DOCUMENT IMAGE SECRET SHARING USING BIT-LEVEL PROCESSING

Rastislav Lukac and Konstantinos N. Plataniotis

Bell Canada Multimedia Laboratory, The Edward S. Rogers Sr. Department of ECE, University of Toronto, 10 King's College Road, Toronto, M5S 3G4 Ontario, Canada
lukacr@ieee.org, kostas@dsp.utoronto.ca

ABSTRACT

A new bit-level based secret sharing scheme for encryption of private financial and pharmaceutical digital documents, and digital signature images is provided. The proposed $\{k, n\}$ secret-sharing method allows for secret sharing of both scanned binary documents and the computer-generated artworks encrypting the document image into n shares. The secret information is recovered only if k (or more) allowed shares are available for decryption. Cryptographic operations for both encryption and decryption procedures are directly performed in the decomposed bit-level domain. The methods reveals the original document unchanged and thus, the scheme satisfies the perfect reconstruction property.

1. INTRODUCTION

A $\{k, n\}$-visual secret sharing (VSS) scheme [1],[3],[6] is the most popular secret sharing technique used for protection of image information. Based on the nature of visual cryptography, binary images such as scanned documents are perfectly suitable for VSS-based encryption. The procedure encrypts the document splitting the image content into n, seemingly random, shares. The secret information can be visually revealed if at least k shares printed as transparencies are stacked together on an overhead projector. If the digital document contains computer-generated artworks such as gray-scale or/and color graphics, company logos, signatures and stamps, which are essential features for document authentication and validity, such a B-bit image is first converted using the image halftoning techniques [7],[8] into the binarized images and then further processed by the VSS scheme [2],[3]. However, due to the frosted/transparent representation of the binary shares as well as the employed halftoning technology, the decrypted document significantly differs from the original document. This decreases the applicability of $\{k, n\}$-VSS schemes.

The proposed $\{k, n\}$-secret sharing scheme operates directly in the decomposed bit-level binary domain of the document images. By stacking individually encrypted bit pla-nes, the scheme produces the B-bit shares useful for secure distribution over the untrusted public networks [4]. The decryption function recovers the original B-bit image content unchanged and without the need for expensive postprocessing operations. The decrypted output is readily available in digital form, and there is no requirement for external hardware or manual intervention. Since the decrypted document image, identical to the original, is available in a digital format, the method is attractive for modern communication and document image processing systems.

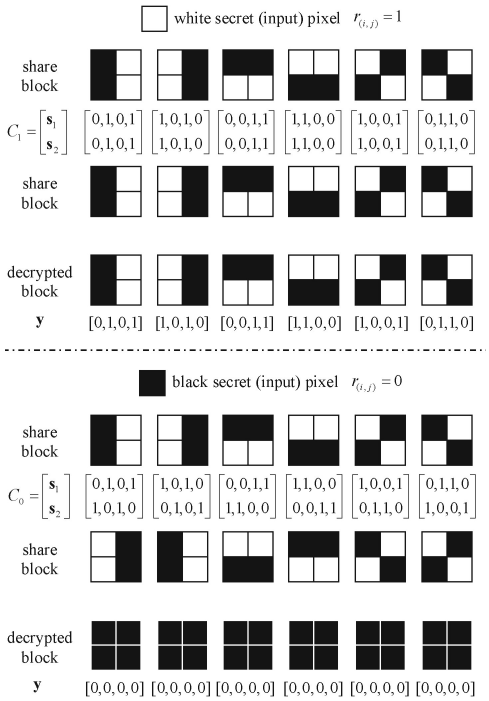

Fig. 1. Visual cryptography strategy.

