Color Extended Visual Cryptography Using Error Diffusion

InKoo Kang, *Member, IEEE*, Gonzalo R. Arce, *Fellow, IEEE*, and Heung-Kyu Lee, *Member, IEEE*

***Abstract*—Color visual cryptography (VC) encrypts a color secret message into n color halftone image shares. Previous methods in the literature show good results for black and white or gray scale VC schemes, however, they are not sufficient to be applied directly to color shares due to different color structures. Some methods for color visual cryptography are not satisfactory in terms of producing either meaningless shares or meaningful shares with low visual quality, leading to suspicion of encryption. This paper introduces the concept of visual information pixel (VIP) synchronization and error diffusion to attain a color visual cryptography encryption method that produces meaningful color shares with high visual quality. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates shares pleasant to human eyes. Comparisons with previous approaches show the superior performance of the new method.**

***Index Terms*—Color meaningful shares, digital halftoning, error diffusion, secret sharing, visual cryptography (VC).**

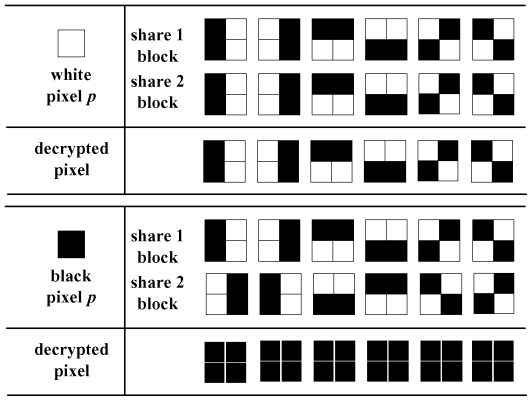

Fig. 1. Construction of (2, 2) VC scheme: a secret pixel is encoded into four subpixels in each of two shares. The decrypted pixel is obtained by superimposing the blocks in shares one and two.

I. Introduction

VISUAL CRYPTOGRAPHY (VC) is a type of secret sharing scheme introduced by Naor and Shamir [1]. In a k-out-of-n scheme of VC, a secret binary image is cryptographically encoded into n shares of random binary patterns. The n shares are xeroxed onto n transparencies, respectively, and distributed amongst n participants, one for each participant. No participant knows the share given to another participant. Any k or more participants can visually reveal the secret image by superimposing any k transparencies together. The secret cannot be decoded by any $k-1$ or fewer participants, even if infinite computational power is available to them. VC scheme proposed by Naor and Shamir [1] serves as a basic model and has been applied to many applications. Aside from the obvious applications to information hiding, there are many applications of VC, which include general access structures [2], copyright protection [3], watermarking [4], [5], visual authentication and identification [6], print and scan applications [7], etc.

To illustrate basic principles of VC scheme, consider a simple (2, 2)-VC scheme in Fig. 1. Each pixel p from a secret binary image is encoded into m black and white subpixels in each share. If p is a white (black) pixel, one of the six columns is selected randomly with equal probability, replacing p. Regardless of the value of the pixel p, it is replaced by a set of four subpixels, two of them black and two white. Thus, the subpixel set gives no clue as to the original value of p. When two subpixels originating from two white p are superimposed, the decrypted subpixels have two white and two black pixels. On the other hand, a decrypted subpixel having four black pixels indicates that the subpixel came from two black p pixels. Fig. 2 shows an example of a simple (2, 2)-VC scheme with a set of subpixels shown in Fig. 1. Fig. 2(a) shows a secret binary message, Fig. 2(b) and (c) depict encrypted shares for two participants. Superimposing these two shares leads to the output secret message as shown in Fig. 2(d). The decoded image is clearly identified, although some contrast loss is observed.

Several new methods for VC have been introduced recently in the literature. Blundo [8] proposed an optimal contrast k-out-of-n scheme to alleviate the contrast loss problem in the reconstructed images. Ateniese [2] proposed a more general method for VC scheme based upon general access structure. The access structure is a specification of qualified and forbidden subsets of shares. The participants in a qualified subset can recover the secret image while the participants

Manuscript received December 17, 2008; revised January 29, 2010 and May 30, 2010; accepted June 11, 2010. Date of publication July 08, 2010; date of current version December 17, 2010. A subset of this paper appeared at the IEEE ICASSP 2009Taipei, TaiwanApr.2009. This work was supported in part by the National Research Lab(NRL) program and WCU through the NRF of Korea funded by the MEST under Grant (R0A-2007-000-20023-0) and (R31-2010-000-30007-0), and by the MCST and KOCCA in the Culture Technology(CT) Research and Development Program 2009. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Oscar C. Au.

I. Kang and G. R. Arce are with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: ikkang@gmail.com; arce@ece.udel.edu).

H. Lee is with the Department of Computer Science and Division of Web Science and Technology(WCU), Korea Advanced Institute of Science and Technology, Daejeon, Republic of Korea (e-mail: hklee@mmc.kaist.ac.kr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIP.2010.2056376

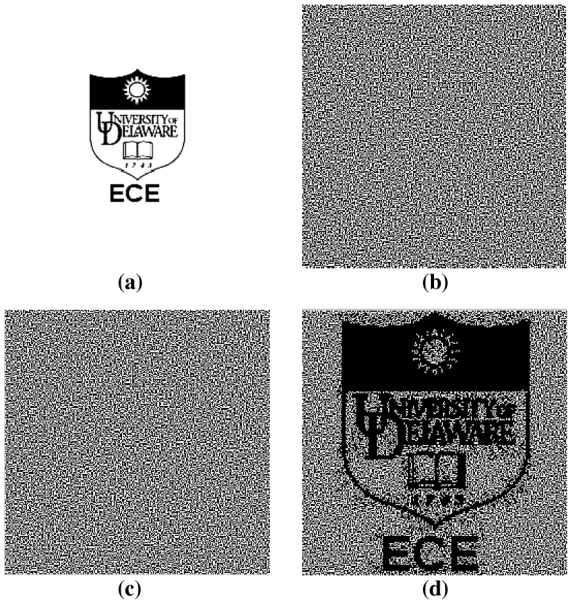

Fig. 2. Example of 2-out-of-2 scheme. The secret image is encoded into two shares showing random patterns. The decoded image shows the secret image with 50% contrast loss. (a) Binary secret image. (b) Encrypted share 1. (c) Encrypted share 2. (d) Decrypted secret message.

in a forbidden subset cannot. The VC scheme concept has been extended to grayscale share images rather than binary image shares [9]–[12]. Blundo [10] proposed VC schemes with general access structures for grayscale share images. Hou [13] transformed a gray-level image into halftone images and then applied binary VC schemes to generate grayscale shares. Although the secret image is grayscale, shares are still constructed by random binary patterns carrying visual information which may lead to suspicion of secret encryption.

Ateniese [14] developed a method of extended visual cryptography (EVC) in which shares contain not only the secret information but are also meaningful images. Hypergraph colorings are used in constructing meaningful binary shares. Since hypergraph colorings are constructed by random distributed pixels, the resultant binary shares contain strong white noise leading to inadequate results. Wang [15] generalized the Ateniese's scheme using concatenation of basis matrices and the extended matrices collection to achieve more simpler deviation of basis matrices. Nakajima [16] extended EVC to a scheme with natural grayscale images to improve the image quality. Zhou *et al.* [17] used halftoning methods to produce good quality halftone shares in VC. Fu [4] generated halftone shares that carry visual information by using VC and watermarking methods. Myodo [18] proposed a method to generate meaningful halftone images using threshold arrays. Wang et. al. [32] produced halftone shares showing meaningful images by using error diffusion techniques. This scheme generates more pleasing halftone shares owing to errors diffused to neighbor pixels.

Visual secret sharing for color images was introduced by Naor and Shamir [19] based upon cover semigroups. Rijimen [20] presented a 2-out-of-2 VC scheme by applying the idea of color mixture. Stacking two transparencies with different colors rises a third mixed color. Hou [13] devised schemes for color shares by applying halftone methods and color decomposition. Hou decomposed the secret color image into three (yellow, magenta and cyan) halftone images. He then devised three colored 2-out-of-2 VC schemes which follow the subtractive model for color mixture by exploiting some of the existing binary VC schemes. All of the previously mentioned methods, however, discuss color schemes for 2-out-of-2 [13], [20], [21] or 2-out-of-n [19] secret sharing where the reconstructed colors are interpreted by some mixing rules of colors. The general construction of a k-out-of-n VC scheme for the color shares was first introduced by Verheul [22]. He proposed a k-out-of-n VC scheme for a c-colored image with pixel expansion q^{k-1}, where $q \geq c$. Koga and Yamamoto [23] used a lattice structure to define the mixing result of arbitrary two colors. All of these VC schemes for color images produce random pattern shares. Even though the decrypted messages show messages with various colors, it is more desirable to generate meaningful shares which are less suspicious of encryption. Other approaches to color VC attempting to generate meaningful color shares include [14], [24], [25]. These methods, however, produce shares with low visibility due to color inconsistency across color channels as discussed in the experiment section of this paper. Ching-Nung Yand and Tse-Shih Chen proposed a VCS for color images based upon an additive color mixing method [26]. In this scheme, each pixel is expanded by a factor of three. We found that this scheme suffers from the problem of pixel expansion in the size of encrypted shares. In order to reduce the size of encrypted shares we propose the VC for color image using visual information pixel (VIP) synchronization with error diffusion technique.

This paper introduces a color VC encryption method which leads to meaningful shares and is free of the previously mentioned limitations. The method is simple and efficient. It relies on two fundamental principles used in the generation of shares, namely, error diffusion and VIP synchronization. Error diffusion is a simple but efficient algorithm for image halftone generation. The quantization error at each pixel is filtered and fed to future inputs. The error filter is designed in a way that the low frequency differences between the input and output images are minimized and consequently it produces pleasing halftone images to human vision. Synchronization of the VIPs across the color channels improves visual contrast of shares. In color VC schemes, the colors of encrypted pixels and the contrast can be degraded due to random matrix permutation. Random matrix permutations are key security features in VC schemes. In grayscale VC schemes, it does not affect the visual quality; however, in color schemes, independent execution of random matrix permutation for each color channel can cause color distortion by placing VIPs at random positions in subpixels which finally degrades the visual quality. VIP synchronization prevents the color and contrast of original images from degradation even with matrix permutation. We will further elaborate this feature in Section III-A.

