Image Scrambling Without Bandwidth Expansion

Dimitri Van De Ville, *Member, IEEE*, Wilfried Philips, *Member, IEEE*, Rik Van de Walle, *Member, IEEE*, and Ignace Lemahieu, *Senior Member, IEEE*

***Abstract*—Image-scrambling schemes are designed to render the image content unintelligible. Wyner has proposed an elegant one-dimensional (1-D) scrambling scheme without bandwidth expansion, making use of the discrete prolate spheroidal sequences (DPSS). The DPSS are optimal regarding their energy concentration in a given frequency subband. In this paper, we propose the two-dimensional (2-D) extension and application of this algorithm. We discuss new possibilities introduced by the 2-D approach. We also include experimental results.**

***Index Terms*—Conditional access, content protection, discrete prolate spheroidal sequences (DPSS), Hadamard matrix, image scrambling, orthogonal transforms.**

I. Introduction

SECURITY of image and video data becomes increasingly important for many applications, e.g., pay-TV, confidential transmission of video conferencing, video surveillance, secure facsimile, medical, and military applications. Two main groups of technologies have been developed for this purpose. The first one is content protection through encryption. Proper decryption of the data requires a key [1]–[4]. The second one is digital watermarking, which aims at embedding a message into the multimedia data [5]–[8]. These two technologies could be used complementary to each other. This paper will focus on the first type of technique.

A scrambling scheme, which renders content unintelligible, can be part of a secure multimedia system [9]. In particular, an image-scrambling scheme transforms an image into another unintelligible image, based on keys only known to the senders and the receivers. Initially, video scrambling schemes were fairly simple because they needed to be implemented in analog electronics. The advent of fast and affordable VLSI electronics made it possible to store images into a frame buffer and perform (de)scrambling operations digitally. The early digital scrambling techniques include methods such as line reversal, line dispersal, and line segment swapping. A commercially deployed algorithm permutes lines [10]. These simple techniques are prone to "correlation attacks;" i.e., the correlation properties available in typical images could be employed to restore the image [11]. Matias *et al.* [12] presented a more advanced way to reorder the pixel data: they change the scan order according to a space-filling curve. Essentially, all these techniques change the scan order of the images.

Another possibility is to scramble the image in a transformed domain. Zeng *et al.* [13] presented a technique to scramble an MPEG video sequence in the DCT domain. Their main concern is to have a minimum impact on the compression efficiency after scrambling DCT coefficients. Digital encryption could also be applied after (MPEG) compression, resulting in high security.

Wyner presented an interesting technique designed for speech scrambling [14], [15]. Making use of an optimal set of basis functions, he proposed a scrambling scheme based on an orthonormal linear transform which results in a negligible expansion of bandwidth. In this paper, we extend the transform to two-dimensional (2-D), which makes it suitable for image scrambling. This opens up a new class of image-scrambling schemes. We also show that the 2-D scrambling scheme offers a wider scrambling potential compared to the one-dimensional (1-D) scheme. The scrambling operation itself needs a key. We will only briefly engage into the key management—the selection and the update of this key—using Hadamard matrices.

The paper is organized as follows. In Section II, we briefly review the original 1-D scrambling method presented by Wyner [14]. Next, in Section III, we show the 2-D extension and apply it to image scrambling. Next, we add a note on the encryption; i.e., the selection of the key. In Section V we present some experimental results of the scrambling method, followed by a discussion in Section VI.

II. Brief Review of the 1-D Scrambling Problem

Consider a discrete sequence of real numbers $a(n), -\infty < n < \infty$. The Fourier transform or spectrum of $a(n)$ equals

$$A(f) = \sum_{n=-\infty}^{\infty} a(n)e^{-\mathrm{i}2\pi nf}, \qquad -\infty < f < \infty. \quad (1)$$

Note that the spectrum $A(f)$ is periodic with period 1, and we will consider it only for $|f| \leq (1/2)$. The inner product of two sequences $a(n)$ and $b(n)$ is defined by

$$\langle a, b\rangle = \sum_{n=-\infty}^{\infty} a(n)b(n) \quad (2)$$

and the l_2-norm of $a(n)$ is $\|a\| = \langle a, a\rangle^{1/2}$. All sequences that we consider are part of the vector space l_2 of square-summable sequences.

The sequence a is said band-limited to $[-W, W], 0 \leq W \leq (1/2)$, if the spectrum $A(f) = 0$, for $W < |f| \leq (1/2)$. We

Manuscript received May 2, 2001; revised February 20, 2003. This work was supported in part by the Fund for Scientific Research (FWO), Flanders, Belgium, through a mandate of Research Assistant D. Van De Ville. This paper was recommended by Associate Editor C.-W. Chen.