2. VISUAL SECRET SHARING SCHEME

Assuming a $K_1 \times K_2$ binary image, each binary pixel $r_{(i,j)}$ (with the value 0 denoting the black and 1 denoting the white) determined by spatial coordinates $i = 1, 2, ..., K_1$ and $j = 1, 2, ..., K_2$ is replaced with a $m_1 \times m_2$ block of black and white pixels in each of the n shares [1]. Repeating the process for each input pixel, a $K_1 \times K_2$ binary image is encrypted into n binary shares $S_1, S_2, ..., S_n$ 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 $\{2, 2\}$-threshold scheme which is the basic case designed within the $\{k, n\}$-VSS framework [2]. Assuming for simplicity 2×2 share 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 via $[\mathbf{s}_1, \mathbf{s}_2]^T \in C_0$ for $r_{(i,j)} = 0$, and $[\mathbf{s}_1, \mathbf{s}_2]^T \in C_1$ for $r_{(i,j)} = 1$.

0-7803-8554-3/04/$20.00 ©2004 IEEE.

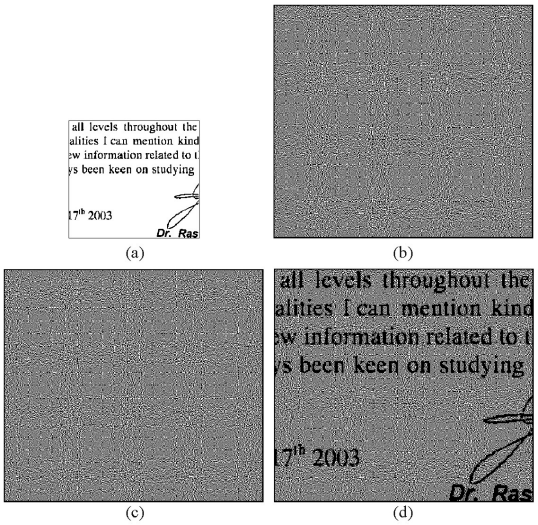

Fig. 2. Conventional $\{2,2\}$-VSS [6]: (a) original binary document, (b,c) share images, (d) decrypted document.

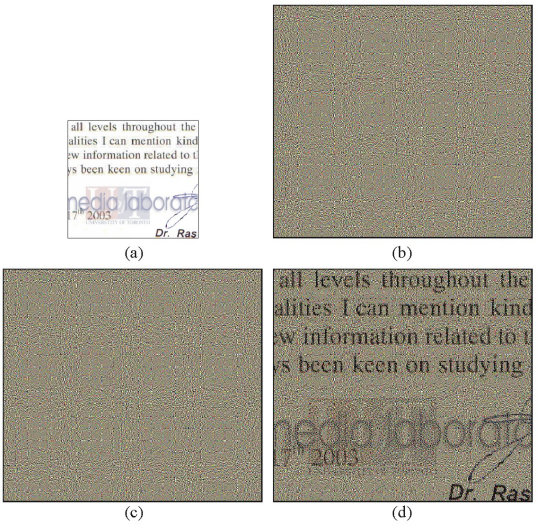

Fig. 3. Halftoning based $\{2,2\}$-VSS [2]: (a) original document with a color artwork, (b,c) share images, (d) decrypted document.

The sets C_0 and C_1 are obtained by permuting the columns of the $n \times m_1 m_2$ basis matrices A_0 and A_1, respectively [3]. 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 [6]. For a $\{2,2\}$-scheme considered here, the basis matrices

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

correspond to 2×2 blocks $\mathbf{s}_1$ and $\mathbf{s}_2$, i.e. $m_1 = 2$ and $m_2 = 2$.

Fig.1 shows the principle of both encryption and decryption used in visual cryptography. 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.