The rest of this paper is organized as follows: Section II provides preliminaries about standard VC, the extended VC scheme, and the fundamentals of halftone techniques for easy understanding of the proposed VC method. Section III describes the proposed encryption method including the VC

matrix derivation method and a halftone process to generate final shares. Section IV shows experimental results of the new method and comparisons with previous approaches to prove its effectiveness. In Section V, we discuss topics about image quality, security and advantages of our scheme, and we conclude this paper in Section VI.

II. Preliminaries

In this section, we give a brief description of VC, extended VC, color models in VC and an error diffusion quantization. For more details about these topices, refer to [1], [14], and [17].

A. Fundamentals of VC

Generally, a (k, n)-VC scheme encrypts a secret message into n shares to be distributed to n participants. Each share shows noise-like random black and white patterns and does not reveal any information of the secret image by itself. In a k-out-of-n scheme, access to more than k shares allows one to recover the secret image by stacking them together, but access to less than k shares is not sufficient for decryption. A black and white (k, n)-VC scheme consists of two collections of $n \times m$ binary matrices S_0 and S_1, having elements denoted by 1 for a black pixel and 0 for a white pixel. To encrypt a white (black) pixel, a dealer randomly chooses one of the matrices in $S_0(S_1)$ and distributes its rows to the n participants. More precisely, a formal definition of the black and white (k, n)-VC scheme is given next.

Definition 1: Let k, n, m and h be nonnegative integers satisfying $2 \leq k \leq n$ and $0 \leq h \leq m$. The two collections of $n \times m$ binary matrices (S_0, S_1) constitute a black and white (k, n)-VC scheme if there exists a value $\alpha(> 0)$ satisfying the following.

1) Contrast: for any $s \in S_0$, the "OR" operation of any k out of n rows of s is a vector v that satisfies $w(v) \leq h - \alpha m$ where $w(v)$ is the Hamming weight of the vector v, m is the pixel expansion of the scheme and α is the contrast of the scheme.
2) Contrast: for any $s \in S_1$, the "OR" operation of any k out of n rows of s is a vector v that satisfies $w(v) \geq h$.
3) Security: for any $i_1 < i_2, \ldots, < i_t$ in $\{1, 2, \ldots, n\}$ with $t < k$, the two collections of $t \times m$ matrices D_j, $j = 0$, 1, obtained by restricting each $n \times m$ matrix in S_j, $j = 0$, 1, to rows $i_1, i_2, \ldots, i_t$, are indistinguishable in the sense that they contain the same matrices.

In the previously mentioned definitions, the first two contrast conditions ensure that the stacking of k out of n shares can recover the secret image. The security condition ensures that any less than k shares cannot get any information of the secret image other than the size of the secret image. That means no matter what the secret message pixel is 0 or 1, the expected appearances of a restricted matrix D_j is same, i.e., D_0 and D_1 are equal to a column permutation of the other in all possible ways [24].

Based upon the principle of VC, extended VC has been proposed whose shares take meaningful images rather than random noise-like patterns to avoid suspicion.

B. Extended VC

Generally, a (k, n)-EVC scheme takes a secret image and n original images as input and produces n encrypted shares with approximation of original images that satisfy the following three conditions:

- any k out of n shares can recover the secret image;
- any less than k shares cannot obtain any information of the secret image;
- all the shares are meaningful images; encrypted shares and the recovered secret image are colored.

Denote $S_c^{c_1, c_2, \ldots, c_n}$ as the collection of matrices from which the dealer chooses a matrix to encrypt, where $c, c_1, \ldots, c_n \in \{0, 1\}$. For $i = 1, \ldots, n$, c_i is the bit of the pixel on the ith original image and c is the bit of the secret message. For a black and white (k, n)-EVC scheme, we have to construct 2^n pairs of such collection $(S_0^{c_1, \ldots, c_n}, S_1^{c_1, \ldots, c_n})$, one for each possible combination of white and black pixels in the n original images. Here we give a definition of the black and white EVC scheme.

Definition 2: A family of 2^n pairs of collection of $n \times m'$ binary matrices $\{S_0^{c_1, \ldots, c_n}, S_1^{c_1, \ldots, c_n}\}_{c_1, \ldots, c_n \in \{0,1\}}$, constitute a black and white (k, n)-EVC scheme if there exist values $\alpha_F(> 0)$, $\alpha_S(> 0)$ and h satisfying the following.

1) Contrast: for any $M \in S_0^{c_1, \ldots, c_n}$ the "OR" operation of any k out of n rows of M is a vector v that satisfies $w(v) \leq (h - \alpha_F m)$, and for any $M \in S_1^{c_1, \ldots, c_n}$, $w(v) \geq h$.
2) Security: for any $i_1 < i_2 < \ldots < i_t$ in $\{1, 2, \ldots, n\}$ with $t < k$, the two collections of $t \times m'$ matrices $D_j^{c_1, \ldots, c_n}$, $j = 0$, 1, obtained by restricting each $n \times m'$ matrix in $S_j^{c_1, \ldots, c_n}$ to rows $i_1, i_2, \ldots, i_t$ are indistinguishable in the sense that they contain the same matrices.
3) Contrast: after the original images are encrypted they are still meaningful. Formally for any $i \in \{1, 2, \ldots, n\}$ and any $c, c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n \in \{0, 1\}$, denote $M[i]$ as the ith row of M, we have

$$\min_{M \in M_1} w(M[i]) - \max_{M \in M_0} w(M[i]) \geq \alpha_S m' \tag{1}$$

where

$$M_1 = \bigcup_{c, c_1, \cdots, c_n \in \{0,1\}} S_c^{c_1 \cdots c_{(i-1)} 1 c_{(i+1)} \cdots c_n} \quad \text{and}$$
$$M_0 = \bigcup_{c, c_1, \cdots, c_n \in \{0,1\}} S_c^{c_1 \cdots c_{(i-1)} 0 c_{(i+1)} \cdots c_n} \tag{2}$$

m' is the pixel expansion of the black and white (k, n)-EVC scheme.

α_F and α_S are the contrast of the recovered secret image and the contrast of the shares, respectively. The first and second conditions correspond to the contrast and security conditions of Definition 1. The third condition implies that after we encrypt the n original images by using the 2^n pairs of collections $\{(S_0^{c_1, \ldots, c_n}, S_1^{c_1, \ldots, c_n})\}$, the encrypted shares are still meaningful.

C. Color Models

The *additive* and *subtractive* color models are widely used to describe the constitutions of colors. In the additive color model, the three primary colors are red, green, and blue (RGB), with desired colors being obtained by mixing different RGB channels. By controlling the intensity of red, green, blue channels, we can modulate the amount of red, green, blue in the compound light. The more the colors are mixed, the more the brightness of

the light. When mixing all red, green and blue channels with equal intensity, white color will result. The computer screen is a good example of the additive color model. In the subtractive model, color is represented by applying the combination of colored-lights reflected from the surface of an object. By mixing cyan, magenta and yellow pigments, we can produce a wide range of colors. The more the pigments are added, the lower the intensity of the light is and, thus, the darker the light is. This is the reason it is called the subtractive model. Cyan, magenta, and yellow are the three primitive colors of pigment which cannot be composed from other colors. The color printer is a typical application of the subtractive model and, hence, the VC model of Naor and Shamir is also of such kind.

A natural color image can be divided into three color channels red, green and blue (cyan, magenta, and yellow, respectively) and each channel constitutes a grey-level image, where each pixel is represented by a 8-bit binary value. Denote $x_{(p,q)} = [x_{(p,q)1}, x_{(p,q)2}, x_{(p,q)3}]$ as the color of a pixel located at the position (p,q) of a color image of size $K_1 \times K_2$, for $p = 1,2,\ldots,K_1$ and $q = 1,2,\ldots,K_2$. Let t describe the color channel and the color component $x_{(p,q)t}$ is coded with 8-b binary value allowing $x_{(p,q)t}$ to be an integer value between 0 and 255. Hence, the color of the pixel $x_{(p,q)}$ can be expressed in a binary form as

$$x_{(p,q)} = \sum_{i=1}^{8} x^i_{(p,q)} 2^{8-i}$$

where $x^i_{(p,q)} = [x^i_{(p,q)1}, x^i_{(p,q)2}, x^i_{(p,q)3}] \in \{0,1\}^3$ denotes the binary vector at the ith bit-level with $i = 1$ denoting the most significant bit.

D. Error Diffusion

Error diffusion is a simple yet efficient way to halftone a grayscale image. The quantization error at each pixel is filtered and fed into a set of future inputs. Fig. 3 shows a binary error diffusion diagram where $f(m,n)$ represents the pixel at (m,n) position of the input image. $d(m,n)$ is the sum of the input pixel value and the diffused errors, $g(m,n)$ is the output quantized pixel value. Error diffusion consists of two main components. The first component is the thresholding block where the output $g(m,n)$ is given by

$$g(m,n) = \begin{cases} 1, & \text{if } d(m,n) \geq t(m,n) \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

The threshold $t(m,n)$ can be position dependant. The second component is the error filter $h(k,l)$ where the input $e(m,n)$ is the difference between $d(m,n)$ and $g(m,n)$. Finally, we compute $d(m,n)$ as

$$d(m,n) = f(m,n) - \sum_{k,l} h(k,l) e(m-k, n-l) \tag{4}$$

where $h(k,l) \in H$ and H is a 2-D error filter. A widely used filter is the error weight originally proposed by Floyd and Steinberg

$$h(k,l) = \frac{1}{16} \times \begin{bmatrix} & \bullet & 7 \\ 3 & 5 & 1 \end{bmatrix} \tag{5}$$

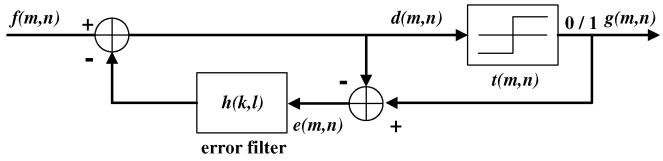

Fig. 3. Error diffusion block diagram. The pixel $f(m,n)$ is passed through a quantizer to obtain the corresponding pixel $g(m,n)$. The difference between these two, $e(m,n)$, is diffused away to the neighboring pixels by the filter $h(k,l)$. The threshold value $t(m,n)$ determines $g(m,n)$.

where $\bullet$ is the current processing pixel.

