HADAMARD TRANSFORMS

Arithmetic operations in $GF(2)$ [$GF(2)$ is the Galois or finite field with two elements: 0 and 1] are computationally simpler than in the real domain. This is one of the salient features of the Hadamard transform. The entries of the Hadamard matrices are ± 1, which are related to the (0, 1) field elements in $GF(2)$ by a simple linear transformation. The computational simplicity makes the Hadamard transform suitable for such applications as error correction coding, image compression and processing, signal representation, and others.

We begin with a discussion of the properties of the Hadamard transform and the construction of the associated Hadamard matrices. The key to applying the Hadamard transform to practical problems is the identification of the basis functions and algorithms that perform fast implementations. This article discusses the ramifications of fast implementation algorithms and their application in error correction coding, image compression and processing, and signal representation.

HADAMARD TRANSFORMS

The first work on the Hadamard transform was done by Sylvester, (1), who in 1867 proposed a recursive method for the construction of Hadamard matrices of order $N = 2^k$, for $k = 0, 1, 2, \ldots$. Later, in 1898, Scarpis proved the existence of Hadamard matrices of order $p + 1$ for $p = 3 \pmod 4$ and $p + 3$ for $p = 1 \pmod 4$. In 1893, Hadamard proved that the bound on the determinant of matrices of order N ($M^N N^{N/2}$, where $A = [a_{i,j}]$ and $|a_{i,j}| \leq M$ for all $1 \leq i, j \leq N$) which is met only for Hadamard matrices (2,3,4,5).

The Hadamard Matrix

For any real square, $N \times N$, nonsingular matrix $A = [a_{ij}]$, the Hadamard inequality states that

$$\det A \leq \left[\prod_{i=1}^{N}\left(\sum_{j=1}^{N} a_{ij}^2\right)\right]^{1/2}$$

A matrix H that satisfies the bound with equality is called a *Hadamard matrix.* Multiplying a row or a column by -1 does not destroy the Hadamard property. Similarly, permuting rows and columns does not destroy this property. A matrix H in which the elements of the first row and column are all $+1$'s is called a normalized *Hadamard matrix.*

Definition 1. The *Hadamard matrix,* $H_N = [h_{ij}]_{N\times N}$, of order N is defined as an $N \times N$ square matrix in which (1) all elements are ± 1, and (2) $\sum_k h_{ik}h_{jk} = 0$, $i \neq j$, that is, any two distinct rows are orthogonal. This condition requires that the order N be at least even for a Hadamard matrix to exist.

Existence of the Hadamard Matrix. Except for the all $+1$'s row (or all -1's row), any row of an N-dimensional Hadamard matrix must have exactly $N/2$ $+1$'s and $N/2$ -1's. Moreover, orthogonality requires that, for any two distinct rows, i and j, not involving the all $+1$'s (or -1's) row, there must be $N/4$ columns, where elements of rows i and j are both $+1$'s, both -1's, $+1$'s and -1's, and -1's and $+1$'s. Therefore a Hadamard matrix cannot exist for $N > 2$ which is not a multiple of 4.

Theorem 1. The order of any Hadamard matrix greater than 2 must be divisible by 4.

Proof: Suppose H_N is a normalized Hadamard matrix of order N, $N \geq 3$, and consider the first 3 rows of this matrix. Rows 2 through N must have an equal number of $+1$'s and -1's. Permute the columns of H_N so that the first $N/2$ elements of the second row are $+1$'s and the remaining $N/2$ elements are -1's. Suppose there are α elements of $+1$ in the first $N/2$ elements of the third row. Permute the columns so that the first α elements of the third row are $+1$'s and the elements in the third row in column $N/2 + 1$ to $N/2 + (N - \alpha/2)/2$ are $+1$'s. For the second and third rows to be orthogonal, it requires that

$$2\left[\alpha - \left(\frac{N}{2} - \alpha\right)\right] = 0$$

which implies that $N = 4\alpha$. It follows that the order of any Hadamard matrix of order greater than 2 is divisible by 4.

It remains an open question as to a whether Hadamard matrix of order $4N$, N any positive number, exists. There is no method for constructing Hadamard matrices of order $4N$ for all integer N. In the next subsection we present several methods for the construction of Hadamard matrices with the order of special sequences.

Construction of the Hadamard Matrix

There are a number of approaches to constructing Hadamard matrices. These can be divided into two general categories: those which are based on the construction of S matrices and those which are constructed directly.

The Hadamard matrix, H_N, is said to be in a normal form if the first row and column of the matrix contain only $+1$'s. Aside from the trivial cases of $N = 1$, 2, these conditions can be satisfied only if $N > 2$ is an integer multiple of 4.

