A $\{k, n\}$ -Secret Sharing Scheme for Color Images

Rastislav Lukac, Konstantinos N. Plataniotis, and
Anastasios N. Venetsanopoulos

The Edward S. Rogers Sr. Dept. of Electrical and Computer Engineering,
University of Toronto, 10 King's College Road, Toronto, M5S 3G4, Canada
{lukacr,kostas,anv}@dsp.utoronto.ca

Abstract. This paper introduces a new $\{k, n\}$ -secret sharing scheme for color images. The proposed method encrypts the color image into n color shares. The secret information is recovered only if the k (or more) allowed shares are available for decryption. The proposed method utilizes the conventional $\{k, n\}$ -secret sharing strategy by operating at the bit-levels of the decomposed color image. Modifying the spatial arrangements of the binary components, the method produces color shares with varied both the spectral characteristics among the RGB components and the spatial correlation between the neighboring color vectors. Since encryption is done in the decomposed binary domain, there is no obvious relationship in the RGB color domain between any two color shares or between the original color image and any of the n shares. This increases protection of the secret information. Inverse cryptographic processing of the shares must be realized in the decomposed binary domain and the procedure reveals the original color image with perfect reconstruction.

1 Introduction

Visual cryptography [2],[3],[4],[8],[11] is a popular cryptographic tool used for protection of scanned documents and natural digital images which are distributed via public networks. These techniques are based on the principle of sharing secret information among a group of participants. The shared secret can be recovered only when a coalition of willing participants are polling their encrypted images, the so-called shares, together. Secret sharing schemes are usually termed visual since the secret (original) information can be directly revealed from stacked shares (e.g realized as transparencies) through simple visual inspection, without any computer-guided processing [9],[11].

A $\{k, n\}$ -threshold visual cryptography scheme [5],[6],[11] often called $\{k, n\}$ -visual secret sharing (VSS), is used to encrypt an input image by splitting the original content into n , seemingly random, shares. To recover the secret information, k (or more) allowed shares must be stacked together.

Fig. 1. Visual cryptography: (a) original binary image, (b,c) share images, (d) decrypted, output image

2 $\{k, n\}$ -Secret Sharing Scheme

Due to its algorithmic nature, conventional visual cryptography schemes operate on a binary input (Fig. 1) [10]. Assuming a $K_1 \times K_2$ binary image (black and white image with 0 values denoting the black and 1 values denoting the white), each binary pixel $r_{(i,j)}$ determined by spatial coordinates $i = 1, 2, \dots, K_1$ and $j = 1, 2, \dots, K_2$ is replaced via an encryption function $f_e(\cdot)$ with a $m_1 \times m_2$ block of black and white pixels in each of the n shares. Repeating the process for each input pixel, a $K_1 \times K_2$ input binary image is encrypted into n binary shares each one with a spatial resolution of $m_1 K_1 \times m_2 K_2$ pixels. Since the spatial arrangement of the pixels varies from block to block, the original information cannot be revealed without accessing a predefined number of shares.

Let us assume a basic $\{2, 2\}$ -threshold structure which is the basic case designed within the $\{k, n\}$ -VSS framework [1],[7]. Assuming for simplicity a basic structure with 2×2 blocks $\mathbf{s}_1 = [s'_{(2i-1, 2j-1)}, s'_{(2i-1, 2j)}, s'_{(2i, 2j-1)}, s'_{(2i, 2j)}] \in S_1$ and $\mathbf{s}_2 = [s''_{(2i-1, 2j-1)}, s''_{(2i-1, 2j)}, s''_{(2i, 2j-1)}, s''_{(2i, 2j)}] \in S_2$, the encryption process is defined as follows:

$$f_e(r_{(i,j)}) = \begin{cases} [\mathbf{s}_1, \mathbf{s}_2]^T \in C_0 & \text{for } r_{(i,j)} = 0 \\ [\mathbf{s}_1, \mathbf{s}_2]^T \in C_1 & \text{for } r_{(i,j)} = 1 \end{cases} \quad (1)$$

where C_0 and C_1 are the sets obtained by permuting the columns of the $n \times m_1 m_2$ basis matrices A_0 and A_1 , respectively [10]. Since $m_1 m_2$ represents the factor by which each share is larger than the original image, it is desirable to make $m_1 m_2$ as small as possible. In the case of the $\{2, 2\}$ -VSS the optimal choice m_1 and m_2 leads to $m_1 = 2$ and $m_2 = 2$ resulting in 2×2 blocks $\mathbf{s}_1$ and $\mathbf{s}_2$.