The recursive structure of the block diagram indicates that the quantization error $e(m,n)$ depends upon not only the current input and output but also the entire past history. The error filter is designed in such a way that the low frequency difference between the input and output image is minimized. The error that is diffused away by the error filter is high frequency or "blue noise." These features of error diffusion produce halftone images that are pleasant to human eyes with high visual quality [33], [34], and [35].

III. Color VC Encryption Based upon Pixel Synchronization and Error Diffusion

In this section, we describe the encryption method for color meaningful shares with a VIP synchronization and error diffusion. First, we describe the VC matrix derivation method for VIP synchronization from a set of standard VC matrices. We then introduce an error diffusion process to produce the final shares. The halftone process is independently applied to each cyan (C), magenta (M), and yellow (Y) color channel so each has only one bit per pixel to reveal colors of original images. A secret message is halftoned ahead of the encryption stage.

A. Matrix Derivation With VIP Synchronization

Our encryption method focuses on VIP synchronization across color channels. VIPs are pixels on the encrypted shares that have color values of the original images, which make the encrypted shares meaningful. In each of the m subpixels of the encrypted share, there are λ number of VIPs, denoted as c_i and the remaining $(m - \lambda)$ pixels deliver the message information of the secret message image. Thus, in our method, each subpixel m carries visual information as well as message information, while other methods in [1], [17], [22], and [24] extra pixels are needed in addition to the pixel expansion m to produce meaningful shares. Since each VIP is placed at the same bit position in subpixels across the three color channels, VIP represents accurate colors of the original image. We further elaborate on this feature in Section III-B.

First, we derive the basis matrices from a given set of matrices used in standard VC scheme. Algorithm 1 generates a set of basis matrices $S_c^{c_1,\ldots,c_n}$ $(c, c_1, \ldots, c_n \in \{0,1\})$ where c is a bit pixel from the message image and $c_1,\ldots,c_n$ indicate the corresponding pixel bits from the original images. In each row of $S_c^{c_1,\ldots,c_n}$, there are λ number of c_i and the values are unknown in the matrix derivation stage. Halftoning then defines actual bit values of c_i by referring the pixel values of original images and errors diffused away. The $w(S_c[i])$ in the algorithm is a

hamming weight of a "OR"-ed row vector up to ith rows in $S_c^{c_1,\cdots,c_n}$. It should be noted that the "OR"-ed row vector should not have any c_is as elements. Since the c_is are undefined values which can be defined as 0 or 1 in halftone stage, we cannot ensure the contrast difference between matrices $S_0^{c_1,\cdots,c_n}$ and $S_1^{c_1,\cdots,c_n}$. An example with given (2, 2)-VC scheme matrices is follows.

Algorithm 1 Construction of Matrices with VIP Synchronization

Given the matrices S_0 and S_1 of size $n \times m$, let $S_c[i_j]$ be a jth bit of ith row in S_c, $c \in \{0,1\}$ $(1 \le i \le n, 1 \le j \le m)$. Let γ be the number of 1's in each row of S_c and let λ indicate the number of c_i in each row of S_c $(1 \le \lambda \le m - \gamma - 1)$. The algorithm produces a set of matrices $S_c^{c_1,\cdots,c_n}$ $(c, c_1, \ldots, c_n \in \{0,1\})$.

1: **procedure** MATRICES CONSTRUCTION (S_0, S_1, λ)

2: **for** $i = 1, \cdots, n$ **do**

3: **for** $j = 1, \cdots, m$ **do**

4: (a): set $count = 0$

5: (b): if $S_0[i_j] = S_1[i_j] = 0$ is found, then $S_0[i_j] \leftarrow c_i$ and $S_1[i_j] \leftarrow c_i$ and $count = count + 1$.

6: goto (d) if $i < k$ or goto (e) if $i \ge k$.

7: (c): if $S_0[i_j] = S_1[i_j] = 0$ is not found, then switch element $S_0[i_{j1}]$ and $S_0[i_{j2}])$ $(j_1 \ne j_2)$ or

8: switch element $S_1[i_{j1}]$ and $S_1[i_{j2}])$ $(j_1 \ne j_2)$, and goto (b).

9: (d): if $count = \lambda$ and $i < k$, then goto (a) with i increased by 1.

10: (e): if $count = \lambda$ and $i \ge k$, then check if there exists an α satisfying:

$$W(S_1[i]) - W(S_0[i]) \ge \alpha \cdot m$$

if α exists, goto (a) with i increased by 1 until i reaches at n.

if α doest not exists, *undo* all changes of ith row and goto (c).

11: **end for**

12: **end for**

13: **end procedure**

Example 1 ((2, 2)-Color EVC Matrices Derivation): Consider the basis matrices S_0 and S_1 of (2, 2)-VC scheme with $m = 4$, $\lambda = 1$ such that

$$S_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad S_0 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}.$$

Let assume λ be 1, then the example given in the following generate the EVCS matrices VIP synchronized. The first row in each of the matrices S_1 and S_0 are (1100) and (1100). We begin by inserting the c_1s in the first row of each matrix as $(11c_10)$ and $(11c_10)$; the 0s at third position in each row is replaced with c_1. Check the step (d) and go back to step (a) with $i = 2$. For the second rows, the condition of $S_0[i_j] = S_1[i_j] = 0$ is not found. Switch the second and the third bits of S_1 by the step (c) leading (0101) for S_1. The condition $S_0[i_j] = S_1[i_j] = 0$ is found at third position and replace them with c_2 resulting in $(01c_21)$ for S_1 and $(11c_20)$ for S_0 by (b). So far, we have matrices $S_1^{c_1c_2}$ and $S_0^{c_1c_2}$ as

$$S_1^{c_1c_2} = \begin{bmatrix} 1 & 1 & c_1 & 0 \\ 0 & 1 & c_2 & 1 \end{bmatrix}, \quad S_0^{c_1c_2} = \begin{bmatrix} 1 & 1 & c_1 & 0 \\ 1 & 1 & c_2 & 0 \end{bmatrix}.$$

Go to the step (e) and check the condition, however, there is no α satisfying the condition. Un-do the changes of the second row and go back to the step (c). This time let the second bit and the third bit of S_0 be switched by (c), leading (1010). Then, we find the second bits of both matrices that meets the condition. Replace them with c_2 in both matrices by (b), then we then have matrices $S_1^{c_1c_2}$ and $S_0^{c_1c_2}$ as

$$S_1^{c_1c_2} = \begin{bmatrix} 1 & 1 & c_1 & 0 \\ 0 & c_2 & 1 & 1 \end{bmatrix}, \quad S_0^{c_1c_2} = \begin{bmatrix} 1 & 1 & c_1 & 0 \\ 1 & c_2 & 1 & 0 \end{bmatrix}.$$

By (e), the "OR"-ed vectors are (1111) for $S_1^{c_1c_2}$, (1110) for $S_0^{c_1c_2}$ and there exists the $\alpha = 1/4$ satisfying the contrast difference.

The algorithm guarantees the placement of c_i at the same positions in ith row of $S_c^{c_1c_2}$ and the corresponding ith rows of $S_c^{c_1c_2}$ are used to encrypt an ith share. Furthermore, each ith row in $S_0^{c_1c_2}$ and $S_1^{c_1c_2}$ are used to encrypt bit 0 and 1 on each color channel of original images, respectively. Thus, each encrypted subpixel has the same VIP positions across three channels, which means that these subpixels carry accurate visual information of the original images. In the example, subpixels on three color channels of the first share have VIPs at the third pixel and those of the second share have VIPs at the second pixel throughout all channels. Consequently, VIP positions are synchronized across channels regardless of pixel colors and this results in high visual quality of the encrypted shares.

