feature. A β-probabilistic PVCS has the feature that the correct probability of the reconstructed black (respectively white) pixel is larger than a threshold β. This factor characterizes the probabilistic nature whereby larger β results in a perceptually better reconstructed image. Notice that the DVCS has $\beta=1$. By using Eqs. (2)–(5) in Ref. 7, we compute β for Cimato's (2, 3) PVCSs with $(m,h,l)=(3,1,0)$ and $(m,h,l)=(3,2,1)$. The result is shown in Table II where h' and l' are the whiteness of white and black color in m' subpixels. For example, the (2, 3)-threshold Cimato PVCS with $m'=1$ has

$$C'_B=\left\{\begin{bmatrix}1\\0\\1\end{bmatrix}\cdot\begin{bmatrix}1\\1\\0\end{bmatrix}\cdot\begin{bmatrix}0\\1\\1\end{bmatrix}\right\} \quad \text{and} \quad C'_W=\left\{\begin{bmatrix}1\\1\\1\end{bmatrix}\cdot\begin{bmatrix}1\\1\\1\end{bmatrix}\cdot\begin{bmatrix}0\\0\\0\end{bmatrix}\right\}.$$

When stacking every two shadows let the probability of a black subpixel correctly recovered as a black pixel be $p_{b/b}$, and the probability of a white subpixel incorrectly recovered as a black pixel be $p_{b/w}$. Similarly, we define $p_{w/w}$ and $p_{w/b}$. From C'_B and C'_W, it is obvious that $p_{b/b}=1$, $p_{b/w}=2/3$, $p_{w/w}=1/3$, and $p_{w/b}=0$. So the differences $(p_{b/b}-p_{b/w})$ and $(p_{w/w}-p_{w/b})$ are all greater than 1/3 and thus $\beta=1/3$. For this case, because we only use one subpixel to represent a secret pixel, the whiteness of a black pixel is $l'=0$ and the whiteness of a white pixel is $h'=1$.

Because the contrast in a PVCS is guaranteed only with a certain probability, the authors in Ref. 7 suggested that the goodness of a PVCS should be measured by the probabilistic factor β. Therefore, we evaluate the probabilistic factors instead of contrast among the DVCS, the PVCS and the proposed DPVCS. Since the β of DVCS is 1, so the probabilistic factors for our DPVCS $\beta_H^{(1)}$ (using IP and RP) and $\beta_H^{(2)}$ (using IP_1 and RP_1) can be defined as follows:

$$\beta_H^{(1)}=\overset{\text{use D operation}}{(m'/(m+m')\times 1)}+\overset{\text{use P operation}}{(m/(m+m')\times \beta_{(m,h,l,m')})},$$

where $\beta_{(m,h,l,m')}$ is the probabilistic factor of PVCS with (m,h,l,m'),

$$\beta_H^{(2)}=\overset{\text{use } D_1 \text{ operation}}{(1/2\times 1)}+\overset{\text{use } P_1 \text{ operation}}{(1/2\times \beta_{(m,h,l,m')})},$$

where $\beta_{(m,h,l,m')}$ is the probabilistic factor of PVCS with (m,h,l,m').

Table III lists the probabilistic factors for all (2, 3) VCSs when using $(m,h,l)=(3,1,0)$ and (3, 2, 1). Our DPVCS

Table II. β for Cimato *et al.*'s (2, 3) PVCS using $(m,h,l)=(3,1,0)$ and $(m,h,l)=(3,1,1)$.

	$(m,h,l)=(3,1,0)$			$(m,h,l)=(3,1,1)$		
$(m'\backslash h',l')$	1, 0	2, 1	3,2	1, 0	2, 1	3,2
1	1/3	—	—	1/3	—	—
2	2/3	0	—	1/3	1/3	—
3	1	0	0	0	1	0

Table III. Probabilistic factors β for all (2, 3) VCSs.

