Measurement 51 (2014) 81–90

Contents lists available at ScienceDirect

Measurement

journal homepage: www.elsevier.com/locate/measurement

Color transfer in visual cryptography

Hao Luo [a], Hua Chen [a], Yongheng Shang [a,*], Zhenfei Zhao [b], Yanhua Zhang [b]

[a] School of Aeronautics and Astronautics, Zhejiang University, Hangzhou 310027, China
[b] School of Electronics and Information, Zhejiang University of Media and Communications, Hangzhou 310018, China

ARTICLE INFO

Article history:
Received 16 September 2013
Received in revised form 14 December 2013
Accepted 27 January 2014
Available online 4 February 2014

Keywords:
(*k*, *n*) Visual cryptography model
Color transfer
Digital halftoning
Monochrome output device
Cheating prevention
Cholesteric liquid crystal display

ABSTRACT

Visual cryptography is an important technique for image encryption. This paper proposes a color transfer scheme which can be incorporated into the (*k*, *n*) visual cryptography model. In encoder, a color image is encrypted into *n* noise-like binary share images. When any *k* or more than *k* shares are collected, a high quality colorful version of the secret image can be reconstructed with low complexity computations. The principle is motivated to develop a color image secret sharing for output devices such as monochrome printer or fax machines. The generated share images are still binary transparencies which can be directly produced by these low cost output devices. Meanwhile, the security of a (*k*, *n*) visual cryptography model is perfectly preserved. When stacking a qualified set of transparencies, the gray level version of secret content can be revealed by human visual system. Nevertheless, the proposed paradigm is cheating immune. It also can be integrated into some emerging display technologies such as cholesteric liquid crystal display. Experimental results and related examples demonstrate the effectiveness and efficiency.

1. Introduction

As a powerful technique for image encryption [1–4] and secret sharing, the paradigm of visual cryptography scheme (VCS) is first introduced by Naor and Shamir [5]. In their (*k*, *n*) VCS model, a binary secret image is encrypted into *n* random noise-like shares (also called transparencies, shadows) and further printed on transparencies held by *n* participants. When superimposing a qualified set of *k* or more shares, the secret content is visible to human eyes. In other words, no computer participation or prior knowledge is required for secret decryption. Meanwhile, this VCS is perfectly secure for no secret information will be revealed when less than any *k* transparencies are overlaid.

In recent years, many various VCS methods are proposed in literatures. Most of them can be summarized as following three aspects. An extensive survey can be referred to [6].

(1) Extend the basic VCS model for grayscale and color image encryption. In these schemes, digital halftoning or its produced halftone images are usually involved [7]. The transparencies could be binary or color halftone images. In order to enhance the security, some transparencies are meaningful images which are jointly produced by VCS and a given camouflage image.
(2) Introduce computer participation for incorporating an extra ability into the conventional VCS. These abilities include progressive transmission, confidential data hiding for authentication, nearly lossless data reconstruction, etc. As a result, the applications of these VCS models are broadened in some specific scenarios.

* Corresponding author. Address: No. 38, ZheDa Road, Yuquan Campus, Zhejiang University, School of Aeronautics and Astronautics, Hangzhou 310027, PR China. Tel.: +86 15858259064.
E-mail address: luohao723@126.com (Y. Shang).

http://dx.doi.org/10.1016/j.measurement.2014.01.033
0263-2241/

(3) Reducing the size expansion of transparencies and enhancing the decrypted image quality [8]. The former work is beneficial to reducing the burden of limited transmission channel and saving storage space. The latter work is useful when a high fidelity secret image should be recovered. This is because the contrast and distortion of stacking decryption mechanism are not acceptable in most cases.

In [9], Hou proposed a VCS for color image secret sharing with following two properties. (1) To obtain a hardcopy of a color transparency, color printers must be available to convert it into cyan, magenta and yellow (CMY) space first (i.e., the complementary red, green and blue (RGB) space), and then adopt C, M, Y inks for color display. However, as the color inks are much more expensive, this scheme is not applicable in the cases where only a monochrome printer can be used. (2) The decrypted image quality is not satisfactory due to the stacking mechanism. In general, the contrast of the decrypted image is much lower in comparison with the original version. In addition, the color inks may be printed slightly out of register due to the mechanical tolerances and hence further visual distortions are introduced.

In Hou's and some other VCS methods, digital halftoning is involved. It is a process to transform a continuous-tone (e.g. 8-bit gray level) image into a two-tone (e.g. 1-bit binary) image. As a product, halftone image is a special kind of binary image for monochrome printing and low cost devices display. It resembles the continuous-tone version by the low-pass filtering of the human visual system (HVS) when viewed from an appropriate distance. So far, the popular halftoning techniques consist of ordered dithering, error diffusion, and iterative methods. Among these three categories, error diffusion achieves a better tradeoff between low complexity computations and moderate halftone image quality.

Generally speaking, the ordinary ink jets and laser printers are only able to apply or not apply ink at a given spatial location of paper or transparency. During gray level image printing, the ink dots were black; while in color image printing, a cyan, magenta, or yellow ink dot is possible at each location. In fact, many color printers can also produce a black ink dot. In digital products, the low cost liquid crystal displays (LCDs) have the same limitation in that they can only turn a pixel on or off.

As one of the most important image features, color has been used in a large quantity of applications [10] including image retrieval, object detection and recognition, target segmentation and tracking, etc. This paper proposes a (k, n) color transfer VCS (CTVCS for short) technique. It can improve the deficiencies of Hou's scheme due to an extra ability of color transfer is incorporated. Color transfer [11] means to recolorize a gray level image using its original color when captured by camera or generated by computer. In [12], a reversible color transfer technique is proposed based on wavelet transform. But it cannot be used in VCS. Actually, reversibility is also the key property of the proposed method. That is, the color information can be nearly recovered from the binary shares or their hardcopy transparencies. In particular, a color image is encrypted into n binary transparencies and the colors can be retrieved from any k or more than k transparencies at a later time.