B. Distribution of Matrices Across Color Channels

The encryption process starts with basis matrices distribution by referring secret message pixels. The encryption shares should be in a form of 3-b per pixel because they will be the results of the halftoned shares. Furthermore, the secret message of size $K_1 \times K_2$ should be halftoned ahead of the encryption stage as

$$X_{(p,q)} = \left[x^C_{(p,q)}, x^M_{(p,q)}, x^Y_{(p,q)}\right] \in \{0,1\}^3 \tag{6}$$

where $1 \le p \le K_1$, $1 \le q \le K_2$. $X_{(p,q)}$ is a pixel of the message image at location (p, q) composed of three binary bits $x^C_{(p,q)}, x^M_{(p,q)}, x^Y_{(p,q)}$ representing values for Cyan, Magenta and

Yellow color channels, respectively. Each message pixel composed of 3 b is encoded and expanded to subpixels of length m in the encrypted shares i as

$$X^i_{(p',q')} = \left[x^C_{(p',q')}, x^M_{(p',q')}, x^Y_{(p',q')}\right]^i \in \left\{S_0^{c_1,\cdots c_n}[i], S_1^{c_1,\cdots c_n}[i]\right\}^3 \quad (7)$$

where

$$\begin{aligned} &1 \le i \le n \\ &p' = p \cdot m_x - (m_x - 1) \\ &q' = q \cdot m_y - (m_y - 1) \\ &m = m_x \cdot m_y \end{aligned}$$

m_x and m_y are nonnegative integers and decide the aspect ratio of encryption shares. The $S_c^{c_1,\cdots,c_n}[i]$ is the ith row of the matrix $S_c^{c_1,\cdots,c_n}$. Each $X^i_{(p',q')}$ corresponds to subpixels on three channels starting at the position (p', q') and each subpixel takes one of the rows in $S_0^{c_1,\cdots,c_n}$ or $S_1^{c_1,\cdots,c_n}$ according to the bit value of the corresponding color channel of the message pixel. A Pseudo-code of the general algorithm for matrices distribution is described in Algorithm 2. This algorithm produces n encryption shares X^i. An example of the matrices distribution for (2, 2)-color EVC scheme is depicted in Fig. 4. Fig. 4(a) shows the matrices distribution along with each message pixel. Each binary bit on three color channels of message pixel is expanded into four subpixels on corresponding color channels throughout the n encryption shares by taking the matrix S_0 or S_1 according to its bit value. Since the VIPs are placed at the same spot on the ith row in matrices S_0 and S_1, each encrypted subpixels has the VIPs at the same positions throughout the color channels, where colored in gray in the figure. This feature makes the shares carry accurate colors of the original image after encryption. Fig. 4(b) depicts a decryption mechanism by the unit of subpixels showing how they present the desired color of the original message pixel. Regardless of the VIP values which will be decided in the error diffusion stage, the decrypted subpixels reveal the color of the message pixel $X_{(p,q)}$ with 1/4 contrast loss. Since the matrices S_0 and S_1 are derived in a way that the contrast difference is α, the decrypted subpixels show the intended color of the message pixel with probability α.

Algorithm 2 Matrices Distribution

For the basis matrices $S_0^{c_1,\cdots,c_n}$ and $S_1^{c_1,\cdots,c_n}$ of size $n \times m$, the secret image $X_{(p,q)}$ of size $K_1 \times K_2$ and encryption shares $X^i_{(p',q')}$, let $S_c^{c_1,\cdots,c_n}[i]$ be a ith row in $S_c^{c_1,\cdots,c_n}$, $c, c_n \in \{0, 1\}$ $(1 \le i \le n)$, $X_{(p,q)} = [x^C_{(p,q)}, x^M_{(p,q)}, x^Y_{(p,q)}] \in \{0, 1\}^3$ $(1 \le p \le K_1, 1 \le q \le K_2)$ and $X^i_{(p',q')} = [x^C_{(p',q')}, x^M_{(p',q')}, x^Y_{(p',q')}]^i \in \{S_0^{c_1,\cdots c_n}[i], S_1^{c_1,\cdots c_n}[i]\}^3$. m_x and m_y define the aspect ratio of subpixels m, where $m = m_x \times m_y$. The algorithm produces n matrix distributed shares X^i.

1: **procedure** MATRICES DISTRIBUTION $(X, S_0^{c_1,\cdots,c_n}, S_1^{c_1,\cdots,c_n})$

2: **for** $p = 1, \cdots, K_1$ and $q = 1, \cdots, K_2$ **do**

3: find the starting pixel position on share X^i, $p' = p \cdot m_x - (m_x - 1)$, $q' = q \cdot m_y - (m_y - 1)$

4: conduct random column permutation, $P(S_0^{c_1,\cdots,c_n}, S_1^{c_1,\cdots,c_n})$

5: **for** the color channel C of the secret message, $x^C_{(p,q)}$ **do**

6: **if** the bit $x^C_{(p,q)} = 1$, **then**

place ith row of the $S_1^{c_1,\cdots,c_n}$ to $[x^C_{(p',q')}]^i$ of size $m_x \times m_y$

$[x^C_{(p',q')}]^i$ goes to the channel C of the ith share

7: **else if** the bit $x^C_{(p,q)} = 0$, **then**

place ith row of the $S_0^{c_1,\cdots,c_n}$ to $[x^C_{(p',q')}]^i$ of size $m_x \times m_y$

$[x^C_{(p',q')}]^i$ goes to the channel C of the ith share

8: **end if**

9: **end for**

10: Repeat 5 to 9 for the channel M and Y.

11: **end for**

12: **end procedure**

The random permutation for S_0 and S_1 is done independently in standard VC schemes having one color channel. On the contrary, the random permutation of our scheme should be executed for $S_0^{c_1,\cdots c_n}$ and $S_1^{c_1,\cdots c_n}$ at the same time, denoted as $P(S_0^{c_1,\cdots c_n}, S_1^{c_1,\cdots c_n})$, since each row in the matrices has VIPs and their positions are correlated between $S_0^{c_1,\cdots c_n}$ and $S_1^{c_1,\cdots c_n}$. This feature should be reflected on the permutation process so as to preserve the VIP structure.

C. Share Generation via Error Diffusion

Once the distribution of the basis matrices is completed, a halftoning algorithm is applied to produce the final encrypted shares. Error diffusion is used in our scheme as it is simple and effective. The quantization error at each pixel is filtered and fed back to future inputs. Fig. 5(a) shows a binary error diffusion diagram designed for our scheme. To produce the ith halftone share, each of the three color layers are fed into the input.

The process of generating halftone shares via error diffusion is similar to that shown in Fig. 3 except that $f_{ij}(m, n)$ is the (m, n)th pixel on the input channel $j(1 \le i \le n, 1 \le j \le 3)$ of ith share. The other difference between our scheme from standard error diffusion is that the message information components, nonc_i, are predefined on the input shares such that they are not modified during the halftone process, i.e., the process is applied when the input is c_i. Fig. 5(b) depicts this process. 1s and 0s in black are message information pixels that should not

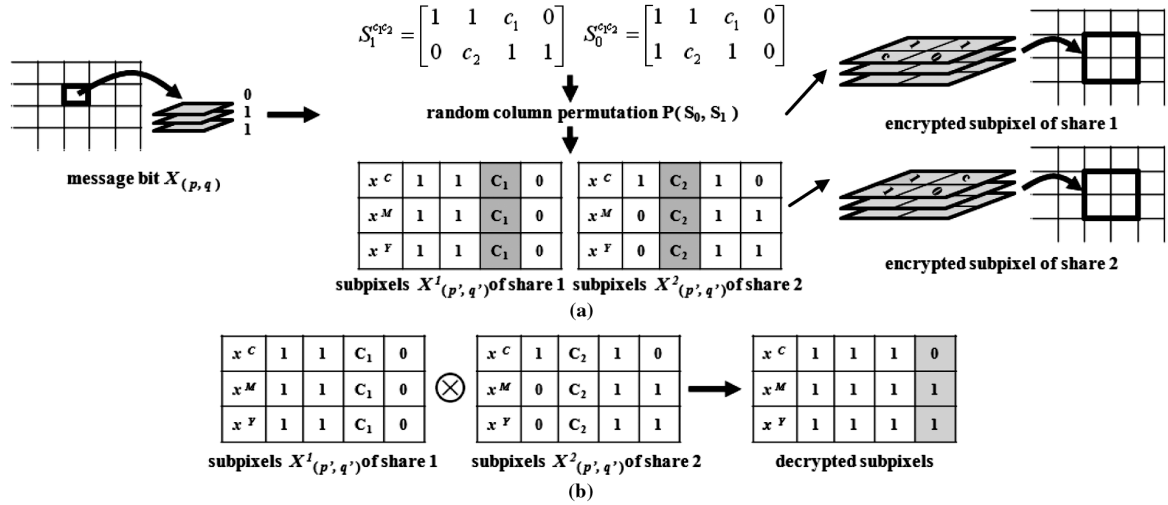

Fig. 4. General illustration of matrices distribution of (2, 2)-color EVC. (a) Matrices distribution along with a message pixel. Every message pixel composed of 3 b is encoded into four subpixels for each color channel by referring the bit value on each channel of message bit. The positions of VIPs across color channels where colored in gray are preserved after encryption. (b) Decryption example of subpixels. Regardless of VIP values, the decrypted subpixels represent the intended color, the same as that of the original message pixel, where colored in gray. The $\otimes$ represents the logical "OR" operation.

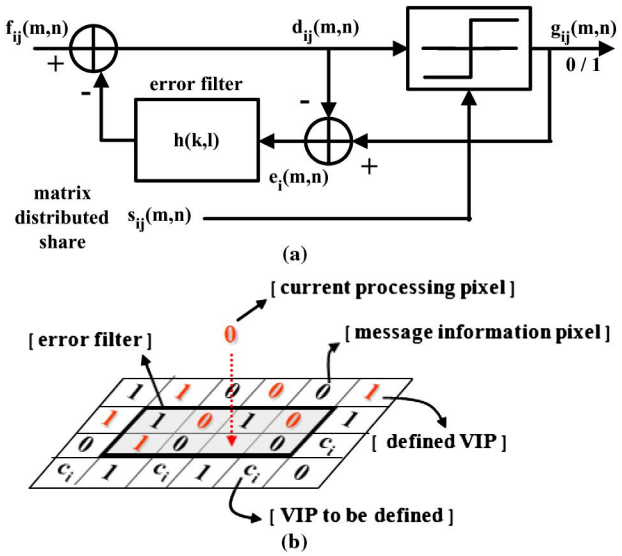

Fig. 5. (a) Block diagram of error diffusion with share encryption. If $s_{ij}(m,n)$ is a VIP, $g_{ij}(m,n)$ is determined by the output of the thresholding quantization. Otherwise, $g_{ij}(m,n)$ is prefixed. (b) Visualization of error diffusion with VIP. Digits in black are prefixed value and that in red are defined value by error diffusion. c_is are VIPs to be defined.

be modified and those are in red are VIPs that are already defined by the error diffusion. The c_i are also VIPs whose values are to be decided by referring the corresponding pixel values of original images and errors from neighboring pixels when the error filter window comes. Nonc_i elements, however, still affect $d_{ij}(m,n)$ and the quantization error $e_{ij}(m,n)$ when they are calculated in the filter window. The nonc_i elements may increase quantization errors added to the shares, but in turn, these errors are diffused away to neighboring pixels.

