COLOR EXTENDED VISUAL CRYPTOGRAPHY USING ERROR DIFFUSION

InKoo Kang, Gonzalo R. Arce

University of Delaware
Department of Elecrtical and Computer Engineering
Newark, Delaware, 91716, USA

Heung-Kyu Lee

Korea Advanced Institute of Science and Technology
Department of Computer Science
Gwahangno, Daejeon, Republic of Korea

ABSTRACT

This paper introduces a color visual cryptography encryption method that produces meaningful color shares via visual information pixel (VIP) synchronization and error diffusion halftoning. VIP synchronization retains the positions of pixels carrying visual information of original shares 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 visual cryptography, error diffusion

1. INTRODUCTION

Visual cryptography (VC) is a type of secret sharing scheme introduced by Naor [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. To illustrate a basic principle of VC, consider a simple $(2,2)$-VCS 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 come from two black p pixels.

The concepts of VC have been extended such that the secret image is allowed to be a grayscale image rather than a binary image [2]. Although the secret image is grayscale, shares are still constructed by random binary patterns. The limitation of all the above mentioned methods lies in the fact that all shares generated are random patterns carrying no visual information. Extended VCS has been suggested in [3] where hypergraph colorings are used in constructing meaningful binary shares. Since hypergraph colorings are constructed by random distributed pixels, the resultant binary share contain strong white noise leading to inadequate results. Zhou *et. al* used halftoning methods to produce good quality halftone shares in VC [4]. Other approaches to color VC attempting to generate meaningful shares include [5], [6]. These methods, however, produce shares with low visibility due to color inconsistency across color channels as shown in Fig.3 (b).

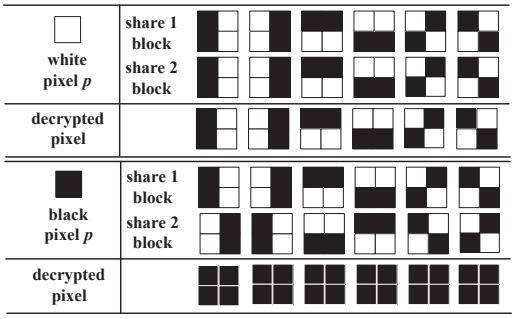

Fig. 1. Conventional visual cryptography

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 pixel synchronization. Error diffusion is a simple but efficient algorithm for image halftone generation. The quantization error at each pixel is filtered and fed back to future inputs. The error filter is designed in a way that the low frequency difference between the input and output image is minimized and subsequently it produces pleasing halftone images for human vision. Synchronizing the visual information pixels across the color channels improves visual contrast of shares. In color VCS, colors of encrypted pixels and contrast can be degraded due to matrix random permutation causing color noise-like patterns.

This work was supported by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD). KRF-2007-357-D00238.

Visual information pixel synchronization prevents colors and contrast of original shares from degradation even with matrix permutation.

The rest of this paper is organized as follows: in Section 2 introduces our proposed encryption method including matrix derivation method and halftone processing to generate final shares. Section 3 gives experimental results to show the effectiveness of our scheme and we will finalize this paper in Section 4.

2. COLOR VC ENCRYPTION BASED ON 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 shares. A secret message is halftoned ahead of the encryption stage.

2.1. Matrix Derivation for VIP Synchronization

Our encryption method focuses on VIP synchronization across color channels. First, we derive basis matrices from a given set of matrices used in standard VCS. Algorithm 1 generates a set of basis matrices $S_c^{c_1,c_2,\ldots,c_n}$ $(c, c_1, \ldots, c_n \in \{0,1\})$ where c is a pixel bit from the message and $c_1, \ldots, c_n$ indicate the corresponding pixel bits from the shares.

VIPs are pixels that have color information of the original shares, which make the encrypted shares meaningful. In each row of $S_c^{c_1,\ldots,c_n}$, there are q number of VIPs, denoted as c_i and the values are unknown in the matrix derivation stage. The halftone processing defines actual bit values of c_i by referring the pixel values of original shares and errors diffused away. The $w(S_c[i])$ in the algorithm is a hamming weight of a 'OR'-ed row vector up to i-th rows in $S_c^{c_1,\ldots,c_n}$. The 'OR'-ed row vector should not have c_i as elements, since the c_is are undefined values in this stage we cannot ensure the contrast difference between $S_0^{c_1,\ldots,c_n}$ and $S_1^{c_1,\ldots,c_n}$. A simple example with given $(2,2)$-VCS matrices is follows:

Example 1 *Consider a given basis matrices S_0 and S_1 of $(2,2)$-VCS with $m = 4$, $p = 2$ and a given $q = 1$:*