D. Van De Ville is with the Biomedical Imaging Group, Swiss Federal Institute of Technology Lausanne (EPFL), CH-1015 Lausanne, Switzerland (e-mail: dimitri.vandeville@epfl.ch).

W. Philips is with the Department for Telecommunication and Information Processing (TELIN), Ghent University, B-9000 Ghent, Belgium (e-mail: wilfried.philips@ugent.be).

R. Van de Walle and I. Lemahieu are with the Department of Electronics and Information Systems, B-9000 Ghent, Belgium (e-mail: rik.vandewalle@ugent.be; ignace.lemahieu@ugent.be).

Digital Object Identifier 10.1109/TCSVT.2004.828325

define a band-limiting operator $\mathcal{B}_W$, such that the spectrum of $a' = \mathcal{B}_W a$ equals

$$A'(f) = \begin{cases} A(f), & |f| \le W \\ 0, & |f| > W. \end{cases} \tag{3}$$

This enables us to express the energy concentration of a sequence a inside the frequency band $[-W, W]$ as[1]

$$\mathcal{C}_W(a) = \frac{\|\mathcal{B}_W a\|^2}{\|a\|^2}. \tag{4}$$

We wish to scramble the sequence a by a linear orthonormal invertible transformation. Such a transform is distance preserving and does not enhance additive noise of the scrambled sequence.

In general, a permutation applied to a band-limited sequence a to form a scrambled sequence will introduce new high-frequency components into the spectrum, which were not present in the original spectrum. Bandwidth-preserving scrambling is based on the following general principle. The set $\mathcal{S}_0$ of band-limited sequences, being a subspace of l_2, has an orthonormal basis $\{e_j(n)\}_{j=-\infty}^{\infty}$. Any sequence $a \in \mathcal{S}_0$ can be decomposed as

$$a(n) = \sum_{j=-\infty}^{\infty} \alpha_j e_j(n) \tag{5}$$

where $\alpha_j = \langle a, e_j \rangle$. If we compute a permutation (or in fact any orthonormal transformation) $\{\beta_j\}$ of the original coefficients $\{\alpha_j\}$, then we obtain a scrambled sequence

$$b(n) = \sum_{j=-\infty}^{\infty} \beta_j e_j(n). \tag{6}$$

Because the scrambled sequence b is still in $\mathcal{S}_0$, this is a band-limited scrambled sequence.

In practice, we have to consider sequences a with a finite support on the interval $[0, N-1]$, i.e., $a(n) = 0$, for $n \notin [0, N-1]$. Although a nonzero sequence with finite support can never be band-limited with $W < (1/2)$, its energy concentration in a certain band $[-W, W]$ can be high. Slepian [16] showed that the DPSS form an orthonormal basis that are able to span the subspace of sequences that are approximately band limited; i.e., with an optimal energy concentration. Wyner used these ideas to design a scrambling scheme for 1-D scrambling with negligible expansion of bandwidth [14]. The DPSS are a set of N real-valued sequences $\{\phi_j(n)\}_{j=0}^{N-1}$, and a corresponding set of real numbers $\{\lambda_j\}_{j=0}^{N-1}$ [16]–[18]. They are related to a given frequency band $[-W, W]$, i.e., the DPSS are the normalized eigenvectors of the real and symmetric matrix

$$[\mathbf{V}]_{m,n} = \frac{\sin(2\pi W(m-n))}{\pi(m-n)} \qquad 0 \le m, \quad n \le N-1. \tag{7}$$

The sets $\{\phi_j(n)\}_{j=0}^{N-1}$ and $\{\lambda_j\}_{j=0}^{N-1}$, correspond to the normalized eigenvectors and the eigenvalues of this kernel. The eigenvalues λ_j are real and with multiplicity 1, all between 0 and 1, and represent the energy concentration $\mathcal{C}_W(\phi_j)$ in the frequency interval $[-W, W]$ of the corresponding eigenvector ϕ_j. The sequences ϕ_j also form an orthonormal basis for any sequence a with support on $[0, N-1]$, such that

$$a(n) = \sum_{j=0}^{N-1} \alpha_j \phi_j(n) \tag{8}$$

where $\alpha_j = \langle a, \phi_j \rangle$. By convention, the vectors ϕ_j are sorted such that the corresponding λ_j are decreasing.