The visual quality of shares via error diffusion can be improved through edge enhancement methods [27]. The measure of a particular halftoning algorithm is its performance in DC regions and its performance near edges or in areas of high frequency image content can be manipulated through prefiltering the image prior to halftoning. So the remedy for the apparent blurring of edges caused by the error diffusion algorithm is to apply an edge sharpening filter prior to halftoning such that

$$X^i_{sharp}[n] = X[n] - \beta\,(\psi[n] * X[n]) \tag{8}$$

where $X[n]$ stands for the original image, $\psi[n]$ is a digital Laplacian filter, $*$ denotes convolution and β is a scalar constant ($\beta > 0$) regulating the amount of sharpening with larger β leading to a sharper image X^i_{sharp}. Consequently, error diffusion produces high quality halftone images. The effectiveness of error diffusion can be confirmed in the simulation result section.

IV. Simulation Results

In this section, we provide some experimental results to illustrate the effectiveness of the proposed method. Examples are composed with a (2,2)-color EVC and (3,4)-color EVC schemes. The secret message of size 128 $\times$ 128 pixels shows letters "U," "D," "E," and "L" in red, blue, green, and yellow, respectively. Original images "Lena" and "Baboon" of size 256 $\times$ 256 and "Lena," "Baboon," "Pepper," and "Flower" of size 384 $\times$ 256 in natural colors are provided for the share generation. We use two different metrics for visual quality comparison between the original images and the encrypted shares. First, we use the peak noise-to-signal ratio (PSNR) distortion measure and assume that the value of original images belong to a Gaussian distribution with $N(0,1)$. Second, we measure the visual quality of the encrypted shares using the perceived error method between the original images and the encrypted shares. The perceived error ϵ is the difference between perceived continuous-tone images and perceived halftone images calculated by employing an approximated human visual system (HVS) model [28]. Let $f[m,n]$ be the continuous-tone image and $f(x,y)$ be the rendition of this continuous-tone image by an ideal printer. An ideal printer is one that can reproduce an

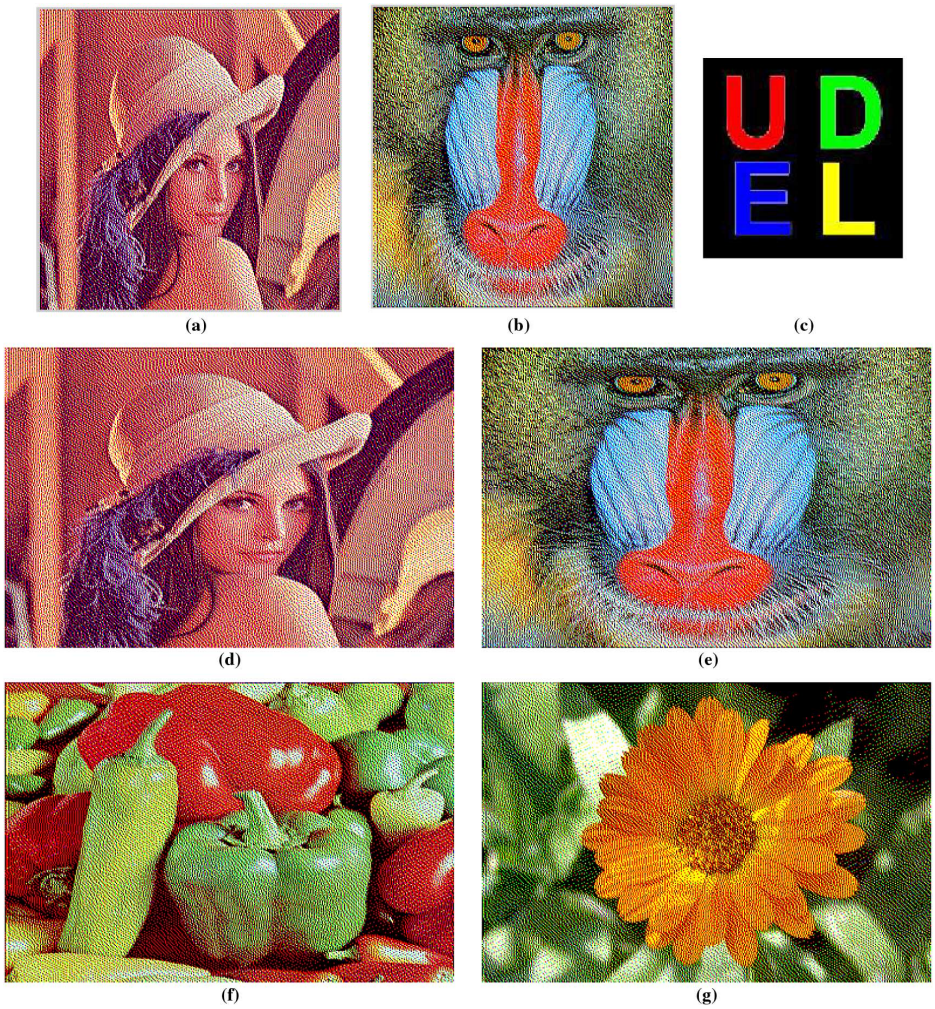

Fig. 6. Halftone shares using error diffusion with the *Floyd and Steinberg* error filter and the secret message. (a) and (b) Lena and Baboon of size 256 × 256 for a (2,2)-color EVC scheme. (d)–(g) Lena, Baboon, Pepper, Flower of size 384 × 256 for a (3,4)-color EVC scheme. (c) Secret message of size 128 × 128. PSNR: (a) 11.93 dB, (b) 11.78 dB, (d) 11.91 dB, (e) 11.73 dB, (f) 12.49 dB, and (g) 13.77 dB. Perceived error: (a) 6.04×10^{10}, (b) 1.74×10^{10}, (d) 4.74×10^{10}, (e) 2.72×10^{10} (f) 6.56×10^{10}, and (g) 1.09×10^{11}.

ideal square pixel equal to that of the continuous-tone pixel. Likewise, let $g[m,n] = 0$ or 1 represent the halftone image. Then, the perceived halftone image $\tilde{g}(x,y)$ is written as

$$\tilde{g}(x,y) = \sum_{m,n} g[m,n]\tilde{p}(x - mX, y - nY) \tag{9}$$

and the perceived continuous-tone image is written as

$$\begin{aligned}\tilde{f}(x,y) &= f(x,y) **h(x,y) \\ &= \sum_{m,n} f[m,n]\tilde{p}(x - mX, y - nY).\end{aligned} \tag{10}$$

The $**$ denotes 2-D convolution and $h(x,y)$ denotes point spread function of the HVS. The $p(x,y) = rect(x/X, y/Y)$ is the dot rendering function of an ideal printer and X and Y are the basis for the lattice of printer addressable dots in units of in/dot. The perceived error between the continuous-tone image and the halftone image is given by

$$\tilde{e}(x,y) = \tilde{g}(x,y) - \tilde{f}(x,y). \tag{11}$$

In Fig. 6, we present halftone shares of original images from (a) to (g). Fig. 6(a) and (b) are halftone images of Lena and Baboon of size 256 × 256, respectively. These two images are provided for the comparison with encrypted shares generated from a (2,2)-color EVC scheme. Fig. 6(d)–(g) are the halftone images of Lena, Baboon, Pepper, and Flower of size 384 × 256, respectively. These are for the comparison with encrypted shares from a (3,4)-color EVC scheme. Fig. 6(c) is the secret message to be cryptographically coded into each of the shares. The PSNRs and perceived errors for each shares are shown in the figure.

Fig. 7 shows the results of a (2,2)-color EVC scheme to prove the effectiveness of the proposed method. In the (2,2)-color EVC, we applied the set of matrices as

$$S_1^{c_1c_2} = \begin{bmatrix} 0 & 1 & 1 & c_1 \\ 1 & c_2 & 0 & 1 \end{bmatrix}, \quad S_0^{c_1c_2} = \begin{bmatrix} 1 & 1 & 0 & c_1 \\ 1 & c_2 & 0 & 1 \end{bmatrix}. \tag{12}$$

Fig. 7(a) and (d) show encryption results of grayscale EVC schemes in [1], [14], [24], and [25],applied to color shares. They show relatively low contrast with barely recognizable shape of the images leading PSNR 10.43 dB and 10.39 dB, perceived error 1.22×10^{11} and 1.09×10^{11}, respectively. The methods

may work well in a black and white or grayscale VC schemes, however, they do not produce satisfactory results in color EVC due to the random permutation at each color channel. Fig. 7(b) and (e) are provided to verify the effectiveness of error diffusion. They are generated from the proposed method in this paper without the error diffusion stage. VIPs are simply copied to the encrypted shares from the halftone shares. Color contrast is improved compared with that of (a) and (d) owing to VIP synchronization so we easily recognize outlines of the shares. PSNR for two shares are slightly increased to 10.81 dB and 10.93 dB and the perceived errors are decreased to 1.04×10^{11} and 6.76×10^{10} for Baboon and Lena, respectively; however, details are still not clear and overall color particles are rough. Fig. 7(c) and (f) are shares from the proposed scheme with the VIP synchronization and the error diffusion methods. In this example, we use Floy–Steinberg error filter shown in (5) for the error diffusion. Output dependent threshold modulation is employed and the threshold $t(m,n)$ at a location (m,n) is given by

$$t(m,n) = 0.25 + 0.33 \times 0.25 \times \left(g(m,n-1) + g(m,n-2) + g(m,n-2)\right). \quad (13)$$

The threshold modulation tries to adjust the current threshold by using the information of three preceding halftone pixels. The proposed scheme with parameters of $m = 4$, $\gamma = 2$ and $\lambda = 1$ produces these shares leading to PSNR 11.00 dB and 11.09 dB and the perceived errors to 7.86×10^{10} and 5.91×10^{10}, respectively. In this example, one out of four pixels is the VIP, however, this one VIP is correlated throughout three color channels and error diffusion produces more natural and pleasing shares to human eyes. Consequently, encrypted shares present better visual quality showing specific details of shares with more vivid colors compared with previous examples. Fig. 9(e) shows the decrypted secret message by stacking two shares Fig. 7(c) and (f) and all letters are in desired colors and clearly recognizable.

