A SECRET SHARING SCHEME FOR IMAGE ENCRYPTION

Rastislav Lukac and Konstantinos N. Plataniotis

The Edward S. Rogers Sr. Department of Electrical and Computer Engineering,
University of Toronto, 10 King's College Road, Toronto, M5S 3G4 Ontario, Canada
lukacr@ieee.org, kostas@dsp.utoronto.ca

Abstract: *This paper presents a secret sharing scheme capable of protecting image data coded with B bits per pixel. The proposed encryption scheme generates B-bit shares by combining bit-level decomposition/stacking with a $\{k,n\}$-threshold sharing strategy. Perfect reconstruction is achieved by performing decryption through simple logical operations in the decomposed bit-levels without the need for any post-processing operations. The method allows for cost-effective cryptographic processing of B-bit images over public networks.*

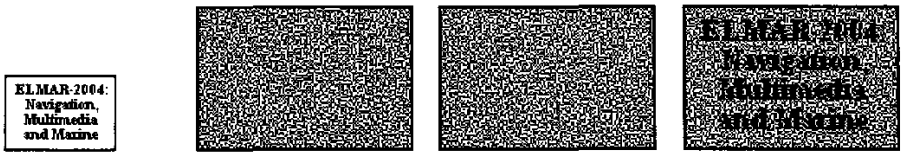
Keywords: *Image secret sharing, $\{k,n\}$-threshold scheme, bit-level processing.*

1. INTRODUCTION

Recent developments of digital communication networks have seen the need for private communication over the untrusted channels. The confidentiality of transmitted personal digital photographs and digital signature images is usually obtained by encryption. Image protection is achieved either by employing data hiding techniques or through secret sharing. Image data hiding techniques embed information by modifying the original image in a imperceptible way [2],[9]. On the other hand, secret sharing schemes 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 shares together [3].

Visual cryptography [8] is a secret sharing procedure for image data, which uses the properties of the human visual system to force the recognition of a secret message from overlapping encrypted images (shares) without additional computations and any knowledge of cryptography. In existing schemes a well-known $\{k,n\}$-threshold procedure is used to encrypt the secret image into n noise-like shares, which are then distributed amongst n recipients. If any k recipients stack their shares printed as transparencies together on an overhead projector the secret image is visually revealed. On the other hand, any $(k-1)$ or fewer shares cannot be used to decrypt the transmitted information. It has to be mentioned that although the visual cryptographic schemes can be realized through logical operations and thus used in the computer-centric environments, such a solution reduces resolution and contrast of the decrypted image and produces unacceptable visual artifacts, [7].

Unlike past image sharing schemes, the recently developed secret sharing scheme of [7] operates directly on the bit planes of the digital input. In a digital image, each pixel value can be represented as B-bit code word. If the input image is decomposed into B bit-levels (planes), each bit-level can be viewed as a binary image. By stacking individually encrypted bit planes, the scheme produces the B-bit shares useful for secure distribution over the untrusted public networks. The scheme allows recovering of the original B-bit image content with perfect reconstruction and the decrypted output is readily available in digital form.



(a) (b) (c) (d)

Fig. 1 A {2,2} visual cryptography scheme operating on a binary image input: (a) original image, (b, c) share images, (d) decrypted output.

2. VISUAL CRYPTOGRAPHY

In visual cryptography [5],[6],[7],[8], a $\{k,n\}$-threshold visual cryptography scheme, often called $\{k,n\}$ visual secret sharing scheme or simply $\{k,n\}$-VSS, is used to encrypt an input binary image by splitting the original content into n, seemingly random, shares $S_1,S_2,...,S_n$. The procedure is termed visual since the secret information is recovered through visual inspection of the stacked k (or more) allowed shares without the need for complicated cryptographic mechanisms and computations (Fig. 1).