	$(m,h,l)=(3,1,0)$			$(m,h,l)=(3,2,1)$		
VCSs	$m'=1$	$m'=2$	$m'=3$	$m'=1$	$m'=2$	$m'=3$
DVCS	—	—	1	—	—	1
Cimato *et al.*'s PVCS	1/3	2/3	1	1/3	1/3	1
The proposed DPVCS $\beta_H^{(1)}$ ($\beta_H^{(2)}$)	1/2 (2/3)	4/5 (5/6)	1 (1)	1/2 (2/3)	3/5 (2/3)	1 (1)

Table IV. Probabilistic factors β for all (2, 4) VCS with $(m,h,l)=(6,3,1)$.

VCSs	$m'=1$	$m'=2$	$m'=3$	$m'=4$	$m'=5$	$m'=6$
DVCS	—	—	—	—	—	1
Cimato *et al.*'s PVCS	1/3	7/15	1/2	4/5	1	1
The proposed DPVCS $\beta_H^{(1)}$ ($\beta_H^{(2)}$)	3/7 (2/3)	3/5 (11/15)	2/3 (3/4)	22/25 (9/10)	1 (1)	1 (1)

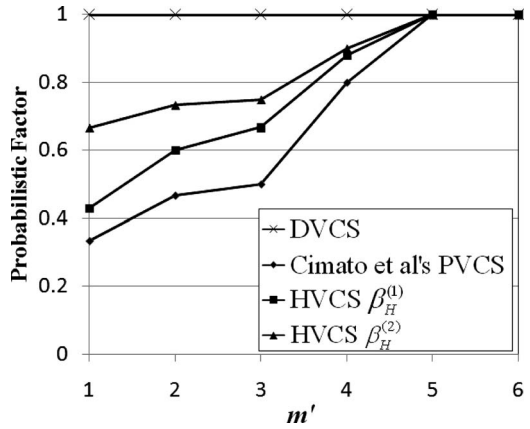

Figure 9. Plot of the probabilistic factors for all (2, 4) VCSs with $(m,h,l)=(6,3,1)$.

based on $(m,h,l)=(3,1,0)$ has $\beta_H^{(1)}=1/4\times1+3/4\times1/3=1/2$ and $\beta_H^{(2)}=1/2\times1+1/2\times1/3=2/3$ for $m'=1$; $\beta_H^{(1)}=2/5\times1+3/5\times2/3=4/5$ and $\beta_H^{(2)}=1/2\times1+1/2\times2/3=5/6$ for $m'=2$. When choosing $m'=3$, Cimato's PVCS and our DPVCS are all reduced to DVCS. To show the effects on the probabilistic factor for more combinations of m and m', we compare all VCSs based on $(m,h,l)=(6,3,1)$ where $m'\in[1,6]$. Table IV lists the result, and the plot is shown in Figure 9. As described in Ref. 7, the bigger probabilistic factor results in a better VCS. In Fig. 9, the β of our DPVCS rises faster than that of the PVCS, which means that the DPVCS is better than the PVCS. The parameter β approaches unity (i.e., the DVCS) when m' approaches m.

Table V summarizes the comparison of VCSs for the following items: (1) the visual quality, (2) the pixel expansion, (3) the probabilistic factor, (4) the feature of generality (the construction method can be applied on any k and n; the soft and hard threshold), and (5) the perfect reconstruction of secret pixels using computation. Let the symbolic notations [1], [2], and [3] represent the goodness judgments, "good," "medium," and "poor," respectively. For example, [1] means good visual quality, less pixel expansion and a high probabilistic factor, while [3] represents poor visual quality, the most pixel expansion and the smallest probabilistic factor. It is observed that the visual quality of the reconstructed image and the pixel expansion are traded-off. DVCS has the best visual quality but smaller shadow size (Figs. 8(a-3) and 8(b-3)). However, the shadow size can be significantly reduced in the PVCS with no expansion, but at the same time the image quality is significantly degraded (Figs. 8(a-3) and 8(b-3)). Cimato's VCS and our DPVCS have this trade-off capability. The notations $[1]\overset{\text{trade}}{\rightleftarrows}[3]$, $[1]\overset{\text{trade}}{\rightleftarrows}[2]$, and $[2]\overset{\text{trade}}{\rightleftarrows}[3]$ mean the Cimato PVCS and the proposed DPVCS have the trading ability, but the pixel expansion of our DPVCS cannot be reduced to "1." The minimum pixel expansion is about "2" for our DPVCS (see $m_H^{(1)}$ in Fig. 6); however, our scheme has better image quality. The size-adjustable VCS in Ref. 31 is strictly incapable of trade-off because it combines the DVCS and PVCS only for reducing pixel expansion. All PVCSs (Refs. 5–7) and our DPVCS have the probabilistic feature and thus we use the measurement β for comparison. Our DPVCS has the scores $[1]\overset{\text{trade}}{\rightleftarrows}[2]$, $[2]\overset{\text{trade}}{\rightleftarrows}[3]$, and [2], respectively, for the visual quality, the pixel expansion, and the probabilistic factor. This result implies that our DPVCS is a good hybrid scheme.