The CTVCS is implemented by flattening the compressed color information into a single bit-plane with digital halftoning and color decomposition exploited. Specifically, the secret image is decomposed into three color channels (R, G, and B) and transformed into the grayscale version first. Then the digital halftoning is applied to convert the grayscale and three color channel images into halftone versions, respectively. Next, four halftones of the grayscale, R, G, B channels are integrated encrypted with a modified (k, n) VCS. In this way, the color information is also embedded into the transparencies during the processing. In the decoding stage, the inverse procedures are executed due to the reversibility is well preserved. To the best of our knowledge, CTVCS is the first VCS model with the ability of color transfer.

The remained part of this paper is organized as follows. Section 2 reviews the principles of the conventional VCS, secure color transfer techniques and error diffusion halftoning. Section 3 extensively describes the proposed scheme and gives some examples. Section 4 demonstrates the experimental results and discussions. Finally, conclusions are given in Section 5.

2. Related work

2.1. The conventional VCS

The conventional (k, n) VCS consists of two collections of N M Boolean (Basis) matrices C_0 and C_1. To share a white (black) pixel, the dealer randomly chooses one of the matrices in C_0 (C_1). Each row of the chosen matrix corresponds to a transparency's subpixels. The solution is regarded as valid if three conditions given in [5] are satisfied.

For description simplicity, an example of (2, 2) VCS principle is shown in Fig. 1. It divides each secret pixel into $M = 2$ subpixels. Each white (denoted by 0) or black (denoted by 1) pixel corresponds to two encryption modes. Each choice contains a pair of white and black pixels.

Three important factors are usually taken into account during a VCS construction. (1) Hamming weight. It refers to the number of non-zero symbols in a symbol sequence. (2) Pixel expansion. It is the number of the subpixels in a shared pixel. (3) Relative difference. It refers to the ratio of the maximum number of black subpixels in a reconstructed white pixel to the minimum number of black subpixels in a reconstructed black pixel.

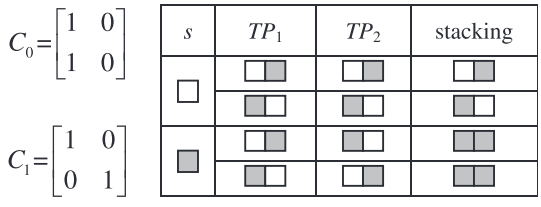

Fig. 1. Encryption and decryption strategies of conventional (2, 2) VCS.

2.2. Secure color transfer

In [19], Leung et al analyze the security of Hou's visual cryptography scheme [9] for color images. Besides, it further extends Hou's method to compromise secret images with more than four colors. However, the C, M and Y shares are still color images which cannot be output by monochrome printers. In [20], Chaumont et al. proposes another method to protect the color information of images with the aid of the corresponding gray level images. It is based on a color reordering algorithm after a quantization step. The color data is embedded in the color palette in the gray level version of the input. In essence, the principle of data hiding is exploited. In [20], Wu et al develop a color VCS with meaningful transparencies used. The transparencies are also color image and the approach cannot be directly extended to (k, n) VCS model.

2.3. Error diffusion halftoning

As the principle of error diffusion shown in Fig. 2, the error is diffused to the neighbors of the current processing pixel when halftoning a continuous-tone image line by line sequentially. Here $x(i, j)$ is the current processing pixel and $x'(i, j)$ is the diffused error sum added up from the neighboring processed pixels. $b(i, j)$ represents the binary output at coordinates (i, j). $u(i, j)$ is the modified gray output and $e(i, j)$ is the difference between $u(i, j)$ and $b(i, j)$. The relationships of these variables are given below.

$$u(i,j) = x(i,j) + x'(i,j) \tag{1}$$

$$x'(i,j) = \sum_{m=0}^{1}\sum_{n=-1}^{1} e(i+m, j+n) \quad k(m,n) \tag{2}$$

$$e(i,j) = u(i,j) - b(i,j) \tag{3}$$

$$b(i,j) = \begin{cases} 0 & \text{if } u(i,j) < t_h \\ 1 & \text{if } u(i,j) \geqslant t_h \end{cases} \tag{4}$$

where the threshold t_h in Eq. (4) is a threshold usually set as 127. From the Fig. 2, different error diffusion kernels $k(m, n)$ correspond to different visual qualities of the output halftone. Three kernels, Floyed-Steinberg, Jarvis and Stucki are widely used. In our case, Floyed-Steinberg kernel is used.

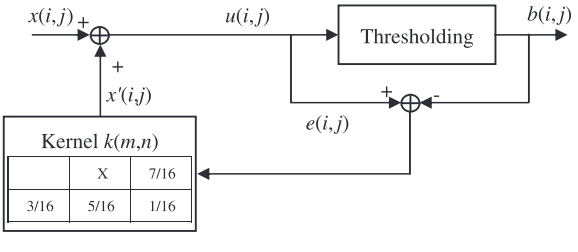

Fig. 2. Flow chart of error diffusion halftoning.

3. Proposed scheme

3.1. Motivation

As the principle of the proposed CTVCS illustrated in Fig. 3, it is motivated to develop a technique for sharing a secret color image and each participant only has black and white printers, fax machines, LCD (including ChLCD) display device to output, transmit or display his transparency. However, the color information of the original secret image is required to be reconstructed during decryption.

In other words, the color image must be converted to binary transparencies during encryption. Later on, any at least k participants might retrieve the colors along with the secret content decryption. It also can be considered as a recolorization processing. For example, suppose a color image is encrypted into n binary transparencies. These transparencies are output by a black and white printer and the hardcopies distributed to n participants. In decryption, a low quality gray level secret content can be revealed by transparencies stacking. Moreover, if scanned this set of transparencies into digitized versions, the original image color can be nearly recovered.