Decrypting 2×2 share blocks $\mathbf{s}_1$ and $\mathbf{s}_2$ used in a $\{2,2\}$-scheme the 2×2 decrypted block $\mathbf{y}$ is produced as black $\mathbf{y} = [0,0,0,0]$ if $\mathbf{s}_1 \neq \mathbf{s}_2$. Otherwise the share blocks $\mathbf{s}_1$ and $\mathbf{s}_2$ are identical and the decrypted block is recovered with the same spatial arrangement of binary pixels as in the share blocks. Note that by utilizing the frosted/transparent representation of the blocks the decryption function can be generalized for any $\{k,n\}$ configuration, however, from an application point of view small practical sharing configurations such as the $\{2,2\}$-scheme will suffice in most cases.

Figs.2-3 show the images obtained using the $\{2,2\}$-VSS scheme applied to both the binary document (*Fig.2*) and the document with a color artwork (*Fig.3*). Visual inspection of both the original image and the recovered image indicates that the decrypted image is darker, the input image is of quarter size compared to the decrypted output, and the output document contains a number of artifacts. Moreover, *Fig.3d* shows that the decrypted output contains a number of shifted colors resulting from the nature of the algorithm.

3. PROPOSED METHOD

Let us consider a digital $K_1 \times K_2$ input image with a B-bit per pixel representation. For example, the 8-bit representation can describe 256 gray-scale levels (integers ranging from 0 to 255). Thus each integer pixel value can be expressed equivalently in a binary form using [4]:

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

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, and from this point of view constitutes the ideal preprocessing step for share-based encryption [4]. Note that the binary documents are available in a binary digital format, and thus, the bit-level decomposition is not needed. However, for the documents with computer-generated gray-scale and color artworks [5], the bit-level decomposition is essential to both encryption and decryption steps.

After achieving B binary planes, the conventional VSS encryption function 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 $s'^b_{(u,v)} \in S^b_1$ and $s''^b_{(u,v)} \in S^b_2$ denote the pixels in the $2K_1 \times 2K_2$ binary shares S^b_1 and S^b_2, respectively, the B-bit share pixels $s'_{(u,v)} \in S_1$ and $s''_{(u,v)} \in S_2$, for $u = 1,2,...,2K_1$ and $v = 1,2,...,2K_2$, are constituted by bit-level stacking as follows [4]:

$$s'_{(\cdot,\cdot)} = s'^1_{(\cdot,\cdot)} 2^{B-1} + s'^2_{(\cdot,\cdot)} 2^{B-2} + ... + s'^{B-1}_{(\cdot,\cdot)} 2 + s'^B_{(\cdot,\cdot)} \tag{3}$$

$$s''_{(\cdot,\cdot)} = s''^1_{(\cdot,\cdot)} 2^{B-1} + s''^2_{(\cdot,\cdot)} 2^{B-2} + ... + s''^{B-1}_{(\cdot,\cdot)} 2 + s''^B_{(\cdot,\cdot)} \tag{4}$$

Depending on the particular bit-levels on which $f_e(\cdot)$ is applied and the random choice of the block representing $o^b_{(i,j)}$, the original pixel $o_{(i,j)}$ and B-bit share pixels $s'_{(2i-1,2j-1)}$, $s'_{(2i-1,2j)}$, $s'_{(2i,2j-1)}$, $s'_{(2i,2j)}$ and $s''_{(2i-1,2j-1)}$, $s''_{(2i-1,2j)}$, $s''_{(2i,2j-1)}$, $s''_{(2i,2j)}$

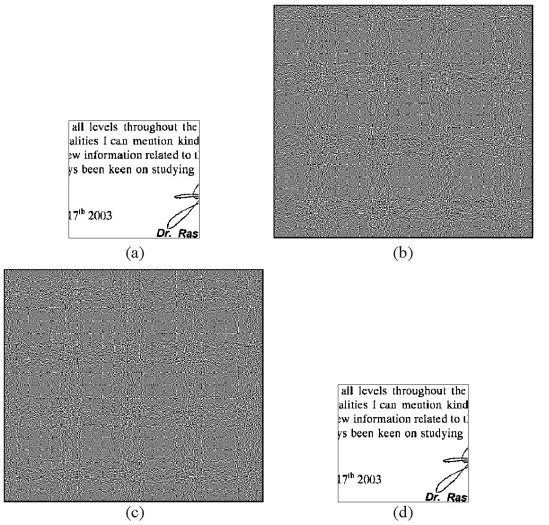

Fig. 4. Proposed $\{2, 2\}$ secret sharing scheme: (a) original binary document, (b,c) share images, (d) decrypted document.