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

The first row in each of the matrices S_1 and S_0 are (1001) and (1100). We begin by inserting the c_1 in the first row of each matrix as $(10c_11)$ and $(11c_10)$. That is, the 0s at the third position in each row is replaced with c_1. For the second rows, we find the fourth positions and replace them with c_2 leading to $(011c_2)$ and $(110c_2)$. So far we have matrices $S_1^{c_1c_2}$ and $S_0^{c_1c_2}$ as :

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

The 'OR'-ed row vectors in S_1 gives (1111), however that of S_0 produces $(11c_1c_2)$. Since the 'OR'-ed vector of S_0 has c_1 and c_2, this cannot ensure the contrast difference between S_0 and S_1. It could be a (1111) when c_1 and c_2 are defined as 1. To prevent this, we need to switch some bit positions in S_1 and S_0 to place c_is at the same positions as well as to guarantee the contrast difference. We switch the second and fourth columns of S_1 and the second and third bits of the second row in S_0. Replace the second bit '0' with c_2 in S_0 and S_1, we then have matrices $S_1^{c_1c_2}$ and $S_0^{c_1c_2}$ as:

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

The 'OR'-ed vectors are (1111) for $S_1^{c_1c_2}$, (1110) for $S_0^{c_1c_2}$ and there exists the $\alpha = 1/4$.

Algorithm 1 Matrices construction with VIP synchronization

For given matrices S_0 and S_1 of size $n \times m$, let $S_c[i_j]$ be a j-th bit of i-th row in S_c, $c \in \{0,1\}$ $(1 \le i \le n, 1 \le j \le m)$. The p is the number of 1 and the given q is the number of c_i in a row i of S_c $(1 \le q \le m - p - 1)$.
procedure MATRICES CONSTRUCTION(S_0, S_1, q)
  for $i = 1$ **do**
    for $l \leftarrow 1, q$ **do**
      if $S_0[1_j] = S_1[1_j] = 0$ **then**
        $S_0[1_j] \leftarrow c_1$ and $S_1[1_j] \leftarrow c_1$
      end if
    end for
  end for
  for $i = 2, n$ **do**
    for $l \leftarrow 1, q$ **do**
      repeat
        if $S_0[i_j] = S_1[i_j] = 0$ **then**
          $S_0[i_j] \leftarrow c_i$ and $S_1[i_j] \leftarrow c_i$
        else
          switch$(S_0[i_{j1}], S_0[i_{j2}])$ or
          switch$(S_1[i_{j1}], S_1[i_{j2}])$,
          where $j_1 \neq j_2$
        end if
      until if there exists an α satisfying
      $w(S_1[i]) - w(S_0[i]) \geq \alpha m$
    end for
  end for
end procedure

The algorithm guarantees the placement of c_i at the same positions in each rows of S_c and corresponding i-th rows of

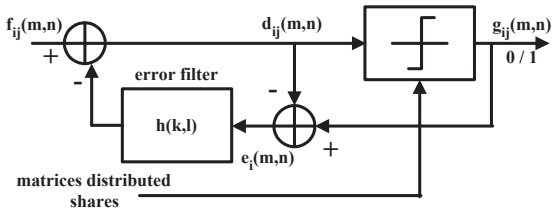

Fig. 2. Error diffusion combined with encryption shares.

S_c are used to encrypt an i-th share. Furthermore, each i-th row in S_0 and S_1 are used to encrypt bit 0 and 1 on each color channel of original shares, 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 shares. In the example, subpixels on three channels of the first share have VIP at the third pixel and those of the second share have VIP at the second pixel throughout all channels. Consequently, VIP positions are synchronized across channels regardless of pixel colors and this results in high color contrast of the encrypted shares.

Once the basis matrices are derived, the other encryption methods are the same as the standard EVCS scheme [3] except for the way of matrices permutation. Subpixel encryptions of three channels corresponding to each message pixel p is followed by the random permutation while it is executed ahead of the subpixel encryption in other methods. Furthermore, a set of encrypted subpixels for three channels should be permutated at the same time to preserve the VIP synchronization. In this way, we complete the matrix distribution stage with VIP synchronization.

2.2. Halftone share 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. 2 shows a binary error diffusion diagram designed for our scheme. To produce the i-th halftone share, each of the three color layers are fed into the input. Let $f_{ij}(m,n)$ be the (m,n)-th pixel on the input channel j $(1 \le i \le n, 1 \le j \le 3))$ of i-th share. The input to the threshold quantization is:

$$d_{ij}(m,n) = f_{ij}(m,n) - \sum_{k,l} h(k,l) e_{ij}(m-k, n-l), \quad (1)$$

where $h(k,l) \in H$ and H is a two dimensional error filter. The $e_{ij}(m,n)$ is a difference between $d_{ij}(m,n)$ and $g_{ij}(m,n)$. The $g_{ij}(m,n)$ is a quantized output pixel value given by :

$$g_{ij}(m,n) = \left\{ \begin{array}{c} 1, \text{ if } d_{ij}(m,n) \ge t_{ij}(m,n), \\ 0, \text{ otherwise,} \end{array} \right\} \quad (2)$$

where threshold $t_{ij}(m,n)$ can be position-dependent. The recursive structure of the block diagram indicates that the quantization error $e_{ij}(m,n)$ depends on not only a current input and output but also the entire past history. The error filter minimizes low frequency differences between the input and output images, in addition the error is high frequency or "blue noise". Consequently, those features generate pleasing halftone images for human vision.