Construction Methods Using *S* Matrices

Definition 2. An S matrix of order $N - 1$ is derived from a Hadamard matrix of order N by deleting the first row and column of the Hadamard matrix (row and column with only $+1$ elements) and replacing $+1$'s by 0's and -1's by 1's. An S matrix is called cyclic if each row is obtained by cyclically shifting the previous row one place to the left.

The Quadratic Residue Construction Method. Let $a_1, a_2, \ldots, a_{N-1}$ be the remainders of the numbers 1, 4, 9, . . ., $((N - 1)/2)^2$, N odd and >2, divided by N. The a_i's are called *quadratic residues* modulo N. Then the first row of the S matrix

is constructed as

$$s_0, s_1, \ldots, s_{N-1}$$

where

$$s_0, s_{\alpha_1}, s_{\alpha_2}, \ldots, s_{\alpha_{(N-1)/2}} \quad \text{are} \quad 1's$$

and all other s_j's are 0's. All other rows of S are constructed by cyclically shifting the previous row by one place to the left. This construction produces S matrices of order $N = 4m + 3$, where $m = 0, 1, 2, 3, \ldots$.

Maximal Length Shift Register Construction Method. In this construction the first row of the S matrix is selected to be a maximal length shift register sequence of length $N = 2^m - 1$, where $m = 1, 2, 3, \ldots$. Construction of maximal length sequences up to degree $m = 20$ can be found in Refs. 6 and 7.

The Twin Prime Construction Method. Let p and $q = p + 2$ be two prime numbers. Define two functions $f(i)$ and $g(i)$ as

$$f(i) = \begin{cases} +1 & \text{if the remainder of } i/p \text{ is a quadratic residue modulo } p \\ 0 & \text{if } p \text{ divides } i \\ -1 & \text{otherwise} \end{cases}$$

and

$$g(i) = \begin{cases} +1 & \text{if the remainder of } i/q \text{ is a quadratic residue modulo } q \\ 0 & \text{if } q \text{ divides } i \\ -1 & \text{otherwise} \end{cases}$$

There are $k = (p - 1)(q - 1)/2$ numbers a_i, $i = 1, \ldots, k$ and $1 \le a_i \le pq - 1$ for which $f(i) = g(i)$. Also, let

$$a_{k+j} = (j - 1)q \quad \text{for} \quad 1 < j < p$$

Then the first row of the S_N matrix would be

$$s_0, s_1, s_2, \ldots, s_{pq-1}$$

where

$$s_{a_i} = 0 \quad \text{for} \quad 1 \le i \le k + p$$

and

$$s_j = 1 \quad \text{for other values of j}$$

Sylvester-Hadamard Matrix. The Sylvester-type Hadamard matrices are constructed recursively as

$$H_1 = [1]$$

and

$$H_{2^n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix} \tag{1}$$

$$= H_2 \otimes H_{2^n-1} \tag{2}$$

where $\otimes$ is the Kronecker product of matrices.

If H_{N_1} and H_{N_2} are Hadamard matrices of orders N_1 and N_2 respectively, then the Kronecker product $H_{N_1} \otimes H_{N_2}$ is easily shown to be a Hadamard matrix of order N_1N_2.

Definition 3. The Kronecker product of two matrices $A_{m\times n}$ and $B_{p\times q}$ is defined as the matrix $C_{mp\times nq} = A_{m\times n} \otimes B_{p\times q}$, and is given by

$$C = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & & & \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix} \tag{3}$$

The Kronecker product is also referred to as the direct product or tensor product of matrices.

Since the permutation of the rows and columns of a Hadamard matrix does not affect the definition in Eq. (2), the Hadamard matrices H^1 and H^2 are said to be equivalent if

$$H^2 = P_r^T H^1 P_c \tag{4}$$

where P_r and P_c are permutation matrices for rows and columns, respectively.

It can be shown that the Sylvester-type Hadamard matrices are equivalent to the Hadamard matrices obtained from S matrices through maximal length shift register sequences. The (i, j)th element of the Sylvester-type Hadamard matrix can be obtained as $(-1)^{i,j}$, where i,j is the number of 1's that the binary representation of i and j have in common.

Basis Functions

The application of an orthogonal transformation depends on the basis functions and the algorithms for implementing the transformation. For example, the discrete Fourier transform is used for frequency domain analysis and filtering operation (8), the discrete cosine transform for data compression (9), the slant transformation for image coding (10), and the Hadamard and Haar transform for dyadic-invariant signal processing (11,12). The inner product of the input signal with the basis functions of the transform represents a measure of similarity between the input signal and its corresponding basis function. Figure 1 shows the basis function of the Hadamard transform of length $N = 16$.