This prototype is useful when only monochrome output devices (printers, fax machines, etc.) and ordinary scanners are available. In a word, the secret image color is also encoded in the binary transparencies during (k, n) VCS encryption with an invertible process.

3.2. (k, n) CTVCS

3.2.1. Encryption

The steps of (k, n) CTVCS model encryption are described as follows. As shown in Fig. 4, suppose the secret I sized u v is a 24-bit color image.

Step 1. Secret image halftoning. I is transformed into an 8-bit grayscale image and decomposed into R, G and B channel images. All of these intermediate products are further halftoned into 1-bit images H, H_R, H_G, H_B, respectively.

Step 2. Pixel expansion. Each pixel p of H is expanded into a vector with three subpixels $[p_1, p_2, p_3]^T$. The values of p_1, p_2, and p_3 are exactly the same as that of p.

Step 3. Color information permutation. Permute the H_R, H_G, H_B concatenated data with a key and thus obtain the resulted color data C_p. Obviously, C_p is a bit-stream of u v 3 bits.

Step 4. Basis matrices construction. To an n m binary basis matrix, n and m refer to the number of participants and ratio of pixel expansion, respectively. There are a variety of methods to construct the basis matrices. Suppose $C_0 \in \{C_0^1, C_0^2, \ldots, C_0^i\}$ and $C_1 \in \{C_1^1, C_1^2, \ldots, C_1^j\}$ correspond to a white and black pixel encryption, respectively. Each element in C_0 or C_1 is an n m binary matrix. More details of basis matrices construction can be referred to [5].

Step 5. Basis matrices partition. Partition the elements in C_0 and C_1 into two sets as $C_0 = \{C_{00}, C_{01}\}$ and $C_1 = \{C_{10}, C_{11}\}$. The utilization of C_{00}, C_{01}, C_{10} and C_{11} are given in Table 1, where "T" means transpose.

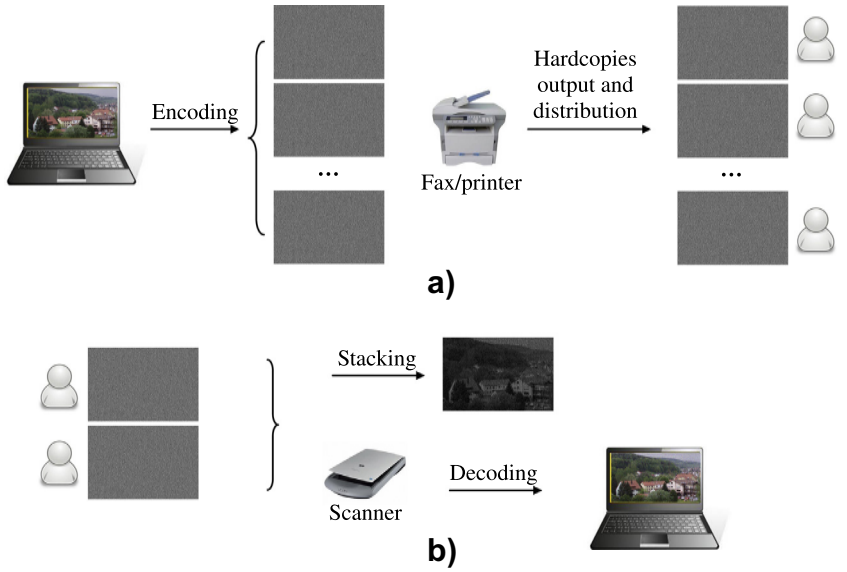

Fig. 3. Principle of the CTVCS, (a) encryption and (b) decryption.

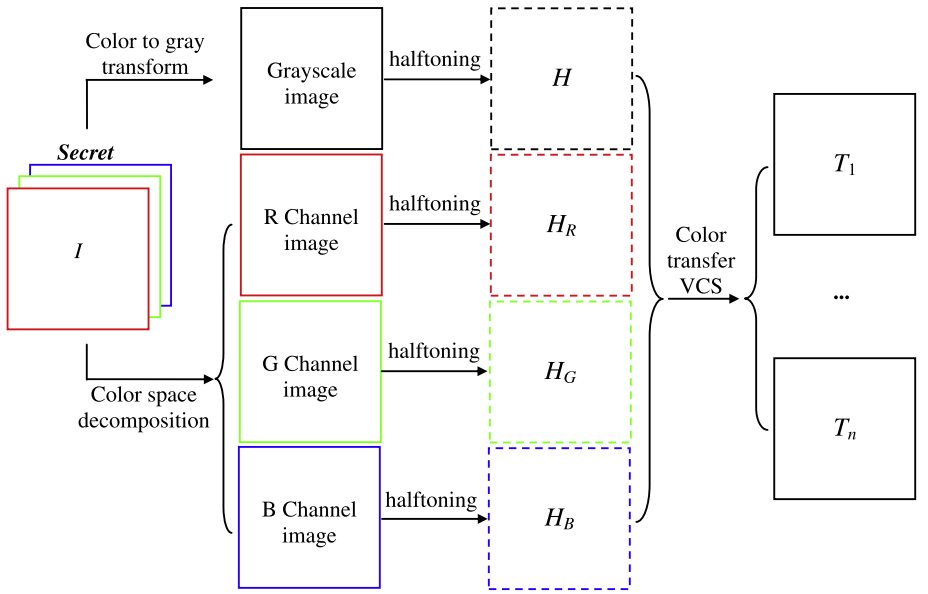

Fig. 4. Flow chart of CTVCS encryption.