Due to the nature of conventional visual cryptography the input is a binary or binarized image [3],[5],[6]. Thus, that the application of a conventional visual secret sharing schemes to a natural image (Fig. 2a) with B-bit/pixel representation requires halftoning. The halftone procedure transforms a natural image to a binary image using the density of the net dots to simulate the gray levels (Fig. 2b), [10],[11]. To encrypt a $K_1 \times K_2$ binary image with spatial coordinates $i=1,2,...,K_1$ and $j=1,2,...,K_2$, each binary pixel $r_{(i,j)}$ is handled separately via an encryption function $f_e(.)$ to produce a $m_1 \times m_2$ block of black and white pixels in each of the n shares. Thus, a $K_1 \times K_2$ input binary image is encrypted into n binary shares $S_1,S_2,...,S_n$ each one with a spatial resolution of $m_1K_1 \times m_2K_2$ pixels. Since the spatial arrangement of the pixels varies from block to block, as it is explained below, it is impossible to recover the useful information without accessing a predefined number of shares.

Assuming for simplicity a basic {2,2} scheme with 2×2 blocks $\mathbf{s}_1=[s_{1:(2i-1,2j-1)},s_{1:(2i-1,2j)},s_{1:(2i,2j-1)},s_{1:(2i,2j)}]$ in the share S_1 and $\mathbf{s}_2=[s_{2:(2i-1,2j-1)},s_{2:(2i-1,2j)},s_{2:(2i,2j-1)},s_{2:(2i,2j)}]$ in the share S_2, the encryption process is given by

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

The sets C_0 and C_1 include all matrices obtained by permuting the columns of the $n\times m_1m_2$ basis matrices A_0 and A_1, respectively [8]:

$$A_0=\begin{bmatrix}0&1&0&1\\1&0&1&0\end{bmatrix} \quad A_1=\begin{bmatrix}0&1&0&1\\0&1&0&1\end{bmatrix} \tag{2}$$

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

The decrypted block is produced through a decryption function $f_d(.)$ which is defined as follows:

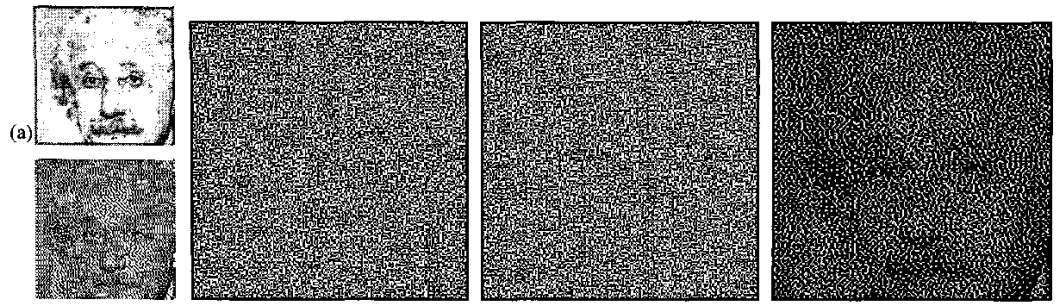


Fig. 2 A $\{2,2\}$ halftoning based visual cryptography scheme applied to a natural image: (a) original image, (b) halftone image obtained using Floyd-Stenberg filter [10], (c, d) share images, (e) decrypted output.

$$y_{(u,v)} = f_d(s_{1:(u,v)}, s_{2:(u,v)}) = \begin{cases} 1 & \text{if } s_{1:(u,v)} = s_{2:(u,v)} = 1 \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

where (u,v), for $u = 1,2,...,m_1K_1$ and $v = 1,2,...,m_2K_2$, denotes the spatial location in a $m_1K_1 \times m_2K_2$ share. The term $y_{(u,v)}$ indicates a pixel in the $m_1K_1 \times m_2K_2$ decrypted image. Note that due to frosted/transparent representation concept of shares the output pixel $y_{(u,v)}$ can be recovered as white only if the share pixels corresponding to the identical spatial location (u,v) are white, i.e. $s_{1:(u,v)} = s_{2:(u,v)} = 1$ for a $\{2,2\}$-scheme. As it can be seen in Fig. 1d and Fig. 2e, the procedure reduces contrast and results in visual artifacts in the recovered image.