We now assume a sequence a with a large energy concentration to the band $[-W, W]$. Using the DPSS corresponding to the support $[0, N-1]$ and the bandwidth W, we compute the coefficients α_j. Next, we choose an integer parameter $v \in [1, N]$, such that λ_{v-1} is still sufficiently large. The coefficients $\alpha_j, 0 \le j < v$, are now scrambled by an orthogonal $v \times v$ matrix $\mathbf{M}$. This matrix is the "key" of the scrambling scheme. We obtain a scrambled sequence

$$b(n) = \sum_{j=0}^{v-1} \beta_j \phi_j(n) + \sum_{j=v}^{N-1} \alpha_j \phi_j(n) \tag{9}$$

where $\boldsymbol{\beta} = \mathbf{M}\boldsymbol{\alpha}$, introducing the vectors $\boldsymbol{\alpha} = (\alpha_j)_{j=0}^{v-1}$ and $\boldsymbol{\beta} = (\beta_j)_{j=0}^{v-1}$. Note that we can rewrite (9) as

$$b(n) = a(n) + \sum_{j=0}^{v-1} (\beta_j - \alpha_j)\phi_j(n) \tag{10}$$

so we only need to compute $\langle a, \phi_j \rangle$ for $j = 0, \ldots, v-1$. Wyner showed that the energy concentration of b differs at most $1 - \lambda_{v-1}$ compared to the concentration of

$$a : |\mathcal{C}_W(a) - \mathcal{C}_W(b)| < (1 - \lambda_{v-1}).$$

Therefore, one should not choose v too large.

The reconstruction of the original sequence is straightforward. The coefficients $\beta_j = \langle b, \phi_j \rangle$ are descrambled by the inverse key: $\boldsymbol{\alpha} = \mathbf{M}^{\mathrm{T}}\boldsymbol{\beta}$. Next, $\boldsymbol{\alpha}$ is used to reconstruct (exactly) the original sequence $a(n)$.

III. 2-D Scrambling Problem

In order to design a 2-D scrambling scheme, we need to extend the basic notions of Section II to two dimensions. We consider a 2-D array $a(n_1, n_2), 0 \le n_1 \le N_1 - 1, 0 \le n_2 \le N_2 - 1$. It is convenient for many operations, such as the inner product, to address the 2-D array lexicographically: $a(n) = a(n \bmod N_1, \lfloor n/N_1 \rfloor)$, where $0 \le n \le N_1 N_2 - 1$. In that way, the inner product can still be expressed as

$$\langle a, b \rangle = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} a(n_1, n_2) b(n_1, n_2) = \sum_{n=0}^{N_1 N_2 - 1} a(n) b(n). \tag{11}$$

The 2-D spectrum can be obtained by

$$A(f_1, f_2) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} a(n_1, n_2) e^{-\mathrm{i}2\pi \langle (n_1 n_2)(f_1 f_2) \rangle}, \quad -\infty < f_1, f_2 < \infty. \tag{12}$$

There are several ways to define a 2-D band-limiting operator. Here we define $\mathcal{B}_W$ such that the spectrum of $a' = \mathcal{B}_W a$ is limited to a 2-D square passband region:

$$A'(f_1, f_2) = \begin{cases} A(f_1, f_2), & |f_1| \le W \quad \text{and} \quad |f_2| \le W \\ 0, & \text{otherwise.} \end{cases} \tag{13}$$

[1] Due to its periodicity, we only consider the spectrum for $|f| \le (1/2)$.