Step 6. Encrypt p_1, p_2, and p_3 one by one. If $p_1 = 0$ and $c = 0$, then a matrix belongs to C_{00} is selected. If $p_1 = 0$ and $c = 1$, then a matrix belongs to C_{01} is selected. If $p_1 = 1$ and $c = 0$, then a matrix belongs to C_{10} is selected. If $p_1 = 1$ and $c = 1$, then a matrix belongs to C_{11} is selected. Then, n rows of this matrix are distributed to n participants sequentially. Likewise, p_2, and p_3 are encrypted with the same way.

Step 7. Repeat the operations from Steps 2 to 6 until all of the pixels in H are processed. In this way, n binary transparencies with each sized $3u \quad mv$ are produced.

3.2.2. Decryption

Suppose a set of k binary transparencies are obtained. If more than k transparencies are collected, randomly select k from them. In our case, a hierarchical decryption mechanism is employed with three quality levels secret image decrypted. As described below, some simple computation is required in the levels 2 and 3 decryption.

Level 1. Stacking the k transparencies and the content of secret image is visible. Compared with levels 2 and 3, the revealed secret is of the lowest visual quality due to the contrast and image size distortions.

Table 1
Basis matrices partition.

Matrix	Encryption	
	Expanded subpixels	Color bit
C_{00}	$[000]^T$	0
C_{01}	$[000]^T$	1
C_{10}	$[111]^T$	0
C_{11}	$[111]^T$	1

In levels 2 and 3 decryption, each transparency is partitioned into 3 m blocks. To the current processing block, retrieve the first rows and reconstruct the encryption matrix. Then the task is reduced to a table look-up operation.

Level 2. The halftone image H can be reconstructed. According to Table 1, the expanded subpixels can be obtained. As $p = p_1 = p_2 = p_3$, the halftone pixel is recovered. As long as all blocks are processed, H is recovered. This level of decryption product is of moderate visual quality for the image color is still discarded.

Level 3. The color halftone image can be reconstructed. According to Table 1, the color bit is recovered. Specifically, if C_{00} or C_{10} is reconstructed, the extracted color bit is "0". Otherwise, "1" is extracted if C_{01} or C_{11} is reconstructed. Repeat this procedure until all the blocks are processed. As a result, the secret image color information is retrieved. It is further inverse permuted and the R, G, B channels halftone images are reconstructed. Recompose these three channels and the color halftone image of the secret is recovered. It can be directly displayed by many low cost devices. If necessary, a continuous-tone version also can be obtained via inverse halftoning technique. The decrypted content is of good visual quality for the original image's color is also nearly recovered.

Table 2
Basis matrices partition of (2, 2) color transfer VCS.

Matrix elements	Encryption	
	Expanded subpixels	Color bit
$C_{00} = \begin{matrix}0&1\\0&1\end{matrix}$	$[000]^T$	0
$C_{01} = \begin{matrix}1&0\\1&0\end{matrix}$	$[000]^T$	1
$C_{10} = \begin{matrix}0&1\\1&0\end{matrix}$	$[111]^T$	0
$C_{11} = \begin{matrix}1&0\\0&1\end{matrix}$	$[111]^T$	1

Table 3
Basis matrices partition of (2, 3) color transfer VCS.

Category	Matrix elements
C_{00}	$\begin{bmatrix}1&0&0\\1&0&0\\1&0&0\end{bmatrix}$
C_{01}	$\begin{bmatrix}0&1&0\\0&1&0\\0&1&0\end{bmatrix}, \begin{bmatrix}0&0&1\\0&0&1\\0&0&1\end{bmatrix}$
C_{10}	$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}, \begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}, \begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}$
C_{11}	$\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}, \begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}, \begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}$

3.3. Examples

Two particular examples are given in this subsection to illustrate the principle of the CTVCS.

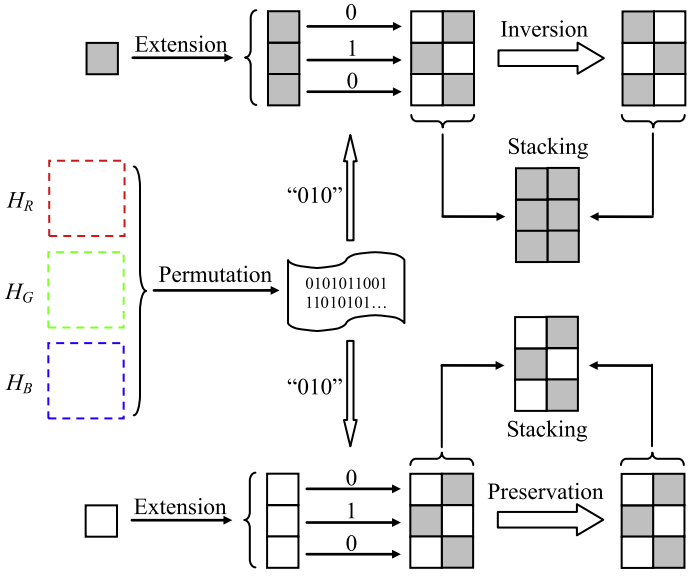

Fig. 5. An example of (2, 2) CTVCS encryption.

Fig. 6. Test images, Airplane, Lena and House (from left to right).