3. PROPOSED METHOD

Instead of a halftone image, our method - the so-called B-bit secret sharing scheme [7], directly operates on a digital $K_1 \times K_2$ input image O with a B-bit per pixel representation. In such a representation, each integer pixel value $o_{(i,j)} \in O$ can be expressed equivalently in a binary form using [1]:

$$o_{(i,j)} = o^1_{(i,j)} 2^{B-1} + o^2_{(i,j)} 2^{B-2} + ... + o^{B-1}_{(i,j)} 2 + o^B_{(i,j)} \tag{4}$$

where (i,j) denotes the spatial location and $o^b_{(i,j)}$ indicates the bit value at the bit level $b = 1,2,...,B$, with $o^1_{(i,j)}$ corresponding to the most significant bit (MSB). The bit-level decomposition is a natural way to decompose the input image to a series of B binary images depicted in Fig. 3, and from this point of view constitutes the ideal preprocessing step for share-based encryption [7].

After achieving B binary planes, the conventional encryption function (1) is utilized to generate the binary shares S^b_1 and S^b_2 using the reference pixel $r_{(i,j)} = o^b_{(i,j)}$. Assuming that $s^b_{1:(u,v)} \in S^b_1$ and $s^b_{2:(u,v)} \in S^b_2$ denote the pixels in the $m_1K_1 \times m_2K_2$ binary shares S^b_1 and S^b_2, respectively, the B-bit share (integer) pixels $s_{1:(u,v)} \in S_1$ and $s_{2:(u,v)} \in S_2$, for $u = 1,2,...,m_1K_1$ and $v = 1,2,...,m_2K_2$, are constituted by bit-level stacking as follows:

$$s_{1:(u,v)} = s^1_{1:(u,v)} 2^{B-1} + s^2_{1:(u,v)} 2^{B-2} + ... + s^{B-1}_{1:(u,v)} 2 + s^B_{1:(u,v)} \tag{5}$$

$$s_{2:(u,v)} = s^1_{2:(u,v)} 2^{B-1} + s^2_{2:(u,v)} 2^{B-2} + ... + s^{B-1}_{2:(u,v)} 2 + s^B_{2:(u,v)} \tag{6}$$

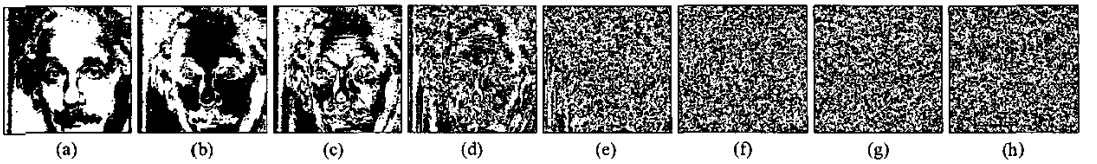


Fig. 3 Binary images corresponding to the bit-levels of the gray-scale image Einstein: (a) $b=1$, (b) $b=2$, (c) $b=3$, (d) $b=4$, (e) $b=5$, (f) $b=6$, (g) $b=7$, (h) $b=8$.

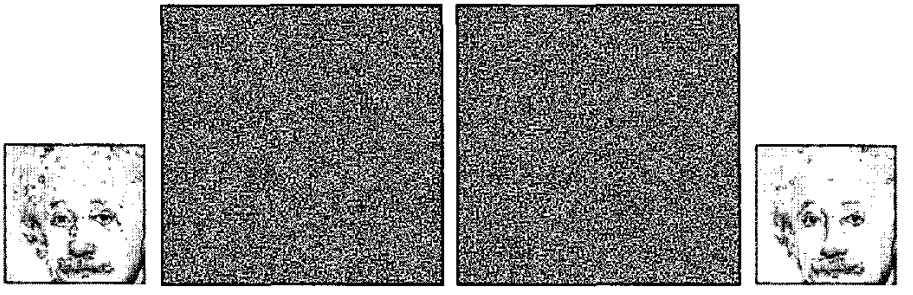


Fig. 4 The proposed $\{2,2\}$-secret sharing scheme applied to a natural (gray-scale) image: (a) original B-bit image, (b, c) B-bit share images, (e) decrypted B-bit image.