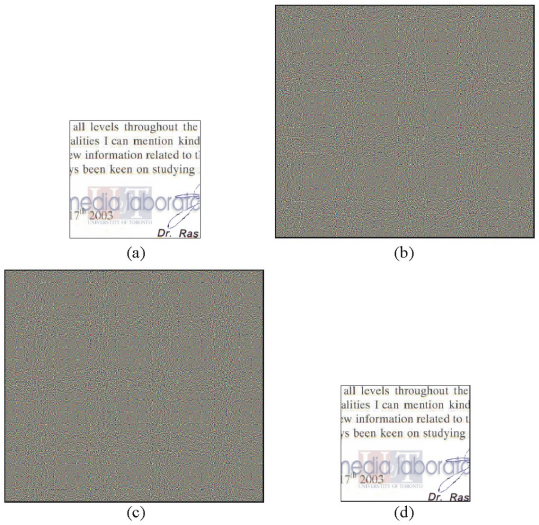

Fig. 5. Proposed $\{2, 2\}$ secret sharing scheme: (a) original document with a color artwork, (b,c) shares, (d) decrypted document.

can differ significantly. Assuming that N denotes the number of unique matrices obtained by column permutations of the basis matrices corresponding to the $\{k, n\}$-scheme, the B-bit pixel is encrypted using one of N^B unique $m_1 \times m_2$ share blocks of B-bit pixels. Thus, compared to the schemes operating on binary (dithered) images which allows for using only N unique share blocks of binary pixels, the method increases security and prevents unauthorized decryption through brute-force enumeration.

To faithfully decrypt the original B-bit image from its B-bit shares, the decryption function must satisfy the perfect reconstruction property meaning that the output should be identical to the original input. This can be obtained only if the encryption and decryption operations are reciprocal. In the case of $\{2, 2\}$-schemes considered in this paper, the decryption function is defined as [4]:

$$o^b_{(i,j)} = \begin{cases} 1 & \text{for } s'^b_{(2i-1,2j-1)} = s''^b_{(2i-1,2j-1)} \\ 0 & \text{for } s'^b_{(2i-1,2j-1)} \neq s''^b_{(2i-1,2j-1)} \end{cases} \quad (5)$$

where (i, j) denotes location in a $K_1 \times K_2$ reference image. This function takes advantage of the arrangements of the binary pixels in the sets C_0 and C_1 for the specific case of a $\{2, 2\}$ scheme. By decimating via a factor of 2 it is possible to associate the share bits located at $(2i - 1, 2j - 1)$ to the original bit located at (i, j) for each of the bit-levels $b = 1, 2, ..., B$. Note that more general expression can be obtained through the reciprocal concept and the comparison of the complete share blocks obtained for a particular $\{k, n\}$ configuration [4]. However, $\{2, 2\}$ secret sharing schemes considered in this paper are suitable for practical purposes.

The bit-level processing allows for a completely different interpretation of the application of the $\{k, n\}$ secret sharing framework. Since encryption and decryption are designed here reciprocal due to computer-centric processing, perfect reconstruction, a property unavailable in conventional $\{k, n\}$ secret sharing schemes is obtained. The faithful recovery of the encryption input in digital form makes our scheme ideal for integration into any image processing and communication solution.