Walsh Functions

Walsh functions are rectangular waveforms orthonormal on the interval [0, 1). They form a complete orthonormal set over this interval and can be expressed as products of Rademacher functions (13). Figure 2 shows the orthogonal waveforms of a Walsh function of order $N = 8$. Uniform sampling of the Walsh functions results in the Hadamard (or Walsh–Hadamard) matrices of corresponding order (14).

Higher-Dimensional Hadamard Matrices

Reference 15 proposes a method for construction of higher-dimensional Hadamard matrices. An N-dimensional Hadamard matrix $[h_{ijk\ldots n}]$ is a matrix with elements ± 1 such that

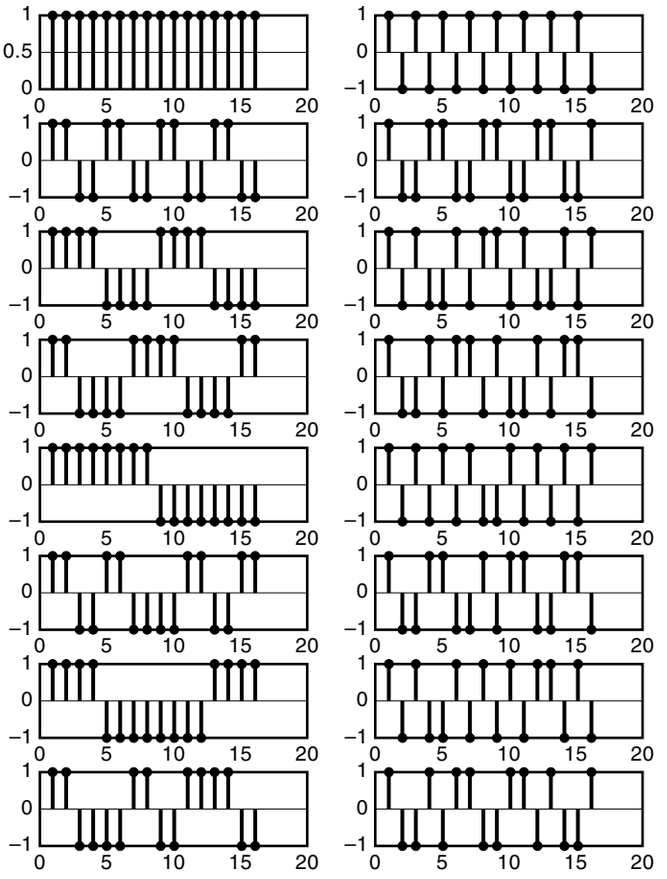

Figure 1. Hadamard basis functions ($N = 16$).

$$\sum_p \sum_q \sum_r \cdots \sum_y h_{pqr\ldots ya} h_{pqr\ldots yb} = m^{(N-1)} \delta_{ab}$$

where m is the order of the matrix. A 3-dimensional Hadamard matrix is one in which all parallel 2-dimensional layers in all normal axes are orthogonal. An N-dimensional Hadamard matrix is called proper if any 2-dimensional layer of the matrix is a 2-dimensional Hadamard matrix. These higher dimensional Hadamard matrices may find applications in error correction codes where their hierarchy of orthogonalities permit a variety of checking procedures. They might also be used in security codes based on their similarity to random binary matrices.

There is no general theory for the construction of high-dimensional Hadamard matrices of any order as there is for 2-dimensional Hadamard matrices. But 3-dimensional matrices of order 2^t can be generated from $t - 1$ successive direct (Kronecker) products of 3-dimensional Hadamard matrices of order 2.

Hadamard Transformation

Consider an N-dimensional source column vector $\boldsymbol{X}$. The Hadamard transform (HT) $\boldsymbol{Y}$ is given by

$$\boldsymbol{Y} = H_N \boldsymbol{X}$$

where H_N is the Hadamard matrix of order $N = 2^n$. Since $H_N H_N^T = NI$, where I is an $N \times N$ identify matrix,

$$H_N^{-1} = \frac{1}{N} H_N^T = H_N$$

where the superscript T denotes the matrix transpose. From definition, the determinant $|H_N|$ of the Hadamard matrix is $|H_N| = \pm N^{N/2}$. By rearranging the rows of the Hadamard matrix, we can obtain the Walsh (or sequency ordered) matrix, the Hadamard (or naturally ordered) matrix, and the Paley (or dyadically ordered) matrix. In the Walsh matrix, the rows of the Hadamard matrix are ordered according to their sequencies. The kth row of the Hadamard matrix is the jth row of the Walsh matrix, where j is the Gray code to binary conversion of k after it has been bit reversed. By premultiplying the naturally ordered Hadamard matrix with the bit-reversed order matrix, we obtain the Paley (or dyadically ordered) transform matrix.