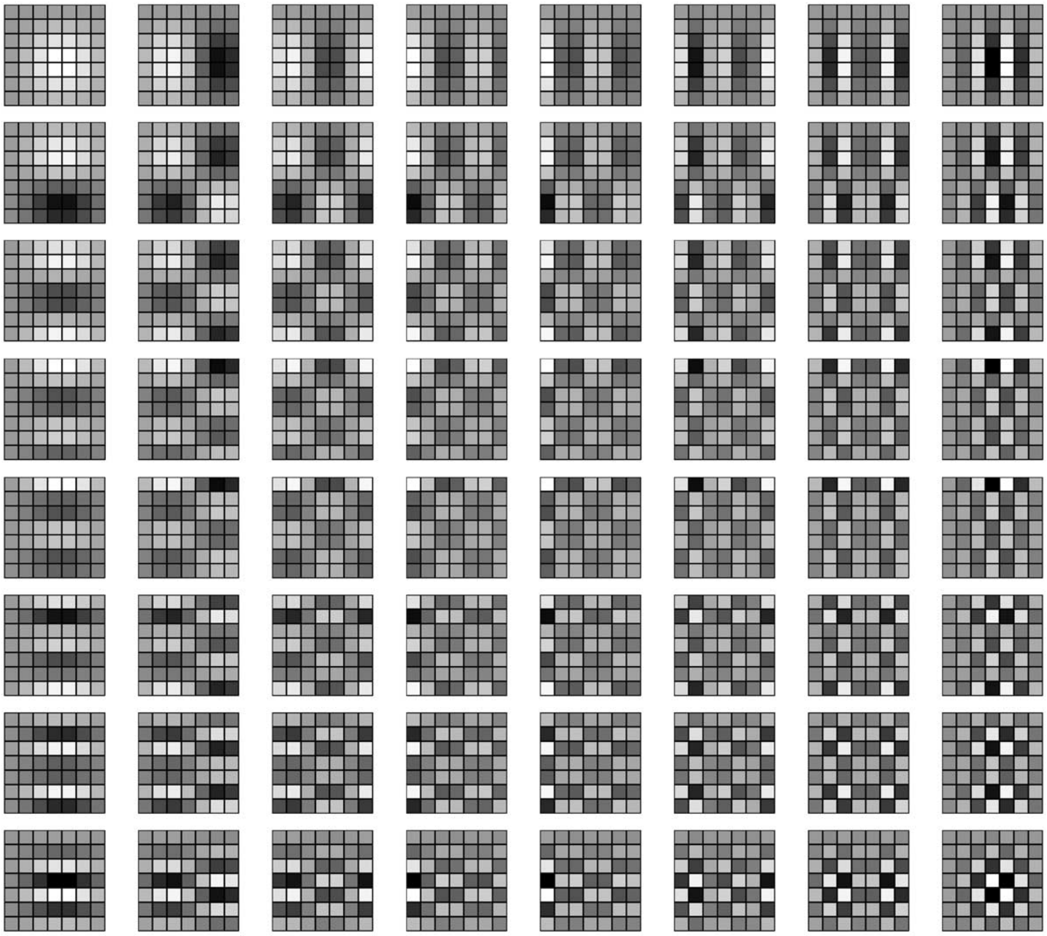

Fig. 1. Example of the 2-D DPSS basis set for $N = 8, W = 0.25$.

The energy concentration of a to this passband equals

$$\mathcal{C}_W(a) = \frac{\|\mathcal{B}_W a\|^2}{\|a\|^2}. \tag{14}$$

The extension of the DPSS to 2-D is straightforward. In particular, the 2-D DPSS corresponding to the square passband region are given by

$$\phi^{(2D)}_{j_1,j_2}(n_1,n_2) = \phi^{(1D)}_{j_1}(n_1)\phi^{(1D)}_{j_2}(n_2) \tag{15}$$

where $0 \leq n_1, j_1 \leq N_1 - 1$ and $0 \leq n_2, j_2 \leq N_2 - 1$. The corresponding eigenvalues are $\lambda^{(1D)}_{j_1}\lambda^{(1D)}_{j_2}$. In the case of square arrays $(N_1 = N_2 = N)$, there are $N(N-1)/2$ pairs of equal eigenvalues and N single eigenvalues. In Fig. 1, we show the basis set of the 2-D DPSS for $N = 8$ and $W = 0.25$.

As mentioned before, the 2-D extension can be approached more generally. Instead of using a square or rectangular passband region, one could also use a circular or hexagonal passband [19], resulting in nonseparable 2-D basis functions.

Analogously to the 1-D scrambling scheme, the coefficients $\alpha_j = \langle a, \phi_j \rangle$ corresponding to large eigenvalues λ_j are scrambled for the 2-D case. The 2-D scrambling scheme offers an additional advantage. The 2-D DPSS have several pairs of equal eigenvalues, corresponding to eigenvectors which are symmetric, i.e., $\phi_{j_1,j_2}(n_1,n_2) = \phi_{j_2,j_1}(n_2,n_1)$. The coefficients belonging to these eigenvectors can be scrambled mutually without bandwidth expansion, and independently, of their eigenvalue λ_j. Table I shows an illustrative example for $N = 3$ and $W = 0.35$. Suppose we choose $v = 3$, then the coefficients corresponding to the three largest eigenvalues can be scrambled freely. However, the coefficients corresponding to the eigenvalues $j = 4, 5$ and $j = 6, 7$, which correspond to eigenvectors that are less well concentrated, can also be scrambled mutually without affecting the bandwidth of the scrambled array because

TABLE I
EIGENVALUES CORRESPONDING TO THE 2-D DPSS PROBLEM FOR $N = 3, W = 0.35$

j	λ_j	corresponding coefficients
0	0.9926	can be scrambled freely
1	0.8482	
2	0.8482	
3	0.7248	
4	0.2514	can be scrambled mutually
5	0.2514	
6	0.2148	can be scrambled mutually
7	0.2148	
8	0.0637	

their eigenvalues are the same, i.e., they do not alter the energy concentration of the scrambled sequence.