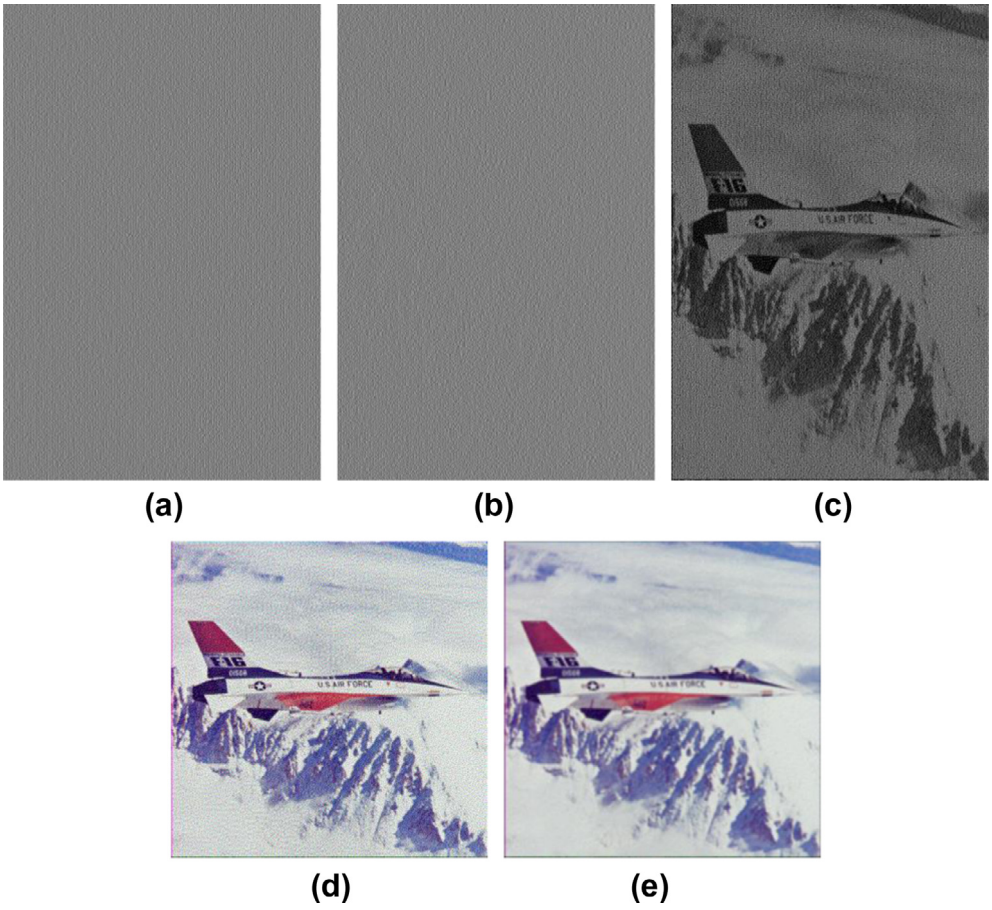

Fig. 7. (2, 2) CTVCS for Airplane, (a) transparency TP_1, (b) transparency TP_2, (c) TP_1 stacking TP_2, (d) reconstructed color halftone image, and (e) reconstructed color continuous-tone image with PSNR = 30.13 dB. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

3.3.1. (2, 2) CTVCS

The encryption of (2, 2) CTVCS is shown in Fig. 5. The basis matrices C_0 and C_1 are given in Eq. (5).

$$C_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad C_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{5}$$

The basis matrices partition is predetermined as Table 2 before secret sharing. It is a special case for each of C_{00}, C_{01}, C_{10} and C_{11} has only one matrix element, respectively.

3.3.2. (2, 3) CTVCS

Without loss of generality, another example is illustrated, i.e., (2, 3) CTVCS. The model can be constructed

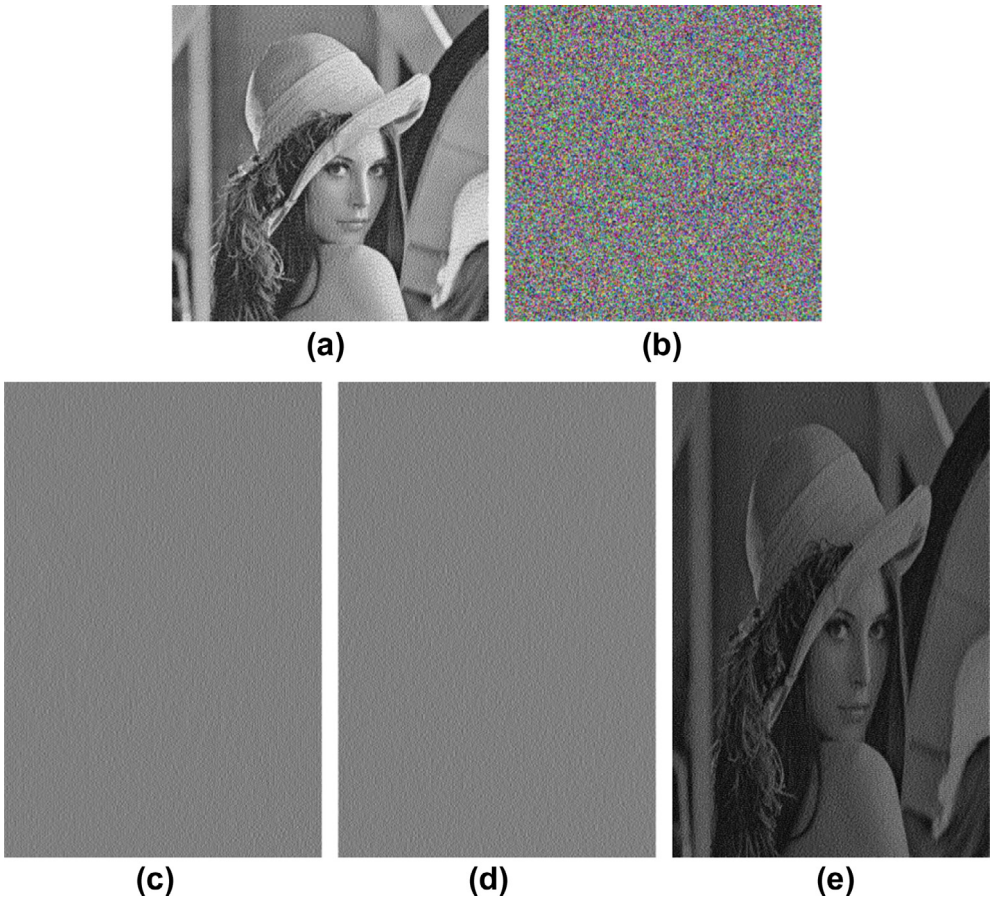

Fig. 8. Application for cheating prevention, (a) fake halftone image, (b) fake reconstructed color halftone image, (c) transparency TP_2, (d) fake transparency FTP_1, and (d) TP_2 stacking FTP_1. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

by the two following sets of 3 3 matrices, which obtained by permuting the columns of C_0 and C_1. Hence, there are 3 and 6 matrices can be selected as C_0 and C_1 candidates, respectively. The basis matrices C_0 and C_1 are given in Eq. (6).