Figs.4-5 show the results obtained through the application of the proposed method. Compared to the results corresponding to popular VSS solutions (*Figs.2-3*) it is not difficult to see that in our method produces a $K_1 \times K_2$ noise-free image depicted in *Fig.4d* and *Fig.5d*. This should be contrasted to the $2K_1 \times 2K_2$ decrypted output of the VSS solutions (*Fig.2d* and *Fig.3d*) which contains a number of random, noise like, pixels. Our $\{2, 2\}$ solution recovers the spatial dimensionality of the input as (5) performs simultaneously subsampling and decryption, and the original B-bit pixels are generated by stacking the decrypted bit levels o^b according to (2). Moreover, simple visual inspection reveals that the document obtained via the application of the proposed method is identical to the original.

Fig.6 provides a visual overview of the differences between the shares generated by the proposed framework for the case of the same document separately treated as binary ($B = 1$), gray-scale ($B = 8$) and color image ($B = 3 \times 8$). Depending on the depth of the B-bit representation of the input document image, the shares contain binary, gray-scale or color random information, respectively. The figure suggests that as we move towards richer visual inputs the degree of security afforded by our method increases, as it becomes increasingly difficult to "guess" by operating on the integer (B-bit) domain [4].

Figs.7-8 demonstrate the sharing capability of selected higher order $\{k, n\}$-configurations. In this case, both logical operations and comparisons of the whole share blocks should be used to decrypt $o^b_{(i,j)}$. *Fig.7a* depicts the input image and *Figs.7b-d* depict the shares obtained using the proposed $\{3, 3\}$ method with the basis matrices defined as follows [6]:

$$A_0 = \begin{bmatrix} 0,0,1,1 \\ 0,1,0,1 \\ 0,1,1,0 \end{bmatrix}, \quad A_1 = \begin{bmatrix} 1,1,0,0 \\ 1,0,1,0 \\ 1,0,0,1 \end{bmatrix} \quad (6)$$

Using any two shares, the procedure does not recover any useful visual information since logical comparisons of the two share blocks obtained using either $o^b_{(i,j)} = 0$ or $o^b_{(i,j)} = 1$ results in decrypted blocks with one white and three black pixels. If the required three shares are available for decryption, the original bit $o^b_{(i,j)}$ is decrypted, and the scheme produces the output (*Fig.7e*) which is identical to the original (*Fig.7a*).

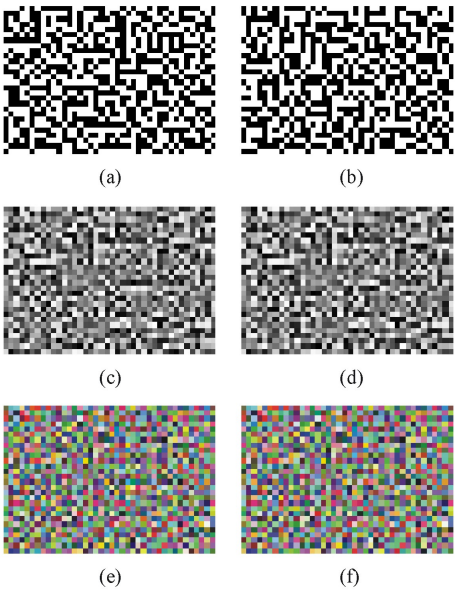

Fig. 6. Details of the shares S_1 (a,c,e) and S_2 (b,d,f) generated by the proposed B-bit $\{2, 2\}$ secret sharing method applied to binary document treated as: (a,b) binary image with $B = 1$, (c,d) gray-scale image with $B = 8$, (e,f) color image with $3 \times (B = 8)$. Based on the image representation of the original document, the shares contain random information in the form of: (a,b) binary noise, (c,d) gray-scale noise, (e,f) color noise.