The 2-D scrambling scheme can be applied in two ways. First, one could send the scrambled coefficients, eventually combined with a compression scheme. We will elaborate on this approach more in Section VI. Second, the scrambled coefficients can be used to reconstruct a scrambled image. In that case, the compound transformation can be written as: a matrix multiplication $\boldsymbol{\alpha} = \mathbf{S}a$, where the $(j+1)$th row of $\mathbf{S}$ contains the basis vector ϕ_j; the scrambling transformation $\boldsymbol{\beta} = \mathbf{M}\boldsymbol{\alpha}$; the composition $b = \mathbf{S}^{\mathrm{T}}\boldsymbol{\beta}$. So we obtain the compound matrix

$$\mathcal{M} = \mathbf{S}^{\mathrm{T}}\mathbf{M}\mathbf{S}. \tag{16}$$

If we want to store the scrambled images using the same representation as the original images, we need to determine the range of the transformation of (16). At this moment, we assume that the pixel values $a(n)$ are in the interval $[-1, 1]$. Since $\mathcal{M}$ is an orthonormal transformation matrix, and therefore distance preserving, any $b(n)$ is bounded by $\max \|a\| = \sqrt{N_1 N_2}$. However, we can also compute the effective maximum scrambled value for a given $\mathcal{M}$

$$\gamma = \max_n \left(\sum_{j=0}^{N_1 N_2 - 1} |\mathcal{M}_{n,j}| \right). \tag{17}$$

Subsequently, we can say that the worst case range covered by elements $b(n)$ is $[-\gamma, \gamma]$. In Section V we will further investigate the influence of γ. We first deduce the following scrambling scheme for 8-bit grayscale pixel values.

- The original pixel values $I(n_1, n_2) \in [0, L-1]$ are stored as $a(n_1, n_2) = I(n_1, n_2) - L/2$.
- The scrambled array is determined, either by using the compound transformation $b = \mathcal{M}a$, or by computing only those coefficients which need to be scrambled [as suggested by (10)].
- The pixel values of the scrambled image are $I'(n_1, n_2) = \mathrm{round}(b(n_1, n_2)/\gamma + L/2)$, where $\mathrm{round}(\,\cdot\,)$ returns the nearest integer.
- The descrambling stage at the receiver side gets the scrambled image and stores it as $\hat{b}(n_1, n_2) = \gamma(I'(n_1, n_2) - L/2)$. After performing the inverse transformation, the descrambled image equals $\hat{I}(n_1, n_2) = \mathrm{round}(\hat{a}(n_1, n_2) + L/2)$.

The (necessary) rescaling operations have two disadvantages. First, due to rounding, the descrambled image $\hat{I}$ will not exactly match the original image. Second, noise added to the scrambled image is amplified by a factor γ.

IV. Note on the Encryption

Although it is not our intention to consider in detail the choice of the "key" (the transformation of a part of the coefficients corresponding to the DPSS basis vectors), we still want to give an indication of the size of the key space.

When the encryption (the choice of $\mathbf{M}$) only takes into account permutations, we are able to transform a vector of length k in $k!$ possible ways. However, many of these possible keys produce only a small change of the coefficients. Another option, based on an article of Šenk [20], is to consider (normalized) Hadamard matrices.

TABLE II
SIZE OF THE SPACE FROM WHICH THE KEY CAN BE CHOSEN IN THE CASE OF PERMUTATIONS AND HADAMARD MATRICES AS FUNCTION OF k (THE NUMBER OF COEFFICIENTS THAT ARE SCRAMBLED) [20]

	k						
	8	12	16_1	16_2	16_3	16_4	16_5
permutations	2^{15}	2^{28}	2^{44}	–	–	–	–
Hadamard matrices	2^{32}	2^{64}	2^{97}	2^{102}	2^{104}	2^{104}	2^{106}

TABLE III
RESULTS OF OUR TEST SET FOR $\gamma = 3$

Test image	Resolution	MAE	MSE
barb	720 × 576	0.771	1.083
board	720 × 576	0.772	1.084
boats	720 × 576	0.770	1.081
cmpnd1	512 × 768	0.697	1.197
finger	512 × 512	0.773	1.086
girl	720 × 576	0.770	1.081
gold	720 × 576	0.771	1.083
zelda	720 × 576	0.771	1.085

A Hadamard matrix $\mathbf{H}$ is a $k \times k$ matrix whose rows and columns are orthogonal and only contains elements $+1$ and -1. The inverse matrix is given by

$$\mathbf{H}^{-1} = \frac{1}{k}\mathbf{H}^{\mathrm{T}} \tag{18}$$

where k is the order of the matrix. The possible orders are restricted to $1, 2$, or $4n, n \in \mathbb{N}$. A Hadamard matrix can be transformed to a new Hadamard matrix by a permutation of the rows and columns or by multiplication of the rows and columns by a factor -1. In this way we can obtain $(k!2^k)^2$ so-called H-equivalent matrices of order k, where some of them are identical [20]. Furthermore, a Hadamard matrix is H-normalized when every element of the first row and first column is equal to $+1$. This matrix is known as "the Hadamard matrix."