For the other two compared characteristics, all schemes have the same general features except the size-adjustable VCS.[29] The DVCS has the deterministic feature that the secret pixel is represented by all m subpixels, and one may spend a large computation loads to recover the original secret pixels. This concept for reconstructing a secret pixel can

Table V. Comparison of VCSs. Notation: ○: satisfied; △: partially satisfied; ×: not satisfied.

VCSs	DVCS[a]	PVCS[b]	Cimato *et al.*'s PVCS[c]	Size-adjustable VCS[d]	The proposed DPVCS
Visual quality	[1]	[3]	[1] $\overset{\text{trade}}{\rightleftarrows}$ [3]	[3]	[1] $\overset{\text{trade}}{\rightleftarrows}$ [2]
Pixel expansion	[3]	[1]	[1] $\overset{\text{trade}}{\rightleftarrows}$ [3]	[1]	[2] $\overset{\text{trade}}{\rightleftarrows}$ [3]
Probabilistic factor	[1]	[3]	[3]	[3]	[2]
Generality	○	○	○	△	○
Perfect reconstruction of secret pixel by computation	○	×	×	×	○

[a]Reference 1.
[b]References 5 and 6.
[c]Reference 7.
[d]Reference 29.

be found in Ref. 2. Nevertheless, the PVCS had deleted some columns in the base matrices and thus lost pixel information permanently. Our DPVCS encrypts some secret pixels by the DVCS, so the secret pixels can be recovered in part by computation.

Furthermore, a comparison between our DPVCS and some other image secret sharing technologies[15,17–23] is given in Table VI to gauge the utility of our research. Descriptions of these image secret sharing technologies are omitted in the interest of brevity. One can find the details in Refs. 15 and 17–23. All schemes provide the feature of sharing a secret image into noise-like shadow images (the proposed scheme and Refs. 15, 17, 22, and 23) or meaningful shadow images, which show cover images (Refs. 19–21). At this time, shadow

Table VI. Comparison between our DPVCS and some other image secret sharing technologies.

	Our DPVCS	Ref. 15	Ref. 17	Ref. 18	Ref. 19	Ref. 20	Ref. 21	Ref. 22	Ref. 23
Purpose	Sharing secret image into noise-like shadows			Sharing secret image into shadows with a shrunken version of the secret	Sharing secret image into shadows with authentication ability			Sharing secret image into noise-like shadows with two decoding options	
Secret image	Black and white image	Gary natural image; can be extended to color image by processing each color plane						Two secret images: black/white and gray image	
Shadow image (note: in Refs. 19–21 is called as stegoimage)	Noise-like shadow images			A shrunken version of secret on shadows	Cover images shown on stego images			Noise-like shadow images	
Visual quality of reconstructed image	Vague	Perfect reconstruction of original secret		Reconstruction of secret image with high PSNR	Perfect reconstruction of original secret			Vague black-and -white image in first decoding phase Perfect reconstruction of Gary image in second decoding phase	
Stacking-to -see capability?	Yes	No	No	No	No	No	No	Yes	Yes
Decoding options	One	One	One	One	One	One	One	Two	Two
Decoding complexity	Easy: photocopy shadows on transparencies and stack them on overhead projector	Semieasy: using simple logic operations	Hard: using Lagrange interpolation to recover the secret image					Two decoding phases: first phase—Easy: stacking transparencies on overhead projector second phase—semieasy: using a dithering table	Two decoding phases: first phase—Easy: stacking transparencies on overhead projector second phase—Hard: using Lagrange interpolation