The difference between our scheme from standard error diffusion is that the message information components, non-c_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. Non-c_i elements, however, still affect only $d_{ij}(m,n)$ and the quantization error $e_{ij}(m,n)$. The non-c_i elements may increase quantization error added to the shares, but in turn, these errors are diffused away to neighboring pixels. Consequently, error diffusion produces high quality halftone images. The effectiveness of error diffusion can be confirmed in the simulation result.

3. SIMULATION RESULTS

In this section, we provide experimental results illustrating the effectiveness of the proposed methods. Examples are composed with a three out of four VC system supported by the matrices derived as:

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

$$S_0^{c_1c_2c_3c_4} = \begin{bmatrix} 0 & c_1 & 1 & 1 & 1 & c_1 \\ 0 & c_2 & 1 & 1 & c_2 & 1 \\ 0 & 1 & c_3 & c_3 & 1 & 1 \\ 0 & 1 & c_4 & 1 & c_4 & 1 \end{bmatrix}.$$

Two VIPs out of six subpixels cause the visual contrast of the encrypted share as $\frac{2}{6}$ with visual contrast of $\frac{1}{6}$ for a decrypted share. The secret image of size 85×128 pixels shows the letters the 'U','D','E' and 'L' in red, blue, green and yellow, respectively. Original images 'Lena', 'Baboon', 'Pepper' and 'Flower' of size 256×256 in natural colors are provided for the share generation. We use the peak noise-to-signal ratio (PSNR) distortion measure for the visual quality comparison between the original images and the encrypted images using three encryption methods. We assume that the original shares belong to a Gaussian distribution with $N(0,1)$. For visual comparison we present halftoned images of an original, unencrypted, image in Fig. 3 (a) of PSNR 11.78 dB. Fig. 3 (b) shows a result of grayscale EVCS in [5], [6], applied to color shares. It shows relatively low contrast with barely recognizable shape of the image of PSNR 10.43 dB. The methods in [5], [6] may work well in a black and white grayscale VC scheme, however, they do not produce satisfactory results in

Fig. 3. Comparison of the proposed method and simulation results.

color VC due to the random permutation at each color channel. Fig. 3 (c) is provided to verify the effectiveness of error diffusion. This figure is generated by the proposed method in this paper without the error diffusion stage. Color contrast is improved compared with that of (b) owing to VIP synchronization so we recognize an outline of the share with PSNR 10.81 dB; however, details are still not clear and overall color particles are rough. Figures from (d) to (g) are result of the proposed scheme with $m = 6$, $p = 3$ and $q = 2$, of PSNR 10.95 dB and 10.88 dB, 11.45 dB, 11.23 dB, respectively. In this example, two out of six subpixels are VIPs, however these are correlated across the three color layers so shares present improved visual quality. VIPs are inserted into the shares naturally via error diffusion. Fig. 3 (h) show a decrypted secret message by stacking four shares and letters are in desired color and we can clearly recognize them.

4. CONCLUSION

This paper develops an encryption method to construct color EVCS with VIP synchronization and error diffusion for visual quality improvement. VIP synchronization retains the original VIP values the same before and after encryption and error diffusion produces shares with high visual quality. Either VIP synchronization or error diffusion can be broadly used in many visual cryptography scheme for color images.

5. REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," *EUROCRYPT '94 Springer-Verlag LNCS*, vol. 950, pp. 1–12, 1995.

[2] C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for grey level images," *Information Processing Letters*, vol. 75, pp. 255–259, 2000.

[3] G. Ateniese, C. Blundo, A. Santis, and D. Stinson, "Extended capabilities for visual cryptography," *ACM Theoretical Computer Science*, vol. 250, pp. 143–161, 2001.

[4] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," *IEEE Transaction on Image Processing*, vol. 15, no. 8, pp. 2441–2453, 2006.

[5] Stefan Droste, "New results on visual cryptography," *CRYPTO '96 Springer-Verlag LNCS*, vol. 1109, pp. 401–415, 1996.

[6] R. Lukac and K. N. Plataniotis, "Colour image secret sharing," *IEE Electronic Letters*, , no. 9, pp. 529–530, 2004.