Fig. 2. Halftoning-based secret sharing of color images: (a) original color image, (b) halftone image obtained using Floyd-Steinberg filter [12], (c,d) share images, (e) decrypted, output image

Assuming the $\{2, 2\}$ -VSS the sets

$$C_0 = \left\{ \begin{bmatrix} 0, 1, 0, 1 \\ 1, 0, 1, 0 \end{bmatrix}, \begin{bmatrix} 1, 0, 1, 0 \\ 0, 1, 0, 1 \end{bmatrix}, \begin{bmatrix} 0, 0, 1, 1 \\ 1, 1, 0, 0 \end{bmatrix}, \begin{bmatrix} 1, 1, 0, 0 \\ 0, 0, 1, 1 \end{bmatrix}, \begin{bmatrix} 1, 0, 0, 1 \\ 0, 1, 1, 0 \end{bmatrix}, \begin{bmatrix} 0, 1, 1, 0 \\ 1, 0, 0, 1 \end{bmatrix} \right\} \quad (2)$$

$$C_1 = \left\{ \begin{bmatrix} 0, 1, 0, 1 \\ 0, 1, 0, 1 \end{bmatrix}, \begin{bmatrix} 1, 0, 1, 0 \\ 1, 0, 1, 0 \end{bmatrix}, \begin{bmatrix} 0, 0, 1, 1 \\ 0, 0, 1, 1 \end{bmatrix}, \begin{bmatrix} 1, 1, 0, 0 \\ 1, 1, 0, 0 \end{bmatrix}, \begin{bmatrix} 1, 0, 0, 1 \\ 1, 0, 0, 1 \end{bmatrix}, \begin{bmatrix} 0, 1, 1, 0 \\ 0, 1, 1, 0 \end{bmatrix} \right\} \quad (3)$$

include all matrices obtained by permuting the columns of the 2×4 basis matrices A_0 and A_1 , respectively [10],[11]. The basic matrices considered here are defined as follows:

$$A_0 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \quad A_1 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad (4)$$

If a secret pixel is white, i.e. $r_{(i,j)} = 1$, then each pixel in $\mathbf{s}_1$ is equivalent to each pixel in $\mathbf{s}_2$, and thus, $[\mathbf{s}_1, \mathbf{s}_2]^T$ can be any member of set C_1 . If a secret pixel is black, i.e. $r_{(i,j)} = 0$, then each pixel in $\mathbf{s}_1$ should complement each pixel in $\mathbf{s}_2$ and thus, $[\mathbf{s}_1, \mathbf{s}_2]^T$ should be selected from set C_0 . The choice of $[\mathbf{s}_1, \mathbf{s}_2]^T$ is guided by a random number generator, which determines the random character of the shares.

The decrypted block is produced through a decryption function $f_d(\cdot)$. In the case of the $\{2, 2\}$ -scheme based on the basis matrices of (4), $f_d(\cdot)$ can be defined as follows:

$$y_{2 \times 2} = f_d(\mathbf{s}_1, \mathbf{s}_2) = \begin{cases} \mathbf{s}_1 & \text{for } \mathbf{s}_1 = \mathbf{s}_2 \\ [0, 0, 0, 0] & \text{for } \mathbf{s}_1 \neq \mathbf{s}_2 \end{cases} \quad (5)$$

Fig. 3. Halftoning-based secret sharing of color images: (a) original color image, (b) halftone image obtained using Floyd-Steinberg filter [12], (c,d) share images, (e) decrypted, output image

where $\mathbf{s}_1 = [s'_{(u,v)}, s'_{(u,v+1)}, s'_{(u+1,v)}, s'_{(u+1,v+1)}] \in S_1$ and $\mathbf{s}_2 = [s''_{(u,v)}, s''_{(u,v+1)}, s''_{(u+1,v)}, s''_{(u+1,v+1)}] \in S_2$, for $u = 1, 3, \dots, 2K_1 - 1$ and $v = 1, 3, \dots, 2K_2 - 1$, are 2×2 share blocks which are used to recover the output block $y_{2 \times 2} = y_{(u,v)}, y_{(u,v+1)}, y_{(u+1,v)}, y_{(u+1,v+1)}$ as $s'_{(u,v)}$ or black pixels described as $[0, 0, 0, 0]$.