$$C_0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad C_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{6}$$

Actually, each of C_{00}, C_{01}, C_{10} and C_{11} must have at least one matrix element although the number of elements may be different. For example, in the partition shown in Table 3, C_{00} and C_{01} have one and two elements, respectively, while both C_{10} and C_{11} have three matrices.

During encryption, the elements in C_{00}, C_{01}, C_{10} and C_{11} are randomly selected and the rows are assigned to 3 participants. Specifically, as long as a matrix is selected, its three rows are distributed to three independent participants one by one.

During decryption, each subpixel p_1 (likewise, p_2 and p_3) are expanded into a row of 3 subsubpixels. According to the "OR" operation, if only one of the pixels is "1", the subpixel is a white pixel. On the contrary, if 2 or more than 2 are "1"s, the subpixel is a black pixel.

4. Experimental results and discussion

As shown in Fig. 6, three 512 512 images, Airplane, Lena and House, are selected as test samples which are obtained from the USC-SIPI database [13].

Fig. 7 shows the results of (2, 2) CTVCS on Airplane. When stacking the two noise-like transparencies TP_1 and TP_2, the secret information is revealed as shown in Fig. 7(c). In Fig. 7(d), the reconstructed color halftone image is exactly the same as the original version. All of the transparencies and decrypted image via stacking are of the size 1536 1024, while the reconstructed color halftone and continuous-tone images are of the same size as that of the secret.

To evaluate the quality of reconstructed image, the color halftone image is convoluted with a Gaussian filter f as Eq. (8) which simulates HVS characteristics [14], and the resulted color continuous-tone image is shown in Fig. 7(e). The PSNR value in comparison with the original secret image can be achieved as 30.13 dB.

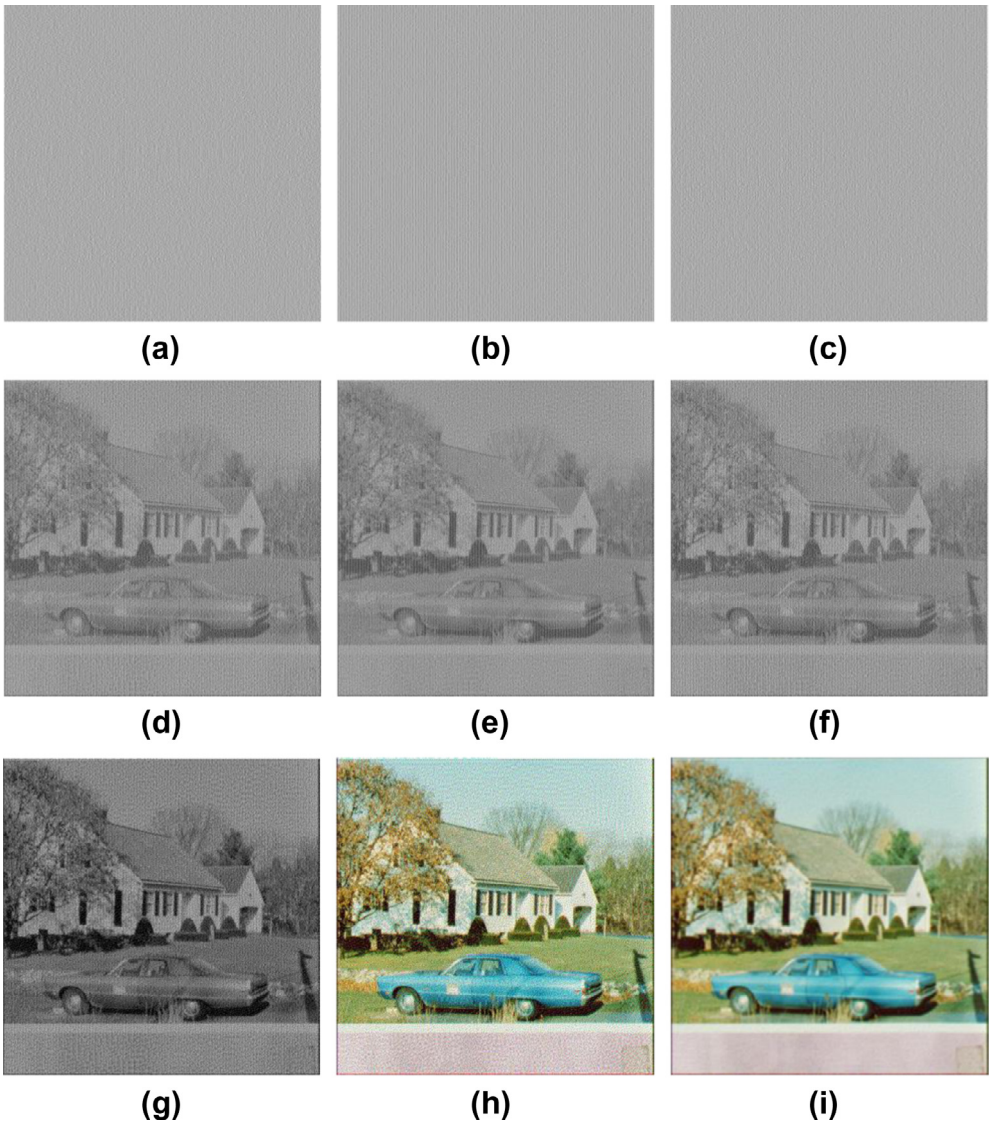

Fig. 9. (2, 3) CTVCS for Lena, (a) transparency TP_1, (b) transparency TP_2, (c) transparency TP_3, (d) TP_1 stacking TP_2, (e) TP_1 stacking TP_3, (f) TP_2 stacking TP_3, (g) stacking of TP_1, TP_2 and TP_3, (h) reconstructed color halftone image, and (i) reconstructed color continuous-tone image with PSNR = 30.06 dB. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