Two-Dimensional Hadamard Transform. The 2-dimensional Hadamard transform (HT) of an array $[X(m, n)]$ of size $N \times N$ is defined as

$$[Y(u, v)] = [H_N(u, v)][X(m, n)][H_N(u, v)] \tag{5}$$

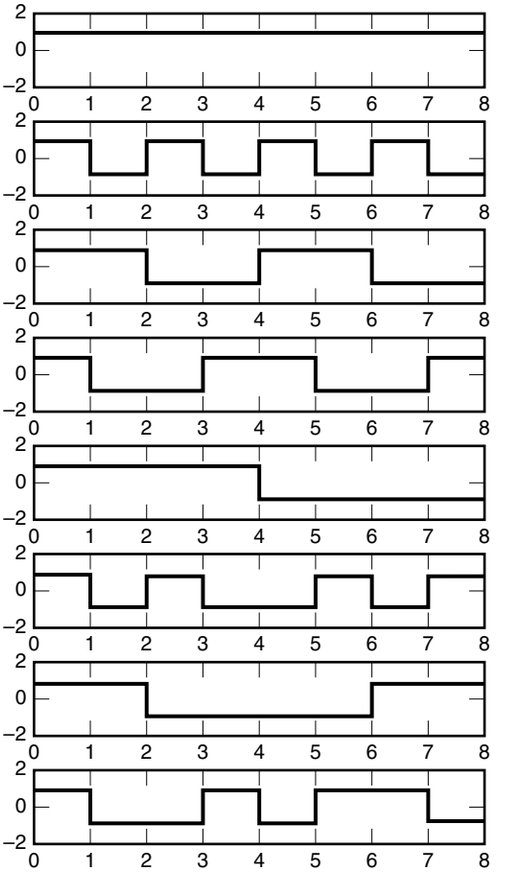

Figure 2. Walsh functions used to construct Hadamard basis ($N = 8$).

where $H_N = [H_N(u, v)]$ is a Hadamard transform of order $N = 2^n$. Pre- and postmultiplying the transformed array $[Y(u, v)]$ by the Hadamard matrix $[H_N(u, v)]$ gives

$$[X(m,n)] = \frac{1}{N^2}[H_N(u,v)][Y(u,v)][H_N(u,v)]$$

The coefficients of the 2-dimensional Hadamard transform of a matrix can be considered as the orthogonal projection of the matrix onto a set of 2-dimensional basis functions. Each transformed coefficient represents a measure of similarity between the input matrix and the corresponding basis function. The 2-dimensional basis functions of the Hadamard transform are shown in Fig. 3.

Fast Algorithms and Implementation

In Ref. 16 an efficient method is proposed to calculate the discrete Fourier transform (DFT) and Walsh–Hadamard transform (WHT) of a vector, one from the other, using a transformation matrix T between Fourier and Hadamard transformations. The method is based on the factorization of the transform matrix T into sparse matrices.

The Least Mean Square (LMS) algorithm for calculation of the forward and inverse orthogonal transformations is described in Ref. 17. Although this method requires twice as much computation as simply using the transform matrix directly, it is useful for parallel computation applications and for VLSI implementations (18).

Reference 19 proposes an algorithm of a simple systolic array processor for the Hadamard transform. It is based on the Hadamard Coefficient Generator (HCG). The HCG makes the signs of the Hadamard matrix elements required to execute the matrix multiplication.

By using the recursive structure of the Sylvester-type Hadamard matrices, efficient algorithms can be developed for Hadamard transformation (20). In general it can easily be shown that the number of 2-point Hadamard transforms required to implement an N-point Hadamard transform is $N/2 \log_2 N$, which is equivalent to $N \log_2 N$ multiply/add operations. By writing

$$\begin{aligned} H_N &= H_2 \otimes H_{N/2} = H_2 \otimes H_2 \otimes H_{N/4} \\ &= H_4 \otimes H_{N/4} \end{aligned}$$

an algorithm to compute an H_4 with only seven multiply/add operations was described in (20). The number of multiply/add operations for computing an N-point Hadamard transform can be reduced to $\frac{7}{8}N \log_2 N$, when N is an even power of 2, and $\frac{7}{8}N \log_2 N + N/8$, when N is an odd power of 2.