Our encryption method is not limited to the two-out-of-two scheme. We show a simulation result for a more general (3,4)-color EVC schemes derived from a standard set of basis matrices in [24]. Fig. 8 is provided to compare the proposed method with standard color EVC: PSNR and perceived error are also denoted. Fig. 8(a)–(d) are shares generated from methods in [1], [14], [24], and [25]. Similarly to the shares of (2,2)-color EVC scheme in Fig. 7(a) and (d), this method produces shares having low color contrast, barely recognizable outlines of shape as well as relatively low PSNR and perceived errors. Fig. 8(e)–(h) show encrypted shares from the proposed method without error diffusion. These shares show more clear outlines of shape and present higher color contrast to human eyes than shares of (a) to (d). In Table II, we can compare the quality of these shares with other ones from different schemes. For comparison, the proposed scheme with $m = 6$, $\gamma = 3$, $\lambda = 2$ is presented in the following. The basis matrices for a scheme with $m = 6, \gamma = 3$, $\lambda = 2$ is

$$S_1^{c_1c_2c_3c_4} = \begin{bmatrix} 0 & c_1 & 1 & 1 & 1 & c_1 \\ 1 & c_2 & 1 & 1 & c_2 & 0 \\ 1 & 1 & c_3 & c_3 & 0 & 1 \\ 0 & 1 & c_4 & 1 & c_4 & 1 \end{bmatrix}$$

$$S_0^{c_1c_2c_3c_4} = \begin{bmatrix} 0 & c_1 & 1 & 1 & 1 & c_1 \\ 0 & c_2 & 1 & 1 & c_2 & 1 \\ 0 & 1 & c_3 & c_3 & 1 & 1 \\ 0 & 1 & c_4 & 1 & c_4 & 1 \end{bmatrix} \quad (14)$$

where $c_i (1 \le i \le 4)$ is the VIP which will be decided during error diffusion. Four halftone images "Lena," "Baboon," "Pepper," and "Flower" of size 384×256 for the visual comparison are shown in Fig. 6 and the corresponding encrypted shares are presented in Fig. 9(a)–(d) with PSNR and perceived errors. The PSNR values are increased and perceived errors are decreased more than that of corresponding shares of Fig. 8. Each original image pixel p is expanded into six subpixels and two subpixels carry visual information of the source images leading to the contrast of the encrypted shares 2/6. Fig. 9(f) are the decrypted secret message by stacking (a), (b), (c), and (d). The contrast of the decrypted share calculated as

$$\frac{w\left(S_1^{c_1,\cdots,c_n}\right) - w\left(S_0^{c_1,\cdots,c_n}\right)}{m} \quad (15)$$

is 1/6, where the $w(S)$ indicates a hamming weight of a "OR"-ed row vector of all rows in matrices S. All message letters are clearly denoted in desired colors and any residue images of encrypted shares are not shown.

Fig. 9(g) and (h) show the decrypted messages of standard encryption shares from Fig. 7(a) and (d), Fig. 8(a)–(d), respectively. Even though they have the same visual contrast when decrypted as that of the proposed method, the encrypted shares from the proposed method have more improved visual quality in terms of showing vivid colors as well as details cause of VIP synchronization and error diffusion. Again, it should be noted that main contribution of the proposed method is to improve the visual quality of the encrypted shares compared to that of previous methods.

Lastly, we present the overall perceived errors for various cases of encryption to see the effectiveness of the proposed scheme. Table I denotes perceived errors of shares from the (2,2)-color EVC scheme and the Table II is for the (3,4)-color EVC scheme. We executed the (2,2)-color EVC scheme with two sets of input images to present the perceived errors for four shares. In the tables, we present the perceived error values for the proposed method in details with sharpening effects. As mentioned before, a sharpening process prior to error diffusion improves the visual quality on high frequency areas. We applied the Laplacian filter ahead of error diffusion with $\beta = 1$ and $\beta = 2$ in the (8). In the tables, we provide from nine different schemes for four original images; a halftone share, a standard EVC, a proposed scheme without error diffusion, three schemes with different β for the proposed scheme with $q = 1$ and $q = 2$. We can see the perceived error of the standard scheme is the worst in all cases and that of the proposed scheme with β are larger than that of other schemes. Moreover, the proposed scheme with larger q leads lower perceived error values and schemes with larger β with same q produces shares having low perceived error. We observe similar situation in the Table II for (3,4)-color EVC experiments.

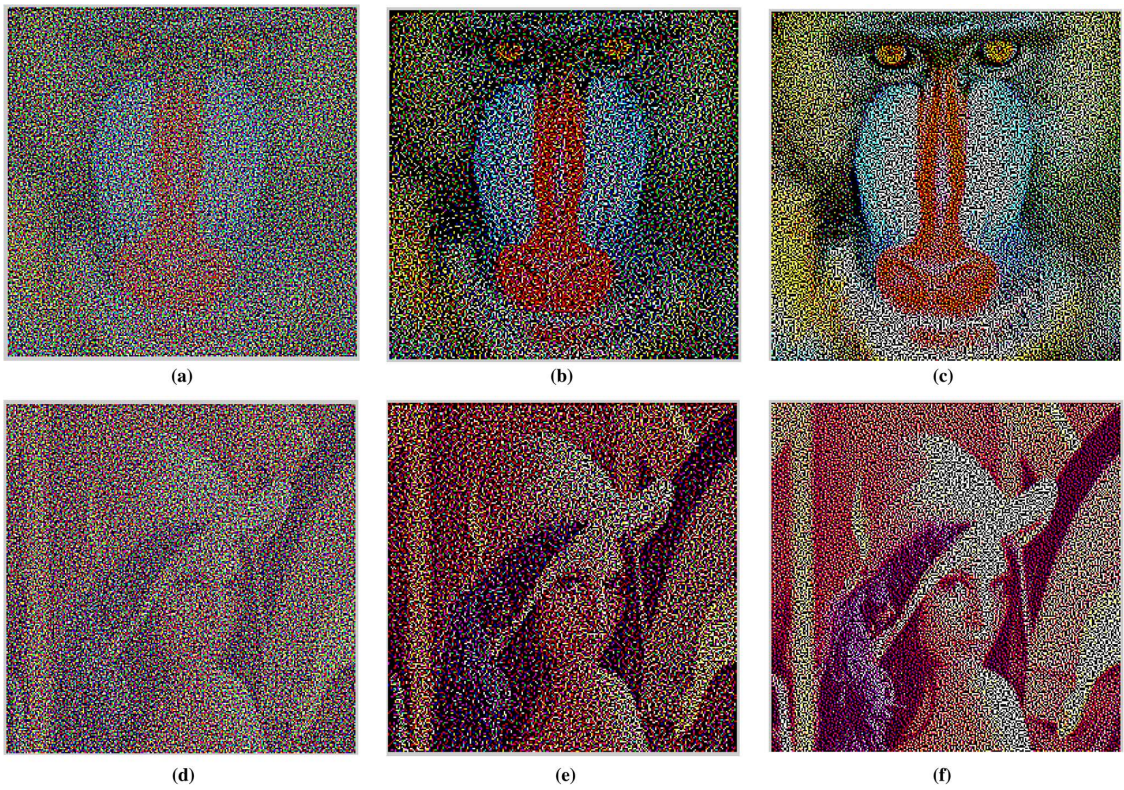

Fig. 7. Experimental results of (2,2)-color EVC scheme. (a) and (d) Shares from standard EVC in [1], [14], [24], and [25]. (b) and (e) Shares with the proposed method without the error diffusion. (c) and (f) Shares of the proposed method with $m = 4$, $\gamma = 2$, $\lambda = 1$. PSNR: (a) 10.43 dB, (b) 10.81 dB, (c) 11.00 dB, (d) 10.39 dB, (e) 10.93 dB, and (f) 11.09 dB. Perceived error: (a) 1.22×10^{11}, (b) 1.04×10^{11}, (c) 7.86×10^{10}, (d) 1.09×10^{11}, (e) 6.76×10^{10}, and (f) 5.91×10^{10}.

V. Discussion

A. Visual Quality of Shares

VIPs are assigned freely to carry the visual information of original images in each subpixels m. Visual quality of the encrypted shares and of the decrypted share, denoted as Q_e and Q_d, respectively, mostly depends upon the size of pixel expansion m, and λ, the number of VIPs and γ, the number of 1 s in each m. The Q_e and Q_d are represented as

$$Q_e = \frac{\lambda}{m} \tag{16}$$

and

$$\begin{aligned} Q_d(=\alpha) &= \frac{w\left(s_1^{c_1,\cdots,c_n}\right) - w\left(s_0^{c_1,\cdots,c_n}\right)}{m} \\ &= 1 - \frac{\gamma+\lambda}{m}. \end{aligned} \tag{17}$$

We assume that the $w(s_1^{c_1,\cdots,c_n})$ in Q_d is m, meaning all elements of the "OR"-ed row vector of the matrix $s_1^{c_1,\cdots,c_n}$ are 1. The Q_d has the same value as contrast difference α in the Algorithm I.

For the Q_e, smaller m and larger q, indicating more number of VIPs in a small pixel expansion, produce better visual quality shares. On the contrary, for the Q_d, larger m and smaller γ and λ are desirable for the reconstructed share with high contrast. Consequently, there exists a tradeoff relationship between m and q for encryption shares and the decryption share and the decision of parameters is up to the purpose of applications. For a scheme with parameters $m = 6$, $\gamma = 3$, $\lambda = 1$ and one with $m = 6$, $\gamma = 3$, $\lambda = 2$, the Q_e and Q_d of the former are 1/6 and 2/6, and those for the latter are 2/6 and 1/6. The higher contrast of encryption shares, the lower contrast of the decryption share, and vice versa.