The transformation matrix $\mathbf{M}$ which will be the key of the algorithm, can be chosen as a scaled version of an H-equivalent matrix

$$\mathbf{M} = \frac{1}{\sqrt{k}}\mathbf{P}_r\mathbf{H}\mathbf{P}_c \tag{19}$$

where $\mathbf{P}_r$ and $\mathbf{P}_c$ are the permutation matrices of rows and columns (possibly with a change of sign), respectively. The central matrix $\mathbf{H}$ is the original H-normalized Hadamard matrix. This approach has many advantages compared to the use of permutations only.

- The size of the key space is substantially extended. Table II compares the size of the space when using permutations and Hadamard matrices. Note that for some orders multiple non-H-equivalent matrices exist (e.g., for order 16 there are five of those), enlarging the size of the key space even more [21].

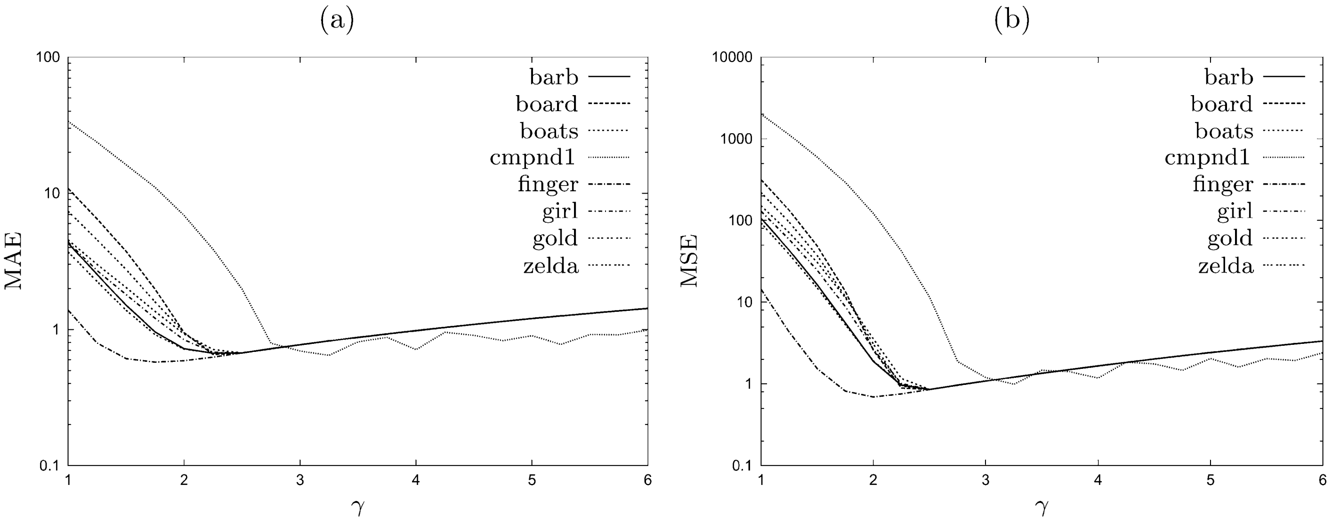

Fig. 2. Error after scrambling/descrambling as a function of the scaling term γ. (a) MAE. (b) MSE. ($L = 255$.)