images in Refs. 19–21 are often called stego images. A so-called user-friendly scheme (Ref. 18) in which shadow images show a shrunken version of the secret image was proposed to address the identification and management problems. Since the portrait on shadow images had already leaked the secret information, this user-friendly scheme is, strictly speaking, not a secret sharing scheme. As is well-known, the reconstructed images from the VCS strategy are vague, while polynomial-based schemes (Refs. 17–21) or the scheme using logic operations (Ref. 15) have the good visual quality with high PSNR. The VCS has distinctive stacking-to-see capability. One can photocopy shadows on transparencies and superimpose them on an overhead projector to visually decode by HVS. However, other schemes need simple logic operations (Ref. 15) and the Lagrange interpolation (Refs. 17–21) for reconstruction. The schemes in Refs. 22 and 23 are two-in-one secret image sharing schemes, and have two decoding options. Both schemes have stacking-to-see capability, and can also perfectly reconstruct the secret image. The scheme in Ref. 22 reconstructs the perfect gray secret image by a dithering look-up table, and the scheme in Ref. 23 uses the Lagrange interpolation to recover the secret. As described above, it can be seen that all schemes are secret sharing schemes and they have achieved the unconditional security. Although our scheme cannot obtain the competitive recovery quality, the novel stacking-and-see property in our VCS has intended applications in imaging. For example, adopting our VCS in two-in-one scheme is reasonable and valuable. We can stack shadows and directly decode the black-and-white secret image by HVS without computation, e.g., when the computer is temporarily unavailable. When the computer is available at the decoding scene, we then carry out more computation to obtain the image with quality sufficient for high-end applications.

When compared with standard encryption, our noise-like shadow images also have high entropy values. As is known, an image pattern with a high entropy value is presumably more random in black and white arrangement, and so is more suitable for hiding more secret data without causing a noticeable change. An entropy value of a black-and-white shadow image is determined as $p_0 \times \log_2(1/p_0) + p_1 \times \log_2(1/p_1)$, where p_0 and p_1 are the occurrence probabilities of black and white pixels in shadows. Our DPVCS is a hybrid of DVCS and PVCS and holds the security condition, and thus the occurrence probabilities p_0 and p_1 in shadows can be directly obtained from black and white base matrices. Consider two VCSs (examples 1 and 2) and use the black-and-white text NDHU as the secret image. According the definition of entropy, the entropy values of our shadows are 1 (example 1) and 0.9183 (example 2). On the other hand, the encrypted NDHU by AES block cipher has the entropy value 0.9998. All of the encrypted images have high entropy values.

CONCLUSION

In this article, we aim at trading-off shadow size for contrast. The proposed DPVCS integrates the DVCS and the PVCS simultaneously. Our main contribution is to prove theoretically that the combination of DVCS and PVCS satisfies the contrast and security properties of VCS. By arranging the subpixels in the proper patterns, we successfully develop their specialties and overcome their drawbacks. Finally, our DPVCS achieves less pixel expansion than does the DVCS and the higher clarity of the reconstructed image than does the PVCS. Moreover, we solve the generality problem of size-adjustable VCS, which is also a hybrid of DVCS and PVCS.