The application of a conventional $\{k, n\}$ -VSS scheme to a $K_1 \times K_2$ natural image requires halftoning [7],[10]. The image is first transformed into a $K_1 \times K_2$ halftone image by using the density of the net dots to simulate the intensity levels [12]. Applying the procedure for each color channel of the original image (Fig. 2a) independently, each color channel of the halftone image (Fig. 2b) is a binary image and thus appropriate for the VSS. Assuming $\{2, 2\}$ -VSS, the two color shares obtained by the procedure are depicted in Fig. 2c,d. Figure 2e shows the $2K_1 \times 2K_2$ decrypted image (result) obtained by stacking the two shares together.

Visual inspection of both the original image (Fig. 1a and Fig. 2a) and the recovered image (Fig. 1d and Fig. 2e) indicates that: i) the decrypted image is darker, and ii) the input image is of quarter size compared to the decrypted output. Moreover, the decrypted color image depicted in Fig. 2e contains a number of color artifacts due to nature of the algorithm. To end this, the conventional $\{k, n\}$ -threshold visual cryptography i) cannot provide perfect reconstruction, either in terms of pixel intensity or spatial resolution, and ii) is not appropriate for real-time applications.

Figure 3 shows the images obtained using the conventional $\{2, 2\}$ -secret sharing scheme applied to the image with the different color scenario compared to Fig. 2. It can be again observed that the decrypted image depicted in Fig. 3e contains shifted colors which often prohibit correct perception of fine image details.

It has to be mentioned that the halftoning-based $\{k, n\}$ -visual secret sharing schemes are the most popular choice for natural image secret sharing. Another secret sharing approach for color images is based on mean color-mixing [8]. However, this method is not appropriate for practical applications due to significant reduction of color gamut and the extreme increase in the spatial resolution of the shares. Other works, e.g. [9],[13] deals with analytical construction of the secret sharing schemes for color images.

3 $\{k, n\}$ -Color Secret Sharing

Let $\mathbf{x} : Z^2 \rightarrow Z^3$ be a $K_1 \times K_2$ Red-Green-Blue (RGB) color image representing a two-dimensional matrix of the three-component color vectors (pixels) $\mathbf{x}_{(i,j)} = [x_{(i,j)1}, x_{(i,j)2}, x_{(i,j)3}]$ located at the spatial position (i, j) , for $i = 1, 2, \dots, K_1$ and $j = 1, 2, \dots, K_2$. Assuming that c describes the color channel (i.e. $c = 1$ for Red, $c = 2$ for Green, and $c = 3$ for Blue) and the color component $x_{(i,j)c}$ is coded with B bits allowing $x_{(i,j)c}$ to take an integer value between 0 and $2^B - 1$, the color vector $\mathbf{x}_{(p,q)}$ can be equivalently expressed in a binary form as follows:

$$\mathbf{x}_{(i,j)} = \sum_{b=1}^B \mathbf{x}_{(i,j)}^b 2^{B-b} \quad (6)$$

where $\mathbf{x}_{(i,j)}^b = [x_{(i,j)1}^b, x_{(i,j)2}^b, x_{(i,j)3}^b] \in \{0, 1\}^3$ denotes the binary vector at the b -bit level, with $b = 1$ denoting the most significant bits (MSB).

3.1 Encryption

If the c -th component of the binary vector $\mathbf{x}_{(i,j)}^b$ is white ($x_{(i,j)c}^b = 1$), encryption is performed through $[\mathbf{s}_1, \mathbf{s}_2]^T \in C_1$ replacing $x_{(i,j)c}^b$ by binary blocks $\mathbf{s}_1$ and $\mathbf{s}_2$ in each of the two shares. Otherwise, the reference binary component is black ($x_{(p,q)c}^b = 0$), and encryption is defined via $[\mathbf{s}_1, \mathbf{s}_2]^T \in C_0$. This forms an encryption function defined as follows:

$$f_e(x_{(i,j)c}^b) = \begin{cases} [\mathbf{s}_1, \mathbf{s}_2]^T \in C_0 & \text{for } x_{(i,j)c}^b = 0 \\ [\mathbf{s}_1, \mathbf{s}_2]^T \in C_1 & \text{for } x_{(i,j)c}^b = 1 \end{cases} \quad (7)$$