The error filter employed in the error diffusion also affects the share quality. An error filter with longer weight leads to high contrast of encryption shares [29]. Since Floyd and Steinberg's filter was first introduced, many modifications to the original error diffusion algorithm have been introduced that address the unwanted artifacts of the original algorithm. A typical problem that occurs is spectral whitening where the variation in average separation distance between minority pixels becomes so great that the pattern starts to resemble the halftone pattern created by white noise. In an effort to break up worm patterns in error diffusion, Jarvis and Stucki introduced 12-element error filters and it is apparent that both filters break up worms at extreme gray levels [27]. Another factor that affects the quality is the position-dependent threshold in the error diffusion stage. To produce better quality shares, output-dependent threshold modulation can be used in the error diffusion to suppress unwanted textures [30].

B. Advantages of Our Scheme

The scheme proposed generates high quality of meaningful color shares as well as the colorful decrypted share using VIP synchronization and error diffusion methods. The VIPs are pixels that carry pixel values of original images to make shares meaningful. When these VIPs are not assigned during

Fig. 8. Encrypted shares of (3,4)-color EVC scheme. (a)–(d) Shares from standard EVC in [1], [14], [24], and [25]. (e)–(h) Shares from the proposed method without the error diffusion. PSNR: (a) 9.70 dB, (b) 9.50 dB, (c) 8.32 dB, (d) 8.95 dB, (e) 9.51 dB, (f) 9.30 dB, (g) 7.91 dB, and (h) 8.64 dB. Perceived error: (a) 1.57×10^{11}, (b) 1.13×10^{11}, (c) 2.61×10^{11}, (d) 1.74×10^{11}. (e) 1.36×10^{10}, (f) 1.35×10^{11}, (g) 2.55×10^{11}, and (h) 1.51×10^{11}.

the halftone stage, the resultant shares are the same as that of standard VC schemes except the colorful decrypted messages. Other schemes deal with EVC schemes in color, however, they do not consider relationship throughout color channels. Some schemes produce colorful noise-like random patterns [13], [31]. Our scheme deals with all these considerations. Furthermore, most color EVC schemes in [1], [17], [21], and [24] need extra pixel expansion in addition to m, the pixel expansion of standard VC schemes, however, we need only m. This feature reduces needless space for one pixel encryption and finally produces shares with as less as possible pixel expansion.

In standard EVC schemes, they need 2^n pairs of collection of $n \times m'$ binary matrices $\{C_0^{c_1,\cdots,c_n}, C_1^{c_1,\cdots,c_n}\}$ to encrypt meaningful shares for n participants, where m' is the pixel expansion of the black and white (k, n)-EVC scheme. Each matrix has n rows having predefined contrast differences in accordance with bit values $c_1, \cdots, c_n$ of original images. In our scheme, however, since the contrast difference is defined in the error diffusion stage as a output of threshold block, we do not need to save all 2^n pairs of matrices of size $n \times m'$ ahead of the encryption stage, but we need space for only two matrices S_0 and S_1.

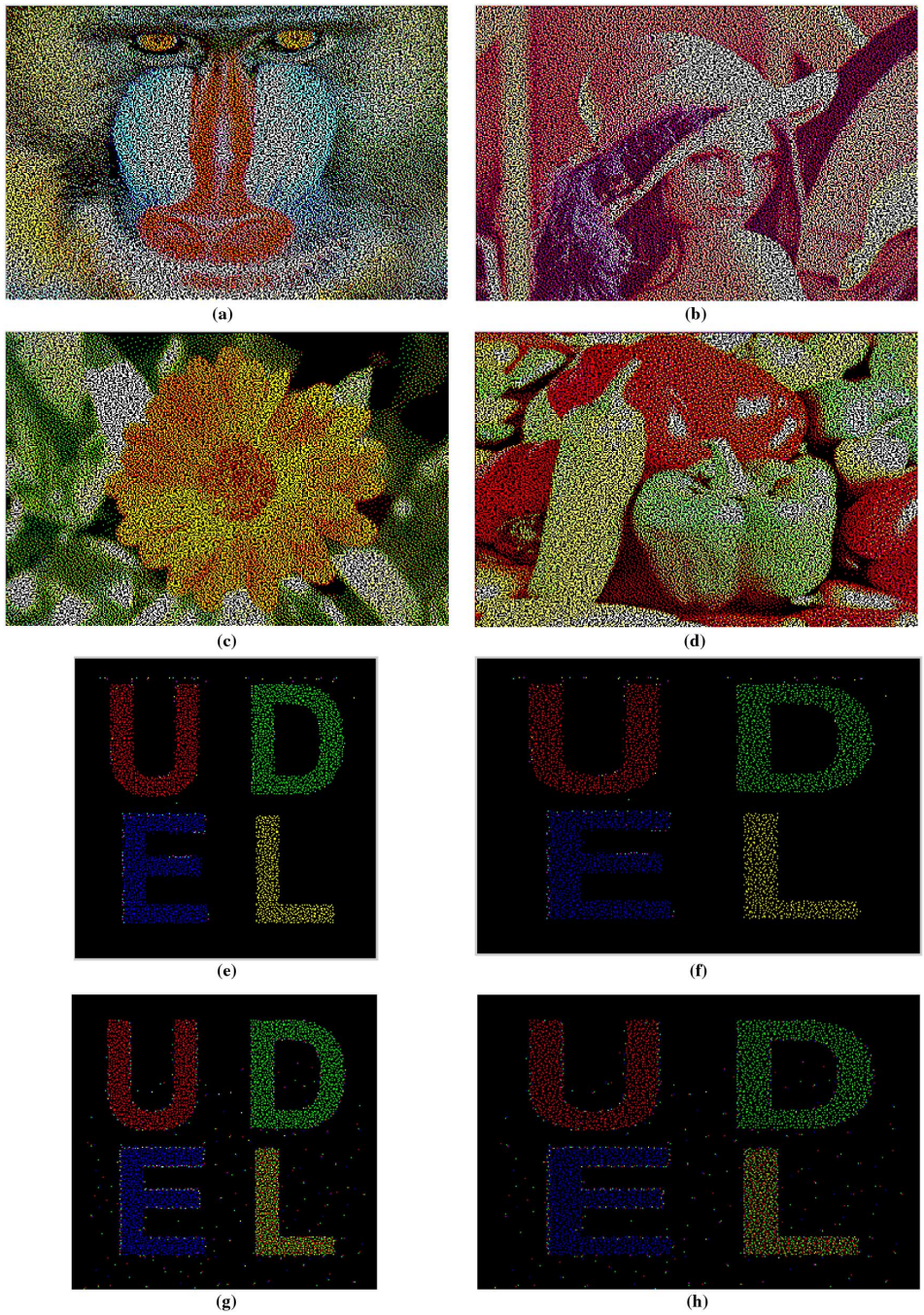

Fig. 9. (a)–(d) Encrypted shares of (3,4)-color EVC scheme using the proposed method with parameters $m = 6, \gamma = 3, \lambda = 2$, leading visual contrast of 2/6. PSNR: (a) 10.84 dB, (b) 10.83 dB, (c) 11.23 dB (d) 11.23 dB. Perceived error: (a) 4.97×10^{10}, (b) 6.98×10^{10}, (c) 1.73×10^{11}, and (d) 1.66×10^{11}. (e) Decoded message from shares (c) and (f) of (2,2)-color EVC scheme in Fig. 7, leading contrast 1/4, (f) a decoded message from shares (a) to (d) of (3,4)-color EVC scheme, leading contrast 1/6. (g) Decoded message from shares (a) and (d) of (2,2)-standard scheme in Fig. 7 with contrast 1/4. (h) Decoded message from shares (a) to (d) of (3,4)-standard scheme in Fig. 8 with contrast 1/6.

C. Security of Our Scheme

In our scheme, each row of basis matrices S_0 and S_1 has the same number of 1 s, 0 s and c_is, regardless of the original image pixel color and the message pixel color is. That means each of the encrypted share has the same amount of information about the original images and the secret message. Furthermore, in some cases without legitimate number of participants, k they have false information about the secret message because the VIP is decided during the error diffusion step. The hamming weight of $S_1[i]$, $W(S_1[i])$, should be greater than $W(S_0[i])$ in the decrypted share, but decryption with less than k shares can cause $W(S_1[i]) \leq W(S_0[i])$ which leads false decrypted information. Only with proper number of shares the correct contrast difference is achieved. Unlike standard EVCS, the robustness of our proposed scheme to cheating comes from that fact that it is impossible to differentiate VIPs and other pixels in the encrypted shares and it is hard to know the actual VIP values which were decided during the error diffusion.

TABLE I
PERCEIVED ERRORS OF (2,2)-COLOR EVC SCHEME: SHARES OF SIZE 256 × 256

	halftone shares	standard scheme [a]	w/o error diffusion	Proposed scheme with $q = 1$			Proposed scheme with $q = 2$		
				w/o filter	Laplacian β=1	Laplacian β=2	w/o filter	Laplacian β=1	Laplacian β=2
Lena	6.04×10^{10}	1.09×10^{11}	6.76×10^{10}	5.91×10^{10}	3.62×10^{10}	7.03×10^{10}	4.99×10^{10}	3.14×10^{10}	8.97×10^{11}
Baboon	1.74×10^{10}	1.22×10^{11}	1.04×10^{11}	7.86×10^{10}	6.74×10^{10}	4.76×10^{10}	2.35×10^{10}	1.87×10^{10}	2.63×10^{10}
Pepper	4.74×10^{10}	1.52×10^{11}	1.31×10^{11}	1.03×10^{11}	8.88×10^{10}	8.72×10^{10}	7.50×10^{10}	5.34×10^{10}	7.69×10^{10}
Flower	8.48×10^{10}	1.93×10^{11}	1.78×10^{11}	1.62×10^{11}	1.55×10^{11}	1.52×10^{11}	1.10×10^{11}	1.02×10^{11}	8.87×10^{10}

[a] This is from EVC schemes in [1], [14], [24], and [25] applied to color shares.