In Ref. 21 a fast algorithm was developed for the sequency-ordered form of the Hadamard transform. The machine architecture obtained for this algorithm is similar to the one derived for the machine-oriented algorithm of the fast Fourier transform (FFT) by Corinthios (22), except that the multipliers are deleted, the add/subtract operator sequencing varies from one iteration to another, and the ideal shuffling is performed before each iteration. The algorithms for the Hadamard transform in its natural order and dyadic order were also derived. It was shown that all three algorithms can be performed with a single machine structure by including a simple binary controller.

The 2-dimensional Hadamard transform, together with a selected set of basis functions and fast computational algorithms, may be used to encode 2-dimensional images. As shown later, the Hadamard matrix with ± 1 entries lacks dynamic range for good image representation at the decoder. On the other hand, the discrete cosine transform (DCT) with cosinusoidal entries provides greater dynamic range and hence better image representation at the decoder. However, the computational complexity of the DCT is very high compared to the Hadamard transform. Nevertheless, the salient features of the HT and DCT may be combined to yield an acceptable performance-complexity tradeoff, as described in the next section.

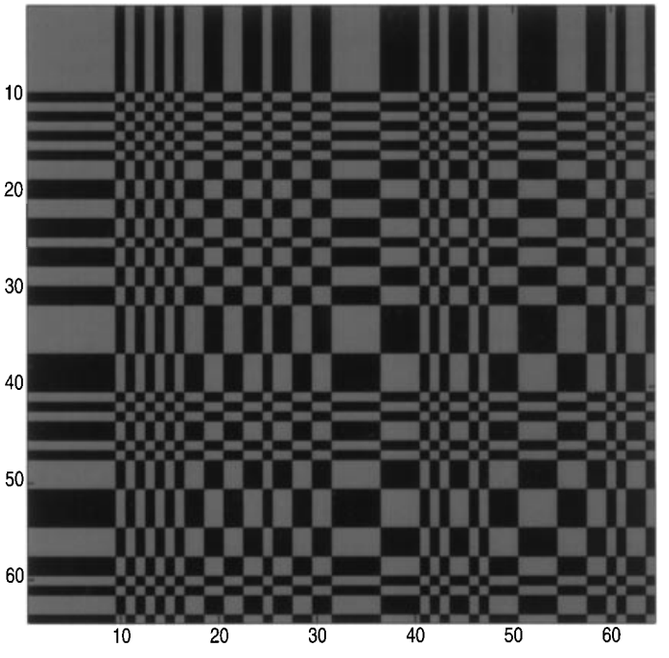

Figure 3. Two-dimensional Hadamard basis functions ($N = 8$).

THE MODIFIED HADAMARD-STRUCTURED DCT (MHDCT)

The salient features of a good image scheme are: (1) good reproduction quality, (2) high compression ratio, and (3) fast computation. The DCT, which forms an integral part of the JPEG and MPEG standards, satisfies the first two features, but is computationally complex. The entries of the DCT matrix are cosine functions, so that all arithmetic operations, such as multiplications and additions, have to be performed in the real domain. On the other hand, the entries of the Hadamard matrix are ± 1, so that arithmetic operations are much simpler. The excellent performance of DCT is attributable to the fact that the transform coefficients are uncorrelated in DCT, but not in HT. Thus, the use of HT for image coding does not yield sufficiently good representation quality. As a performance-complexity tradeoff, it may be feasible to combine the good features of DCT and HT. This was the approach taken in Ref. 23 in the construction of the Hadamard-structured DCT (HDCT). The effectiveness of HDCT as an image coding scheme depends to a large degree on the choice of basis functions.