$$f = \frac{1}{11.566}\begin{bmatrix} 0.1628 & 0.3215 & 0.4035 & 0.3215 & 0.1628 \\ 0.3215 & 0.6352 & 0.7970 & 0.6352 & 0.3215 \\ 0.4035 & 0.7970 & 1 & 0.7970 & 0.4035 \\ 0.3215 & 0.6352 & 0.7970 & 0.6352 & 0.3215 \\ 0.1628 & 0.3215 & 0.4035 & 0.3215 & 0.1628 \end{bmatrix} \tag{7}$$

The reconstructed color image quality is determined by three factors. (1) The digital halftoning approach. Nowadays, many color halftoning methods can be selected, including ordered dithering, classical error diffusion, edge enhancement error diffusion, green noise error diffusion, block error diffusion, minimum brightness variation quadruple error diffusion, vector error diffusion, etc. Different methods correspond to different halftone qualities. The color halftoning method used in our case is a straightforward method among these alternatives. (2) The inverse halftoning technique. Plenty of inverse halftoning methods have been reported in literatures. The average reconstructed image PSNRs can be achieved as more than 30 dB. As human eyes are not sensitive to small distortions, the reconstructed color image quality is acceptable in most cases when PSNR > 30 dB. (3) The printing and scanning distortions. These distortions include rotation, shifting, and scaling on transparencies.

The reconstructed color halftone image is useful enough in many applications such as ChLCD display. As a general-purpose display technique, ChLCD is a burgeoning technique ideally suited battery powered portable devices including electronic paper book and outdoor advertising.

Table 4
Comparison of CTVCS and some representative work.

Indicator	Ref. [5]	Ref. [9]	Ref. [7]	Proposed
Model	(k, n)	(2, 2)	(k, n)	(k, n)
Secret image	Binary	Color	Binary	Color
Transparency image	Binary	Color halftone	Binary	Binary
Reconstructed quality level	Low	Medium	Low	Low, medium, high
Color transfer ability	No	Yes	No	Yes
Cheating prevention ability	No	No	No	Yes

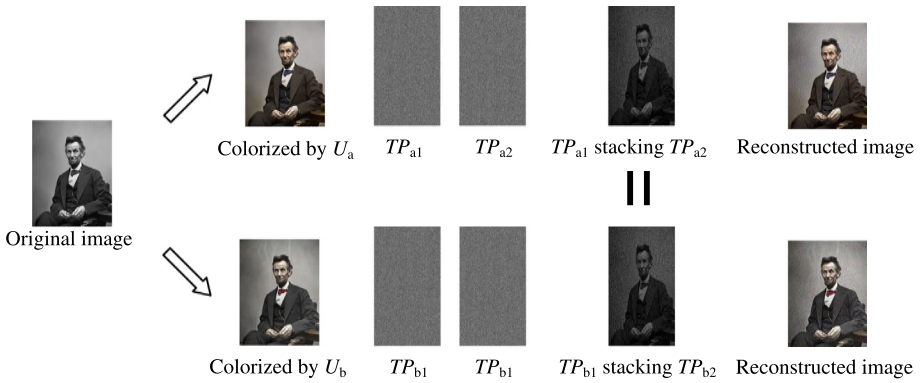

Fig. 10. Application of intellectual property protection in image colorization based on CTVCS.

Up to now, some ChLCD based commercial products (e.g., FLEPia) have been pushed to market by companies such as Fujitsu and Kent Displays. The CTVCS can be easily integrated with FLEPia for both of them are based on the principle of color halftone image display.

The conventional VCS models and many varieties often suffer from the problem of cheating prevention [15,16]. Therefore, cheating immune VCS has drawn much attention among researchers. CTVCS is a cheating immune method with the ability demonstrated in Fig. 8. Nothing is decrypted from the fake reconstructed color halftone image as shown in Fig. 8(b).

Fig. 9 shows the results of (2, 3) CTVCS on House. All of the transparencies and decrypted image via stacking are of the size 1536 1536, while the reconstructed color halftone and continuous-tone images are of the size 512 512. It is easily to find that when any two out of the three transparencies are collected, the secret information is revealed. If all the transparencies are polled, the visual quality of the stacking result is further enhanced. The PSNR of the reconstructed color continuous-tone image is 30.06 dB.

In the CTVCS model, the optimal partition of basis matrices is beneficial to the prototype's security. In general, symmetrical partition is recommended. For example, in Table 3, the choice between C10 and C11 is a symmetrical partition. In contrast, the partition between C00 and C01 is asymmetrical. The reasons lies in only three matrices can be used as candidates. In particular, in symmetrical partition, the specific matrices are selected randomly.

The CTVCS model is secure because it is based on the conventional (k, n) VCS model. In addition, the permutation key of color data, and the basis matrices partition can be kept secret to enhance security if the color information is required to be exploited as confidential data.

In fact, it also can be integrated with other variants. For example, it can be incorporated with Ito's image size invariant VCS [8]. The pixel expansion of one to three mapping should be applied, while the other operations can borrow ideas from the counterparts in [8].