TABLE II
PERCEIVED ERRORS OF (3,4)-COLOR EVC SCHEME: SHARES OF SIZE 384 × 256

	halftone shares	standard scheme [b]	w/o error diffusion	Proposed scheme with $q = 1$			Proposed scheme with $q = 2$		
				w/o filter	Laplacian β=1	Laplacian β=2	w/o filter	Laplacian β=1	Laplacian β=2
Lena	4.74×10^{10}	1.13×10^{11}	1.35×10^{11}	1.09×10^{11}	1.01×10^{11}	8.16×10^{10}	6.98×10^{10}	6.73×10^{10}	6.98×10^{10}
Baboon	2.72×10^{10}	1.57×10^{11}	1.36×10^{11}	9.35×10^{10}	8.07×10^{10}	8.22×10^{10}	4.97×10^{10}	4.57×10^{10}	4.20×10^{10}
Pepper	6.56×10^{10}	1.74×10^{11}	1.51×10^{11}	1.09×10^{11}	1.03×10^{11}	8.95×10^{10}	1.66×10^{11}	1.27×10^{11}	1.02×10^{11}
Flower	1.09×10^{11}	2.61×10^{11}	2.55×10^{11}	2.16×10^{11}	2.01×10^{11}	1.78×10^{11}	1.73×10^{11}	1.26×10^{11}	1.19×10^{11}

[b] This is from EVC schemes in [1], [14], [24], and [25] applied to color shares.

VI. CONCLUSION

This paper develops an encryption method to construct color EVC scheme with VIP synchronization and error diffusion for visual quality improvement. VIPs synchronize the positions of pixels that carry visual information of original images across the color channels so as to retain the original pixel values the same before and after encryption. Error diffusion is used to construct the shares such that the noise introduced by the preset pixels are diffused away to neighbors when encrypted shares are generated. It is obvious that there is a tradeoff between contrast of encryption shares and the decryption share, however, we can recognize the colorful secret messages having even low contrast. Either VIP synchronization or error diffusion can be broadly used in many VC schemes for color images.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Proc. EUROCRYPT* , 1994, pp. 1–12.

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

[3] A. Houmansadr and S. Ghaemmaghami, "A novel video watermarking method using visual cryptography," in *Proc. IEEE Int. Conf. Eng. Intell. Syst.*, 2006, pp. 1–5.

[4] M. S. Fu and O. C. Au, "Joint visual cryptography and watermarking," in *Proc. IEEE Int. Conf. Multimedia Expo*, 2004, pp. 975–978.

[5] C. S. Hsu and Y. C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," *Opt. Eng.*, vol. 44, p. 077003, 2005.

[6] M. Naor and B. Pinkas, "Visual authentication and identification," *Adv. Cryptol.*, vol. 1294, pp. 322–336, 1997.

[7] W. Q. Y, J. Duo, and M. Kankanhalli, "Visual cryptography for print and scan applications," in *Proc. IEEE Int. Symp. Circuits Syst.*, 2004, pp. 572–575.

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

[9] L. A. MacPherson, "Gray level visual cryptography for general access structrue," M. Eng. thesis, Univ. Waterloo, Ontario, Canada, 2000.

[10] C. Blundo, A. D. Santis, and M. Naor, "Visual cryptography for grey level images," *Inf. Process. Lett.*, vol. 75, no. 6, pp. 255–259, 2000.

[11] Y. T. Hsu and L. W. Chang, "A new construction algorithm of visual crytography for gray level images," in *Proc. IEEE Int. Symp. Circuits Syst.*, 2006, pp. 1430–1433.

[12] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, vol. 24, pp. 349–358, 2003.

[13] Y. C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, pp. 1619–1629, 2003.

[14] G. Ateniese, C. Blundo, A. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *ACM Theor. Comput. Sci.*, vol. 250, pp. 143–161, 2001.

[15] D. S. Wang, F. Yi, and X. Li, "On general consturction for extended visual cryptography schemes," *Pattern Recognit.*, pp. 3071–3082, 2009.

[16] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *J. WSCG*, vol. 10, no. 2, 2002.

[17] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," *IEEE Trans. Image Process.*, vol. 18, no. 8, pp. 2441–2453, Aug. 2006.

[18] E. Myodo, S. Sakazawa, and Y. Takishima, "Visual cryptography based on void-and-cluster halftoning technique," in *Proc. IEEE Int. Conf. Image Process.*, 2006, pp. 97–100.

[19] M. Naor and A. Shamir, "Visual cryptography II: Improving the contrast via the cover base," *Lect. Notes Comput. Sci.*, vol. 1189, pp. 197–202, 1997.

[20] V. Rijimen and B. Preneel, "Efficient color visual encryption for shared colors of benetton," presented at the Proc. Eurocrypto Rump Session, 1996 [Online]. Available: http://www.iacr.org/conferences/ec96/rump/index.html

[21] C. N. Yang, "A note on efficient color visual encryption," *J. Inf. Sci. Eng.*, vol. 18, pp. 367–372, 2002.

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

[23] H. Koga and H. Yamamoto, "Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images," *IEICE Trans. Fundamentals*, vol. E81-A, no. 6, pp. 1262–1269, Jun. 1998.

[24] S. Droste, "New results on visual cryptography," in *Proc. 16th Annu. Int. Cryptol. Conf. Adv. Cryptol.*, London, UK, 1996, pp. 401–415.

[25] R. Lukac and K. N. Plataniotis, "Colour image secret sharing," *Electron. Lett.*, vol. 40, no. 9, pp. 529–531, Apr. 2004.

[26] C. N. Yang and T. S. Chen, "Visual cryptography scheme based on additive color mixing," *Pattern Recognit.*, vol. 41, pp. 3114–3129, 2008.

[27] D. L. Lau and G. R. Arce, *Modern Digital Halftoning*. New York: Marcel Dekker, 2001.

[28] S. H. Kim and J. P. Allebach, "Impact of hvs models on model-based halftoning," *IEEE Trans. Image Process.*, vol. 11, no. 3, pp. 258–269, Mar. 2002.
[29] R. A. Ulichney, "Dithering with blue noise," *Proc. IEEE*, vol. 76, no. 1, pp. 56–79, Jan. 1988.
[30] R. Escbbach, Z. Fan, K. T. Knox, and G. Marcu, "Threshold modulation and stability in error diffusion," *IEEE Signal Process. Mag.*, vol. 20, no. 4, pp. 39–50, Jul. 2003.
[31] S. J. Shyu, "Efficient visual secret sharing scheme for color images," *Pattern Recognit.*, vol. 39, no. 5, pp. 866–880, May 2006.
[32] Z. M. 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.
[33] D. L. Lau, G. R. Arce, and N. C. Gallagher, "Digital halftoning by means of green-noise masks," *J. Opt. Soc. Amer. A*, vol. 16, no. 7, pp. 1575–1586, Jul. 1999.
[34] D. L. Lau, G. R. Arce, and N. C. Gallagher, "Digital color halftoning with generalized error diffusion and multichannel green-noise masks," *IEEE Trans. Image Process.*, vol. 9, no. 5, pp. 923–935, May 2000.
[35] D. L. Lau, R. Ulichney, and G. R. Arce, "Blue- and green-noise halftoning models - A review of the spatial and spectral characteristics of halftone textures," *IEEE Signal Process. Mag.*, vol. 20, no. 4, pp. 28–38, Jul. 2003.

InKoo Kang (M'09) received the B.S. degree in computer engineering from Konkuk University, Seoul, Korea in 2002, and the M.S. and Ph.D. degrees in computer science from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2004 and 2007, respectively.

From 2007 to 2009, he was a Postdoctoral Researcher at the University of Delaware, Newark, DE. He joined the Digital Imaging Business Department, Samsung Electronics Co., Ltd., in 2009, where he is currently a Senior Research Engineer. His main research activity has been in various areas of multimedia security, digital watermarking, digital fingerprinting, visual cryptography, image processing, etc.

Gonzalo R. Arce (F'00) is the Charles Black Evans Professor of Electrical and Computer Engineering at the University of Delaware, Newark, DE. He currently holds the Fulbright-Nokia Distinguished Chair in Information and Communications Technologies at the Aalto University, Helsinki, Finland. He has held visiting professor appointments at the Tampere University of Technology and the Unisys Corporate Technology Center. He served as Department Chair at the University of Delaware from 1999 to 2009. His research interests include statistical signal processing, nonlinear signal processing, computational imaging, and network science.

Dr. Arce is the recipient of several awards including the DuPont Young Investigator Award, the NSF Research Initiation Grant, and a fellowship from the Center for Advanced Studies at the University of Delaware. He is coauthor of the texts *Nonlinear Signal Processing* (Wiley, 2004), *Modern Digital Halftoning* (CRC Press, 2008), and *Computational Lithography* (Wiley, 2010). He has served as associate editor of several journals of the IEEE and the OSA.

Heung-Kyu Lee (M'09) received the B.S. degree in electronics engineering from the Seoul National University, Seoul, Korea, in 1978, and the M.S. and Ph.D. Degrees in computer science from the Korea Advanced Institute of Science and Technology (KAIST), in 1981, and 1984, respectively.

Since 1986, he has been a Professor in the Department of Computer Science, KAIST. He is also a General Director for the Center of Fusion Technology for Security (CFTS). He is an author/coauthor of more than 160 international journal and conference papers. His major interests are information hiding and multimedia forensics.

Dr. Lee has been a reviewer of many international journals, *the Journal of Electronic Imaging, Real-Time Imaging*,the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, etc. He was also program chairman of many international conferences including the International Workshop on Digital Watermarking (IWDW) in 2004 and the IEEE International Conference on Real-Time Systems and Applications.