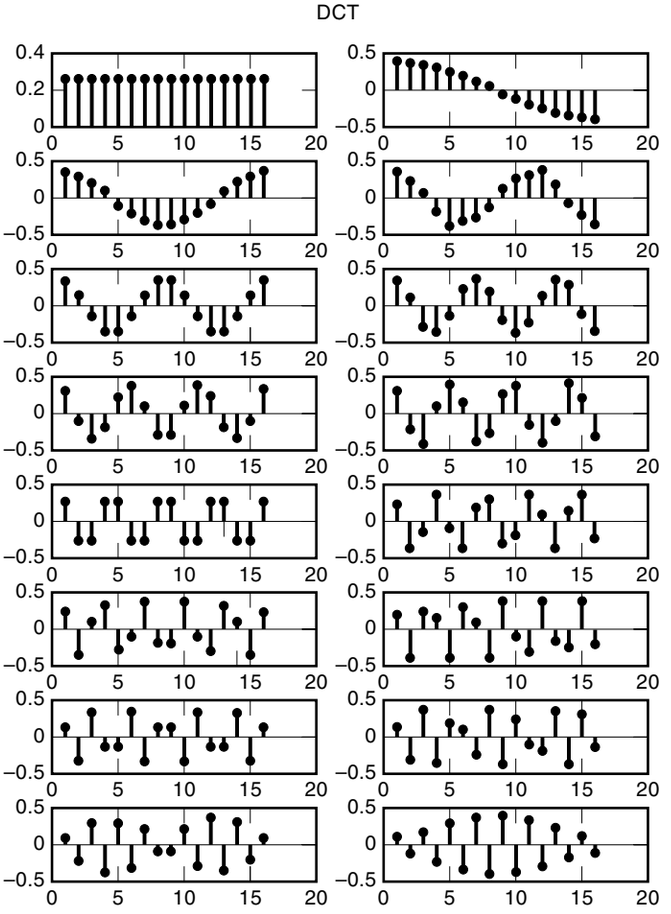

Figure 4. DCT basis vectors ($N = 16$).

Kou and Mark (23) have proposed an HDCT for speech coding. The basis functions used in Ref. 23 lack symmetry to be efficient for image coding. The modified HDCT (MHDCT) presented in Ref. 24 has basis vectors with symmetric and antisymmetric properties suitable for image coding. Examples of the basis vectors for $N = 16$ for DCT and MHDCT are shown in Figs. 4 and 5, respectively. It is noted that the basis vectors of DCT and MHDCT exhibit even and odd symmetry.

The MHDCT transformation matrix of order N is defined by the following recursive structure:

$$T_1 = [1]$$

$$T_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

and

$$T_{2^k} = \frac{1}{\sqrt{2}}\begin{bmatrix} T_{2^{k-1}} & T_{2^{k-1}} \\ C_{2^{k-1}} & -C_{2^{k-1}} \end{bmatrix} \quad \text{for} \quad k = 2, 3, 4, \ldots \tag{6}$$

where C_{2^k} is $2^k \times 2^k$ normalized DCT matrix with mnth entry given by

$$c_{mn} = \eta_n \cos\frac{(2m+1)\,n\pi}{2N} \quad \text{for} \quad m, n = 0, 1, \ldots, N-1 \tag{7}$$

where

$$\eta_n = \begin{cases} \dfrac{1}{\sqrt{N}}, & n = 0 \\ \sqrt{\dfrac{2}{N}}, & n \neq 0 \end{cases}$$

Thus the MHDCT matrix has a mixture of ± 1 and cosine entries as opposed to all cosine entries in DCT.

The sequency of a basis vector is defined as the number of sign changes. Figures 4 and 5 show the basis vectors of DCT and MHDCT, respectively. It is observed that the basis functions of MHDCT take all possible sequencies from 0 to 15. Like the DCT, the MHDCT is an orthogonal transformation, that is, $T_N^{-1} = T_N^t$. Hence we have the transform pair between a source vector $\boldsymbol{X}$ and the transform vector $\boldsymbol{Y}$:

$$\boldsymbol{Y} = T_N \boldsymbol{X} \tag{8}$$

and

$$\boldsymbol{X} = T_N^t \boldsymbol{Y} \tag{9}$$

The MHDCT has the property that the lower order transformation matrix can be obtained from the higher order ones using the following theorem.

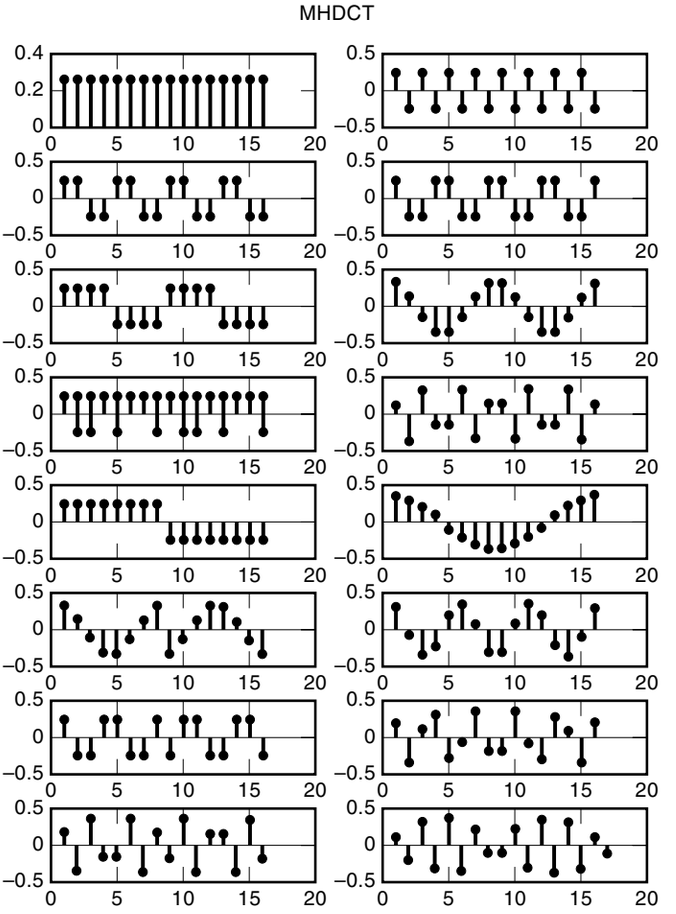

Figure 5. MHDCT basis vectors ($N = 16$).