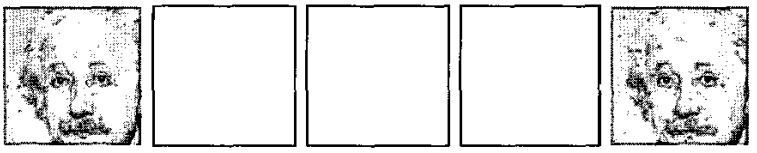
Depending on the particular bit-levels on which $f_e(.)$ is applied and the random choice of the block representing $o^b_{(i,j)}$, the original pixel $o_{(i,j)}$ and the integer-valued share pixels corresponding to the share blocks $\mathbf{s}_1,\mathbf{s}_2,...,\mathbf{s}_n$ can differ significantly.

For faithful decryption of the original B-bit image from its B-bit shares, we introduce here the decryption function $f_d(.)$ defined as follows:

$$o^b_{(i,j)} = f_d(\mathbf{s}^b_1,\mathbf{s}^b_2,...,\mathbf{s}^b_x) = \begin{cases} 1 & \text{if } s^b_{1:(p,r)} = s^b_{2:(p,r)} = ... = s^b_{x:(p,r)} = 1, \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

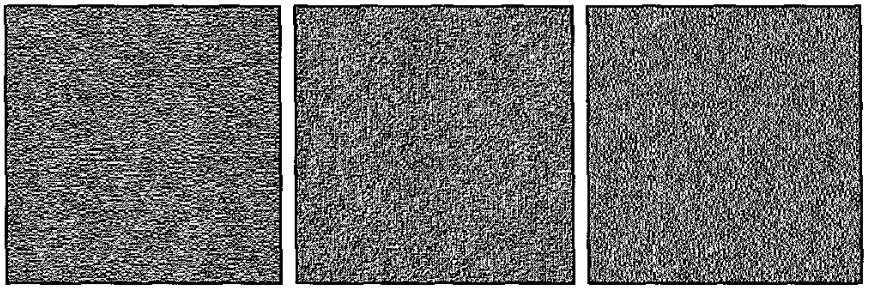
where (i,j) denotes location in a $K_1 \times K_2$ reference image and $\mathbf{s}^b_1 = [s^b_{1:(2i-1,2j-1)}, s^b_{1:(2i-1,2j)}, s^b_{1:(2i,2j-1)}, s^b_{1:(2i,2j)}] \in S^b_1$ denotes a 2×2 block at the b-th bit level S^b_1 of the share S_1. The vector $\mathbf{s}^b_2 = [s^b_{2:(2i-1,2j-1)}, s^b_{2:(2i-1,2j)}, s^b_{2:(2i,2j-1)}, s^b_{2:(2i,2j)}] \in S^b_2$ describes an identical block located at the same spatial position at the b-th bit level S^b_2 of the share S_2 and (p,r) denotes the location inside the share block.

Since the encryption operation (1) increases the spatial resolution of the shares, the decryption function (7) should decrease the spatial resolution of the output image and at the same time, it should to recover the original bit $o^b_{(i,j)}$. Therefore, (7) recovers $o^b_{(i,j)}$ as white, i.e. $o^b_{(i,j)} = 1$, if and only if there exists at least one subset of the share pixels $s^b_{1:(p,r)}, s^b_{2:(p,r)}, ..., s^b_{x:(p,r)}$ equal to 1, for $s^b_{1:(p,r)} \in \mathbf{s}^b_1, s^b_{2:(p,r)} \in \mathbf{s}^b_2, ..., s^b_{x:(p,r)} \in \mathbf{s}^b_x$, coming from x different shares but corresponding to the same spatial location (p,r) located within the share blocks $\mathbf{s}^b_1,\mathbf{s}^b_2,...,\mathbf{s}^b_x$. Note that this idea can be extended for an arbitrary secret sharing scheme defined by the parameters $\{k,n\}$ and the block dimensions m_1 and m_2. The parameter x denotes the number of the shares available for decryption. It has to be mentioned at this point that for less than k shares the procedure does not recover the original image since all bits will be recovered as $o^b_{(i,j)} = 1$ (binary white) resulting in the maximum intensity (white pixel) of $o_{(i,j)}$.