Fig. 4. Proposed $\{2, 2\}$ -secret sharing scheme for color images: (a) original color image, (b,c) share images, (d) decrypted, output image

By replacing the binary components $x_{(i,j)c}^b$ with binary blocks $\mathbf{s}_1$ and $\mathbf{s}_2$ for one particular b , the process generates two $2K_1 \times 2K_2$ vector-valued binary shares S_1^b and S_2^b , respectively. A random number generator guides the choice of $[\mathbf{s}_1, \mathbf{s}_2]^T$ and determines the random character of S_1^b and S_2^b . Thus, the process modifies both the spatial correlation between spatially neighboring binary vectors $\mathbf{s}_{(u,v)}^b = [s_{(u,v)1}^b, s_{(u,v)2}^b, s_{(u,v)3}^b] \in S_1^b$ or $\mathbf{s}_{(u,v)}^b = [s_{(u,v)1}^b, s_{(u,v)2}^b, s_{(u,v)3}^b] \in S_1^b$, for $u = 1, 2, \dots, 2K_1$ and $v = 1, 2, \dots, 2K_2$, and the spectral correlation among components $s_{(u,v)c}^b$ or $s_{(u,v)c}^b$, for $c = 1, 2, 3$, of the individual binary vectors $\mathbf{s}_{(u,v)}^b$ or $\mathbf{s}_{(u,v)}^b$, respectively. Bit-level stacking of the encrypted bit-levels produces the color vectors $\mathbf{s}_{(u,v)}' \in \mathbf{S}_1$ and $\mathbf{s}_{(u,v)}'' \in \mathbf{S}_2$ as

$$\mathbf{s}_{(u,v)}' = \sum_{b=1}^B \mathbf{s}_{(u,v)}^b 2^{B-b} \quad \text{and} \quad \mathbf{s}_{(u,v)}'' = \sum_{b=1}^B \mathbf{s}_{(u,v)}^b 2^{B-b} \quad (8)$$

Due to random processing taking place at the bit-levels, $\mathbf{S}_1$ and $\mathbf{S}_2$ contain only random, color noise like information (Fig. 4b,c). Since encryption is realized in the decomposed binary vector space, no detectable relationship between the original color vectors $\mathbf{x}_{(p,q)}$ and the color noise of $\mathbf{S}_1$ or $\mathbf{S}_2$ can be found in the RGB color domain. This considerably increases security and prevents unauthorized decryption through brute-force enumeration.

3.2 Decryption

The decryption procedure is designed to satisfy the perfect reconstruction property. The original color data must be recovered from the color shares $\mathbf{S}_1$ and $\mathbf{S}_2$ using inverse algorithmic steps. Therefore, the decryption procedure is applied to the decomposed binary vector arrays of the color shares. Assuming that (i, j) , for $i = 1, 2, \dots, K_1$ and $j = 1, 2, \dots, K_2$, denotes the spatial position in the original image and c denotes the color channel, the corresponding 2×2 binary share blocks are $\mathbf{s}_c^b = \{s_{(2i-1, 2j-1)c}^b, s_{(2i-1, 2j)c}^b, s_{(2i, 2j-1)c}^b, s_{(2i, 2j)c}^b\}$ and $\mathbf{s}_c^b = \{s_{(2i-1, 2j-1)c}^b, s_{(2i-1, 2j)c}^b, s_{(2i, 2j-1)c}^b, s_{(2i, 2j)c}^b\}$. Based on the arrangements of the basis matrices A_0 and A_1 in (4) used in the proposed $\{2, 2\}$ -secret sharing

Fig. 5. Proposed $\{2,2\}$ -secret sharing scheme for color images: (a) original color image, (b,c) share images, (d) decrypted, output image

scheme, if both blocks are consistent, i.e. $\mathbf{s}_c^b = \mathbf{s}_c'^b$, the decrypted original bit $x_{(i,j)c}^b$ is assign white, i.e. $x_{(i,j)c}^b = 1$. Otherwise, the blocks are inconsistent, i.e. $\mathbf{s}_c^b \neq \mathbf{s}_c'^b$ and the original bit is recovered as black, i.e. $x_{(i,j)c}^b = 0$. This logical comparison forms the following decryption function

$$x_{(i,j)c}^b = f_d(\mathbf{s}_c^b, \mathbf{s}_c'^b) = \begin{cases} 1 & \text{for } \mathbf{s}_c^b = \mathbf{s}_c'^b \\ 0 & \text{for } \mathbf{s}_c^b \neq \mathbf{s}_c'^b \end{cases} \quad (9)$$

which is used to restore the binary vectors $\mathbf{x}_{(i,j)}^b$. The procedure completes with the bit-level stacking (6) resulting in the original color vector $\mathbf{x}_{(i,j)}$.