Theorem 2. *For $k \geq 3$, T_{2^k} can be expressed as*

$$T_{2^k} = \frac{1}{\sqrt{2^k}}\left[C_2 \oplus \sum_{i=1}^{k-1} C_{2^i}\right]\left[\prod_{i=1}^{k-1}\left((H_2 \otimes I_{2^{k-i}}) \oplus I_{2^k - 2^{k-i+1}}\right)\right] \tag{10}$$

where $\otimes$ is a Kronecker product operation and $\sum$ or $\oplus$ is a direct sum operation.

Proof. Let H^2 be a 2×2 Hadamard matrix. From the definition of MHDCT and the recursion, Eq. (6), for $k \geq 2$ we have

$$\begin{aligned} T_{2^k} &= \frac{1}{\sqrt{2}}\begin{bmatrix} T_{2^{k-1}} & T_{2^{k-1}} \\ C_{2^{k-1}} & -C_{2^{k-1}} \end{bmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix} T_{2^{k-1}} & 0 \\ 0 & C_{2^{k-1}} \end{bmatrix} \cdot \begin{bmatrix} I_{2^{k-1}} & I_{2^{k-1}} \\ I_{2^{k-1}} & -I_{2^{k-1}} \end{bmatrix} \\ &= \frac{1}{\sqrt{2}}\left[T_{2^{k-1}} \oplus C_{2^{k-1}}\right]\left[H_2 \otimes I_{2^{k-1}}\right] \end{aligned} \tag{11}$$

$T_{2^{k-1}}$ in the first term on the right-hand side of Eq. (11) can further be expanded as

$$T_{2^{k-1}} = \frac{1}{\sqrt{2}}\left[(T_{2^{k-2}} \oplus C_{2^{k-2}})(H_2 \otimes I_{2^{k-2}})\right] \tag{12}$$

Substituting Eq. (12) in Eq. (11) yields

$$T_{2^k} = \frac{1}{\sqrt{2}}\left[(T_{2^{k-2}} \oplus C_{2^{k-2}})(H_2 \otimes I_{2^{k-2}}) \oplus C_{2^{k-1}}\right]\left[H_2 \otimes I_{2^{k-1}}\right] \tag{13}$$

By using the matrix operation (25),

$$AD \oplus B = (A \oplus B)(D \oplus I) \tag{14}$$

in Eq. (13), we get

$$T_{2^k} = \frac{1}{\sqrt{2^2}}\left[T_{2^{k-2}} \oplus C_{2^{k-2}} \oplus C_{2^{k-1}}\right]\left[H_2 \otimes I_{2^{k-2}} \oplus I_{2^k - 2^{k-1}}\right] \cdot \left[H_2 \otimes I_{2^{k-1}}\right] \tag{15}$$

As in Eq. (12), we can expand $T_{2^{k-2}}$ as

$$T_{2^{k-2}} = \frac{1}{\sqrt{2}}\left[T_{2^{k-3}} \oplus C_{2^{k-3}}\right]\left[H_2 \otimes I_{2^{k-3}}\right] \tag{16}$$

Substituting $T_{2^{k-2}}$ from Eq. (16) into Eq. (15) yields

$$T_{2^k} = \frac{1}{\sqrt{2^3}}\left[(T_{2^{k-3}} \oplus C_{2^{k-3}})(H_2 \otimes I_{2^{k-3}}) \oplus C_{2^{k-2}} \oplus C_{2^{k-1}}\right] \left[H_2 \otimes I_{2^{k-2}} \oplus I_{2^k - 2^{k-1}}\right] \cdot \left[H_2 \otimes I_{2^{k-1}}\right] \tag{17}$$

Again by using the matrix operation Eq. (14) and Eq. (17) we get

$$T_{2^k} = \frac{1}{\sqrt{2^3}}\left[T_{2^{k-3}} \oplus C_{2^{k-3}} \oplus C_{2^{k-2}} \oplus C_{2^{k-1}}\right] \cdot \left[H_2 \otimes I_{2^{k-3}} \oplus I_{2^k - 2^{k-2}})\right]\left[H_2 \otimes I_{2^{k-2}} \oplus I_{2^k - 2^{k-1}}\right] \cdot \left[H_2 \otimes I_{2^{k-1}}\right] \tag{18}$$

As we continue this iterative procedure and recognize that $T_2 = C_2$, Theorem 2 follows.