(a) (b) (c) (d) (e)

Fig. 5 The proposed $\{3,3\}$ -secret sharing scheme applied to a natural image: (a) original gray-scale image, (b, c, d) images produced using two shares {(b) S_1 and S_2, (c) S_1 and S_3, (d) S_2 and S_3}, (e) image decrypted using required S_1, S_2, and S_3 shares.



(a) (b) (c)

Fig. 6 Shares S_1 (a), S_2 (b) and S_3 (c) generated by the proposed B-bit $\{3,3\}$ -secret sharing scheme applied to a natural (gray-scale) image shown in Fig. 5a. The corresponding results obtained using the proposed decryption procedure are shown in Fig. 5b-e.

As it can be seen in Fig. 4 which shows the images obtained using a $\{2,2\}$ -scheme, the B-bit secret sharing scheme satisfies the perfect reconstruction property and recovers the original image unchanged.

Fig. 5 shows the original and decrypted outputs obtained using a $\{3,3\}$-scheme defined by the following basis matrices:

$$A_0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad A_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \tag{8}$$

It is not difficult to see from these examples that the proposed scheme perfectly works also for higher order configurations. If the users are not in possession of the required amounts of shares, no information is decrypted and the procedure results in a white image.

Figs. 5b-d show the output obtained by stacking any two of the required three shares S_1, S_2 and S_3 depicted in Fig. 6. Since the shares are generated using the column permutations of the basis matrices defined in (8) which describes unique settings of a $\{3,3\}$-secret sharing scheme, no information can be revealed using only two shares. However, the use of three shares in decryption reveals the useful image information. Visual inspection of the images shown in Fig. 5e and Fig. 5a suggests that if the required number of the shares is available for decryption, the proposed decryption procedure always produces the original image.

4. CONCLUSION

In this paper, we focused on a B-bit secret sharing framework that affords perfect reconstruction of the encrypted image input. The method utilizes bit-level decomposition and stacking operations to both encrypt and decrypt B-bit image. The proposed method can be applied for encryption of the images with binary, gray-scale or color representation, making the method attractive for a wide range of applications which require image encryption with the simultaneous capability of secret sharing.

REFERENCES

[1] C.S. Burrus, Digital filter structures described by distributed arithmetic, *IEEE Transactions on Circuits and Systems*, 24(12), 1977, 674-680.
[2] I. Cox, M. Miller, and J. Bloom, *Digital Watermarking*. Morgan Kaufmann Publishers, San Francisco, 2001.
[3] C.C Chang and J.C. Chuang, An image intellectual property protection scheme for gray-level images using visual secret sharing strategy, *Pattern Recognition Letters*, 23(8), 2002, 931-941.
[4] P.A. Eisen and D.R. Stinson, Threshold visual cryptography schemes with specified levels of reconstructed pixels, *Design, Codes and Cryptography*, 25(1), 2002, 15-61.
[5] J.C. Hou, Visual cryptography for color images, *Pattern Recognition*, 36(7), 2003, 1619-1629.
[6] C.C. Lin and W.H. Tsai, Visual cryptography for gray-level images by dithering techniques, *Pattern Recognition Letters*, 24(1-3), 2003, 349-358.
[7] R. Lukac and K.N. Plataniotis, Bit-level based secret sharing for image encryption, *IEEE Signal Processing Letters*, 11, 2004.
[8] M. Naor, A. Shamir, Visual cryptography, *Proc. EUROCRYPT'94, LNCS* 950, 1994, 1-12.
[9] F.A. Petitcolas, R.J. Anderson, and M.G. Kuhn, Information hiding: a survey, *Proceedings of the IEEE*, 87(7), 1999, 1062-1078.
[10] R.A. Ulichney, Dithering with blue noise, *Proceedings of the IEEE*, 76(1), 1988, 56-79.
[11] P.W. Wong and N.S. Memon, Image processing for halftones, *IEEE Signal Processing Magazine*, 20(4), 2003, 59-70.