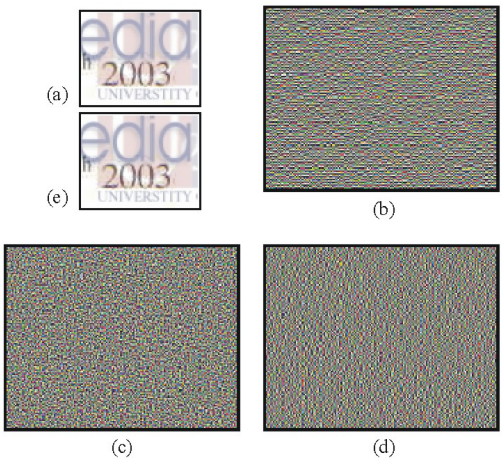

Fig. 7. Proposed $\{3, 3\}$ secret sharing scheme: (a) original document with a color artwork, (b-d) share images, (e) obtained output.

Fig.8 depicts the images obtained using the proposed method with a $\{2, 6\}$-threshold structure. In this case, the basis matrices are defined as follows [6]:

$$A_0 = \begin{bmatrix} 0,1,0,1 \\ 1,0,1,0 \\ 1,1,0,0 \\ 0,0,1,1 \\ 0,1,1,0 \\ 1,0,0,1 \end{bmatrix}, \quad A_1 = \begin{bmatrix} 1,1,0,0 \\ 1,1,0,0 \\ 1,1,0,0 \\ 1,1,0,0 \\ 1,1,0,0 \\ 1,1,0,0 \end{bmatrix} \tag{7}$$

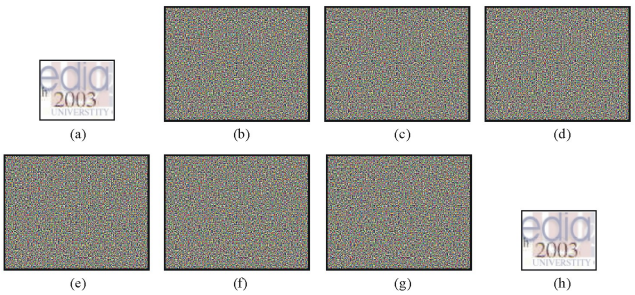

Fig. 8. Proposed $\{2, 6\}$ secret sharing scheme: (a) original document with a color artwork, (b-g) share images, (h) decrypted document obtained using any two shares of (b-g).

As it is shown in *Figs.8b-g*, the proposed scheme produces six, seemingly unrelated, shares. The original document image is decrypted using any two shares (*Fig.8h*).

4. CONCLUSION

A new secret sharing scheme for document image encryption was introduced. The method processes the document images operating at the bit-levels. Using the proposed sche-me, the personal document (financial, medical, signature) images are encrypted into the required number of shares and the secret information is revealed only when the allowed shares are cryptographically processed at the image bit-levels. The proposed computer-centric processing of the shares allows to obtain the original document unchanged and thus, the proposed method satisfies the perfect reconstruction property. This makes the proposed method attractive for a modern image processing and communication system.

5. REFERENCES

[1] 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*, vol. 23, pp. 931-941, June 2002.

[2] J.C. Hou, "Visual cryptography for color images," *Pattern Recognition*, vol. 36, pp. 1619-1629, July 2003.

[3] C.C. Lin and W.H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognition Letters*, vol. 24, pp. 349-358, January 2003.

[4] R. Lukac and K.N. Plataniotis, "Bit-level based secret sharing for image encryption," *IEEE Signal Processing Letters*, vol. 11, 2004.

[5] R. Lukac and K.N. Plataniotis, "Colour image secret sharing," *IEE Electronics Letters*, vol. 40, pp. 529-530, April 2004.

[6] M. Naor and A. Shamir, "Visual Cryptography," *Proc. EUROCRYPT'94, LNCS*, vol. 950, pp. 1-12, 1994.

[7] R.A. Ulichney, "Dithering with blue noise," *Proceedings of the IEEE*, vol. 76, pp. 56-79, January 1988.

[8] P.W. Wong and N.S. Memon "Image processing for halftones," *IEEE Signal Processing Magazine*, vol. 20, pp. 59-70, July 2003.