Figure 4d shows the decrypted color output. Since the proposed method satisfies the perfect reconstruction property, the output image is identical to the original depicted in Fig 4a. Note that perfect reconstruction is demonstrated also in Fig 5, which depicts two full color shares (Fig 5b,c) and the decrypted output (Fig 5d) obtained by the proposed $\{2,2\}$ -secret sharing scheme applied to the test image “Atlas” (Fig 5a).

It has to be mentioned that (9), which is defined for a $\{2,2\}$ -scheme, can be more generally described as follows:

$$o_{(i,j)}^b = f_d(\mathbf{s}_1^b, \mathbf{s}_2^b) = \begin{cases} 1 & \text{for } [\mathbf{s}_c^b, \mathbf{s}_c'^b]^T \in C_1 \\ 0 & \text{for } [\mathbf{s}_c^b, \mathbf{s}_c'^b]^T \in C_0 \end{cases} \quad (10)$$

This concept can be further generalized for the share blocks $\{\mathbf{s}_c^b, \mathbf{s}_c'^b, \mathbf{s}_c''^b, \dots\}$ defined in the specific $\{k, n\}$ -threshold schemes.

4 Conclusion

A $\{k, n\}$ secret sharing scheme with perfect reconstruction of the color inputs was introduced. The method cryptographically processes the color images replacing

the bit components with a block of bits for each of the n shares. By separate encrypting each bit plane of the decomposed color image, the method produces color shares with varied spectral and spatial characteristics. Since encryption is realized in the decomposed binary domain, the procedure increases protection against attacks performed in the RGB color domain. This makes the method attractive for secure transmission over the untrusted public channel. Moreover, the perfect reconstruction property allows to reveal the original color image without visual impairments or color shifts.

References

1. Adhikari, A., Sikdar, S.: A new $(2, n)$ -visual threshold scheme for color images. Proc. INDOCRYPT 2003, LNCS **2904** (2003) 148–161
2. Ateniese, G., Blundo, C., de Santis, A., Stinson, D.G.: Visual cryptography for general access structures. Information and Computation **129** (1996) 86–106
3. Ateniese, G., Blundo, C., de Santis, A., Stinson, D.G.: Extended capabilities for visual cryptography. Theoretical Computer Science **250** (2001) 143–161
4. Droste, S.: New results on visual cryptography. Proc. Advances in Cryptology - CRYPTO'96, LNCS **1109** (1996) 401–415
5. Eisen, P.A., Stinson, D.R.: Threshold visual cryptography schemes with specified levels of reconstructed pixels. Design, Codes and Cryptography **25** (2002) 15–61
6. Hofmeister, T., Krause, M., Simon, H.U.: Contrast optimal k out of n secret sharing schemes in visual cryptography. Theoretical Computer Science **240** (2000) 471–485
7. Hou, J.C.: Visual cryptography for color images. Pattern Recognition **36** (2003) 1619–1629
8. Ishihara, T., Koga, H.: A visual secret sharing scheme for color images based on meanvalue-color mixing. IEICE Trans. Fundamentals **E86-A** (2003) 194–197
9. Koga, H., Iwamoto, M., Yakamoto, H.: An analytic construction of the visual secret sharing scheme for color images. IEICE Trans. Fundamentals **E84-A** (2001) 262–272
10. Lin, C.C., Tsai, W.H.: Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters **24** (2003) 349–358
11. Naor, M., Shamir, A.: Visual Cryptography. Proc. EUROCRYPT'94, LNCS **950** (1994) 1–12
12. Ulichney, R.A.: Dithering with blue noise. Proceedings of the IEEE **76** (1988) 56–79
13. Yang, C.N.: A note on color visual encryption. Journal of Information Science and Engineering **18** (2002) 367–372