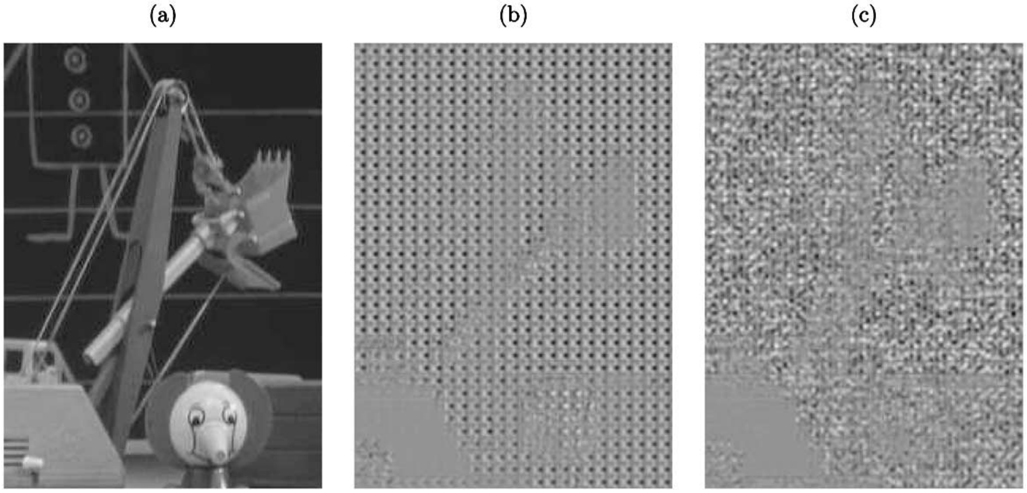

Fig. 3. Part of the "board" test image. (a) Original. (b) Scrambled with one key. (c) Scrambled with a key that is changed each block.

- The possible keys can simply be addressed by means of the enumeration algorithm for permutations of Knuth [22, algo. 3.3.2P].
- As opposed to permutations, every possible H-equivalent matrix provides (about) the same degree of "mixing" the coefficients [23].
- The obtained level of security and unintelligibility can be increased by changing the key for each processed block, for example, based on a cryptographic pseudo-random number generator.

V. Results

To show the effect of the 2-D scrambling scheme, we implemented a prototype in software. In particular, we performed the scrambling operations on 8×8 blocks of the image. We used the 2-D DPSS basis functions for $W = 0.25$. The eight coefficients ($v = 8$) corresponding to the eight largest eigenvalues (out of 64) are scrambled using a Hadamard matrix of (19). The eigenvalue corresponding to $\lambda_{v-1} = \lambda_7$ is 0.970 34, so bandwidth expansion is negligible. Additionally, 50 coefficients corresponding to pairs of equal eigenvalues are permuted mutually. Table III lists the eight images of our test set and their resolutions. Our test set contains typical grayscale images, an image with b/w text ("cmpnd1"), and a fingerprint ("finger").

As we mentioned already in Section III, we want γ to be as small as possible in order not to enhance noise introduced on the scrambled image. Theoretically, γ should be chosen 8, but using (17), we obtain for our key space empirically $\gamma = 6.8 \pm 0.1$ (measured for 1000 random key selections). The computation of the mean absolute error (MAE) and mean squared error (MSE) of our image set for a whole range of γ (see Fig. 2) shows that $\gamma = 3$ is sufficient to obtain an MAE and MSE of about 1 (for $L = 255$). For a lower value of γ, too many values get truncated at the pixel value range, resulting in a distorted reconstruction. The results for $\gamma = 3$ are summarized in Table III. For all test images, the errors are visually unnoticable and tolerable for most applications.

As a representative example, we show in Fig. 3 a part of the "board" test image, respectively, the original, scrambled with one key, and scrambled with a key that is changed for each block. The original image content is highly unintelligible, especially for the third case. These results employ only a quarter of the total frequency range. We also notice that the fixed point of the transformation's matrix multiplication corresponds in the current algorithm to the mid-gray level (i.e., $L/2$), which renders some parts of the image, such as the body of the crane vaguely recognizable. Depending on the application, it might be important to provide a workaround; e.g., one could choose another fixed point or encode the difference between subsequent blocks.

VI. Discussion

The proposed 2-D scrambling scheme puts forward the basic assumption that the image is band-limited. Most images contain some high-frequency components caused by edges. However, the scrambling scheme is still useful for those images. First, the assumption that a significant part of the energy is within a given band is in practice still true. Second, the scrambling operation avoids expanding the image's bandwidth, i.e., the scrambled image does not introduce new frequency components outside a given frequency region.

The computation of the 2-D DPSS is based on the selection of the passband region. In general, a smaller passband will give less DPSS with high energy concentrations and, thus, fewer coefficients to be scrambled, consequently also providing less security. For some applications, it can be interesting though to have a certain level of remaining intelligibility [4].

The image scrambling scheme, as it is proposed in the previous section, is not very interesting for "analog" video applications such as pay-TV. Since the video signal is transmitted line by line, the receiver and sender are required to obtain exactly the same synchronization to prevent missalignment of the blocks. On the other hand, in a digital environment, one could use the scheme in cascade for situations where images are expected with "typical" characteristics, for example, prior to regular image transmission, storage, or compression.

A completely different approach can be used for a custom image processing system. As mentioned before, the (scrambled) DPSS coefficients can also be transmitted as such. Additionally, there is an interesting relationship between the DPSS and the Karhunen–Loeve transform (KLT). The KLT finds the filter that maximizes the concentration of the output energy for a given power spectrum $S(f)$ of the the input signal. If we choose $S(f)$ equal to the indicator function of DPSS's passband region, we obtain exactly the same result [24]. Therefore, the DPSS decomposition can also be applied as a suitable transform prior to lossy image compression. Similar to what classical JPEG does to DCT coefficients, one could quantize "important" DPSS coefficients better (which are also scrambled), while the remaining ones are quantized roughly. In this case, the passband region can determine the amount of scrambling and the compression ratio, i.e., by coarse quantization outside the passband region.