The comparison of CTVCS and some representative work are shown in Table 4. The work in [5] is the first VCS prototype. The work in [9] is the first VCS designed for color image sharing. The work in [7] is an extensive research on halftone-based VCS. It is easily found that only the CTVCS has both color transfer and cheating prevention abilities. It maintains three levels decrypted results ranging from low, medium and high image qualities.

The CTVCS can be used for intellectual property protection [17,18] in image or video colorization. As an example shown in Fig. 10, a historical photo of Abraham Lincoln is captured as a grayscale image due to condition restriction. Then it is colorized by two users U_a and U_b independently. The colorization results can be regarded as the intellectual property of their specific painter. In particular, different colors may be added to the necktie and coat. Here the added color also can be regarded as an intellectual property and should be protected. Accordingly, the colors produced by each user may be kept secret from the others. CTVCS can be used in this scenario. When each user distributed their transparencies to the corresponding groups of participants, the stacking results are exactly the same, i.e., the original captured grayscale content. Nevertheless,

the individual color decryption can be realized as long as the correct key used. That is, two styles colorization results including color halftone and continuous-tone images can be reconstructed. This principle also can be extended to early black and white films colorization. The added color is protected based on CTVCS during the colorized video transmission and distribution.

5. Conclusions

A novel (k, n) color transfer visual cryptography scheme is proposed in this paper. With this model, a color image is encrypted to n binary transparencies and the color information can be nearly recovered from k binary transparencies or their hardcopies. Only some simple decryption computations and inverse halftoning procedures are involved on the digital transparencies. Averagely, the PSNR values of the reconstructed continuous-tone color images can be achieved as larger than 30 dB. Meanwhile, the basic advantages of the conventional VCS are still maintained, including the stacking decryption mechanism, perfect security, etc. The scheme is tailored for low cost output devices such as monochrome printer or fax machines. Also, the reconstructed halftone color images can be used for some low cost electronic products including cholesteric liquid crystal display device. The proposed scheme is cheating immune and can be used for and intellectual property protection in image and video recolorization.

Acknowledgement

This work is supported by the National Science Foundation of China (Grants Nos. 61003255 and 61171150), and Shenzhen Strategic Emerging Industries Program (Grant No. ZDSY20120613125016389). It is also partially supported by fund of Department of Education of Zhejiang Province (Grant No. Y201330167), and Zhejiang Provincial Natural Science Foundation of China (Grant No. LY12A04003).

References

[1] Z. Liu, S. Liu, M.A. Ahmad, Image sharing scheme based on discrete fractional random transform, Optik – Int. J. Light Electron Opt. 121 (6) (2010) 495–499.
[2] S. Bahrami, M. Naderi, Encryption of multimedia content in partial encryption scheme of DCT transform coefficients using a lightweight stream algorithm, Optik – Int. J. Light Electron Opt. 124 (18) (2013) 3693–3700.
[3] Z. Liu, Y. Zhang, H. Zhao, M.A. Ahmad, Shutian Liu, Optical multi-image encryption based on frequency shift, Optik – Int. J. Light Electron Opt. 122 (11) (2011) 1010–1013.
[4] Q. Zhang, L. Guo, X. Wei, A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system, Optik – Int. J. Light Electron Opt. 124 (18) (2013) 3596–3600.
[5] M. Naor, A. Shamir, Visual cryptography, Lect. Notes Comput. Sci. 950 (1995) 1–12.
[6] J. Weir, W. Yan, A comprehensive study of visual cryptography, Trans. Data Hid. Multimedia Secur. V, Lect. Notes Comput. Sci. 6010 (2010) 70–105.
[7] Z. Zhou, G.R. Arce, G.D. Crescenzo, Halftone visual cryptography, IEEE Trans. Image Process. 15 (8) (2006) 2441–2453.
[8] R. Ito, H. Kuwakado, H. Tanaka, Image size invariant visual cryptography, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E82-A (10) (1999) 2172–2177.
[9] Y.C. Hou, Visual cryptography for color images, Pattern Recogn. 36 (7) (2003) 1619–1629.
[10] L.H. Juang, M.N. Wu, MRI brain lesion image detection based on color-converted K-means clustering segmentation, Measurement 43 (7) (2010) 941–949.
[11] E. Reinhard, M. Ashikhmin, B. Gooch, P. Shirley, Color transfer between images, IEEE Comput. Graphics Appl. 21 (5) (2001) 34–41.
[12] R.L. de Queiroz, Reversible color-to-gray mapping using subband domain texturization, Pattern Recogn. Lett. 31 (4) (2010) 269–276.
[13] The USC-SIPI Image Database: <http://sipi.usc.edu/database>.
[14] S.M. Cheung, Y.H. Chan, A technique for lossy compression of error-diffused halftones, in: IEEE International Conference on Multimedia and Expo, 2004, pp. 1083–1086.
[15] C.M. Hu, W.G. Tzeng, Cheating prevention in visual cryptography, IEEE Trans. Image Process. 16 (1) (2007) 36–45.
[16] Q. Kong, P. Li, Y. Ma, On the feasibility and security of image secret sharing scheme to identify cheaters, J. Info. Hid. Multimedia Signal Process. 4 (4) (2013) 225–232.
[17] R.O. Preda, Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain, Measurement 46 (1) (2013) 367–373.
[18] R.O. Preda, D.N. Vizireanu, A robust digital watermarking scheme for video copyright protection in the wavelet domain, Measurement 43 (10) (2010) 1720–1726.
[19] B.W. Leung, F.Y. Ng, D.S. Wong, On the security of a visual cryptography scheme for color images, Pattern Recogn. 42 (2009) 929–940.
[20] H.C. Wu, H.C. Wang, R.W. Yu, Color visual cryptography scheme using meaningful shares, in: Eighth International Conference on Intelligent Systems Design and Applications, vol. 3, 2008, pp. 173–178.