ACKNOWLEDGMENTS

This work was supported in part by iCAST Project under Grant No. NSC 97-2745-P-001-001, and TWISC@NCKU, NSC under Grant No. NSC 97-2219-E-006-009.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography", Advances in Cryptology-EUROCRYPT' 94, Lect. Notes Comput. Sci. **950**, 1 (1995).
[2] H. Kuwakado and H. Tanaka, "Size-reduced visual secret sharing scheme", IEICE Trans. Fundamentals **E87-A**, 1193 (2004).
[3] C. N. Yang and T. S. Chen, "New size-reduced visual secret sharing schemes with half reduction of shadow size", IEICE Trans. Fundamentals **E89-A**, 620 (2006).
[4] Y. C. Hou and S. F. Tu, "A visual cryptographic technique for chromatic images using multi-pixel encoding method", J. Research Pract. Inf. Technol. **37**, 179 (2005).
[5] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography", IEICE Trans. Fundamentals **E82-A**, 2172 (1999).
[6] C. N. Yang, "New visual secret sharing schemes using probabilistic method", Pattern Recogn. Lett. **25**, 481 (2004).
[7] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic visual cryptography schemes", Comput. J. **49**, 97 (2006).
[8] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques", Pattern Recogn. Lett. **24**, 349 (2003).
[9] J. C. Hou, "Visual cryptography for color images", Pattern Recogn. **36**, 1619 (2003).
[10] C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for grey level images", Inf. Process. Lett. **75**, 255 (2000).
[11] E. R. Verheul and H. C. A. Van Tilborg, "Constructions and properties of *k* out of *n* visual secret sharing scheme", Designs, Codes, Cryptogr. **1**, 179 (1997).
[12] C. N. Yang and C. S. Laih, "New colored visual secret sharing schemes", Designs, Codes, Cryptogr. **20**, 325 (2000).
[13] S. Cimato, R. Prisco, and A. De Santis, "Optimal colored threshold visual cryptography schemes", Designs, Codes, Cryptogr. **35**, 311 (2005).
[14] S. J. Shyu, "Efficient visual secret sharing scheme for color images", Pattern Recogn. **39**, 866 (2006).
[15] R. Lukac and K. N. Plataniotis, "Bit-level based secret sharing for image encryption", Pattern Recogn. **38**, 767 (2005).
[16] R. Lukac and K. N. Plataniotis, "A cost-effective encryption scheme for color images", Real-Time Imag. **11**, 454 (2005).
[17] C. C. Thien and J. C. Lin, "Secret image sharing", Comput. Graphics **26**, 765 (2002).
[18] C. C. Thien and J. C. Lin, "An image-sharing method with user-friendly shadow images", IEEE Trans. Circuits Syst. Video Technol. **13**, 1161 (2003).
[19] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication", J. Syst. Softw. **73**, 405 (2004).
[20] C. N. Yang, T. S. Chen, K. H. Yu, and C. C. Wang, "Improvements of image sharing with steganography and authentication", J. Syst. Softw. **80**, 1070 (2007).
[21] C. C. Chang, Y. P. Hsieh, and C. H. Lin, "Sharing secrets in stego images with authentication", Pattern Recogn. **41**, 3130 (2008).
[22] D. Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography", J. Electron. Imaging **14**, 033019-1 (2005).
[23] S. J. Lin and J. C. Lin, "VCPSS: A two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches", Pattern Recogn. **40**, 3652 (2007).
[24] C. N. Yang and T. S. Chen, "An image secret sharing scheme with the capability of previewing the secret image", *Proc. International Conference on Multimedia & Expo (ICME'07)* (IEEE, Beijing, China, 2007) p. 1535.
[25] R. Lukac and K. Platanniotis, "Digital image indexing using secret

sharing schemes: a unified framework for single-sensor consumer electronics", IEEE Trans. Consum. Electron. **51**, 908 (2005).
[26] C. C. Chang and J. C. Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy", Pattern Recogn. Lett. **23**, 931 (2002).
[27] S. C. Tai and C. C. Chang, "A new repeating color watermarking scheme based on human visual model", EURASIP J. Appl. Signal Process. **13**, 1965 (2004).
[28] H. Yamamoto, Y. Hayasaki, and N. Nishida, "Securing information display by use of visual cryptography", Opt. Lett. **28**, 1564 (2003).
[29] P. Tuyls, T. Kevenaar, G. J. Schrije, A. A. M. Staring, and M. van Dijk, "Visual crypto displays enabling secure communications", Security in Pervasive Computing, Lect. Notes Comput. Sci. **2802**, 271 (2003).
[30] C. N. Yang, T. S. Chen, and M. H. Ching, "Embed additional private information into two-dimensional bar codes by the visual secret sharing scheme", Integr. Comput. Aided Eng. **13**, 189 (2006).
[31] C. N. Yang and T. S. Chen, "Size-adjustable visual secret sharing schemes", IEICE Trans. Fundamentals **E88-A**, 2471 (2005).
[32] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography schemes with specified whiteness", Designs, Codes, Cryptogr. **25**, 15 (2002).