VII. Conclusion

Protecting images from unauthorized viewing covers a large range of applications. This paper presented a class of image scrambling schemes, based on the 2-D extension of the DPSS.

Experimental results show that the scrambling scheme can render images unintelligible. The frequency region affected by the scrambling scheme can be chosen freely. An interesting selection of the associated key is to use Hadamard matrices. Descrambled images do not exactly match the originals (if the scrambled images need to be represented in the same format), but the very small error is acceptable for many applications. The 2-D scrambling scheme can be applied in two ways: reconstructing a scrambled image, or transmitting the scrambled DPSS coefficients (eventually combined with image compression).

References

[1] M. E. Hellman, "An extension of the Shannon theory approach to cryptography," *IEEE Trans. Inform. Theory*, vol. 23, pp. 289–294, May 1977.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," *Proc. IEEE*, vol. 87, pp. 1062–1078, July 1999.

[3] J. Menezes, P. C. van Oorschoot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1997.

[4] B. Macq and J. Quisquater, "Cryptology for digital TV broadcasting," *Proc. IEEE*, vol. 83, pp. 944–957, June 1995.

[5] I. Cox, J. Kilian, and F. T. Leighton, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, pp. 1673–1687, Dec. 1997.

[6] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proc. IEEE*, vol. 86, pp. 1064–1088, June 1998.

[7] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," *Proc. IEEE*, vol. 87, pp. 1108–1126, July 1999.

[8] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, pp. 1079–1107, July 1999.

[9] A. M. Eskicioglu and E. J. Delp, "An overview of multimedia content protection in consumer electronics devices," *Signal Process. Image Commun.*, vol. 16, no. 7, pp. 681–699, Apr. 2001.

[10] A. Kudelski, "Method for scrambling and unscrambling a video signal," U. S. Patent 5 375 168, Dec. 20, 1994.

[11] M. G. Kuhn. (1998) Analysis of the Nagravision Video Scrambling Method. [Online]. Available: http://www.cl.cam.ac.uk/~mgk25

[12] Y. Matias and A. Shamir, "Video scrambling apparatus and method based on space filling curves," U.S. Patent 5 058 158, Oct. 15, 1991.

[13] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling for digital video," *IEEE Trans. Multimedia.*, vol. 5, pp. 118–129, Mar. 2003.

[14] A. D. Wyner, "An analog scrambling scheme which does not expand bandwidth, Part I: Discrete time," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 261–274, May 1979.

[15] ——, "Analog signal scrambling system," U.S. Patent 4 379 205, Apr. 5, 1983.

[16] D. Slepian, "Prolate spheroidal wave functions, fourier analysis, and uncertainty—V: The discrete case," *Bell Syst. Tech. J.*, vol. 57, no. 5, pp. 1371–1430, May 1978.

[17] J. M. Varah, "The prolate matrix," *SIAM J. Linear Algebra Applicat.*, no. 187, pp. 269–278, 1993.

[18] T. Verma, S. Bilbao, and T. H. Y. Meng, "The digital prolate spheroidal window," in *Proc. ICASSP*, May 1996, pp. 1351–1354.

[19] D. Van De Ville, W. Philips, and I. Lemahieu, "On the N-dimensional extension of the discrete prolate spheroidal window," *IEEE Signal Processing Lett.*, vol. 9, pp. 89–91, Mar. 2002.

[20] V. Šenk, D. Delić, and V. S. Milošević, "A new speech scrambling concept based on Hadamard matrices," *IEEE Signal Processing Lett.*, vol. 4, pp. 161–163, June 1997.

[21] N. J. A. Sloane. (1999) A library of Hadamard matrices. [Online]. Available: http://www.research.att.com/~njas/hadamard

[22] D. E. Knuth, *The Art of Computer Programming*, 2nd ed. Reading, MA: Addison-Wesley, 1981, vol. Seminumerical Algorithms.

[23] D. Delić, V. S. Milošević, and V. Šenk, "A new speech scrambling method—Comparative analysis and a fast algorithm," in *Proc. 8th Eur. Signal Processing Conf.*, Trieste, Italy, 1996, pp. 1705–1708.

[24] C. L. Fancourt and J. C. Principe, "On the relationship between the Karhunen–Loeve transform and the prolate spheroidal wave functions," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, vol. 1, 2000, pp. 261–264.