Fast MHDCT Algorithm

Theorem 2 also offers a way to implement the MHDCT. In this algorithm, the input signal is hierarchically Hadamard transformed and then the result is DCT transformed using different sizes. The structure of this algorithm for $N = 8$ is given in Fig. 6. It consists of a 2-stage Hadamard structured transform followed by a windowed discrete-cosine transform.

Complexity of the MHDCT

As with the transform methods, the complexity of the MHDCT is defined as the number of multiplications and additions (or subtraction) required to implement the transformation. Let $A_{DCT}(2^i)$ and $M_{DCT}(2^i)$ denote the number of additions and multiplications of a 2^i-point DCT transform, respectively. Then by using Theorem 2, the number of additions and multiplications for a 2^k-dimensional fast MHDCT, $A_{MHDCT}(2^k)$ and $M_{MHDCT}(2^k)$, will be

$$A_{MHDCT}(2^k) = \sum_{i=1}^{k-1} 2 \times 2^{k-1} + A_{DCT}(2) + \sum_{j=1}^{k-1} A_{DCT}(2^j) \tag{19}$$

and

$$M_{MHDCT}(2^k) = M_{DCT}(2) + \sum_{j=1}^{k-1} M_{DCT}(2^j) \tag{20}$$

The total number of multiplications and additions depends on the DCT algorithm used in the MHDCT implementation. Tables 1 and 2 compare the complexity of MHDCT with DCT using the algorithms of Chen et al. (26) and Lee (27).

The results in Tables 1 and 2 show clearly the computational saving of the MHDCT over the DCT. The number of additions and multiplications required to implement MHDCT are remarkably less than those required for DCT. However, this computational saving is only one factor, and we shall compare the performance of MHDCT with those of other transformations.

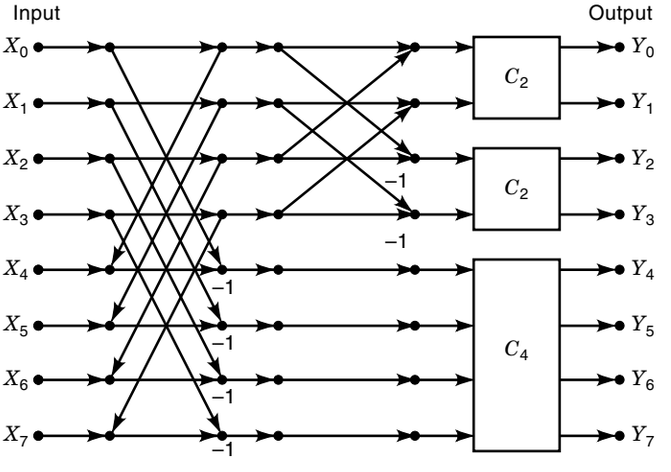

Figure 6. A block diagram for fast computation of MHDCT for $N = 8$.

Table 1. Comparison of Complexity Between DCT and MHDCT (Using Chen's Algorithm)

	Additions		Multiplications	
N	DCT	MHDCT	DCT	MHDCT
8	26	24	16	10
16	74	66	44	26
32	194	172	116	70
64	482	430	292	186
128	1154	1040	708	478
256	2690	2450	1668	1186
512	6146	5652	3844	2854
1024	13826	12822	8708	6698

In the following subsections, different measures are used to evaluate the performance of different transformations and use them to compare the performance of MHDCT with HT and DCT.

Decorrelation Efficiency and Coding Performance

In the previous section we showed that the MHDCT is computationally simpler than the DCT. Now we will compare the performance of MHDCT with those of HT and DCT in terms of decorrelation efficiency and transformation gain. The decorrelation efficiency provides a basis for comparing different orthogonal transforms against each other. With regard to transformation gain, pulse code modulation (PCM) is used as a benchmark for comparing the performance of different coding techniques.

Decorrelation Efficiency. This section presents simulation results of the decorrelation efficiency η_c of the DCT, HT, and MHDCT transforms.

Let R_X and R_Y be the correlation matrix of the source and transformed processes, respectively. Let

$$\lambda_x = \sum_{i=0}^{N-1} \sum_{\substack{j=1 \\ i \neq j}}^{N-1} |R_X(i, j)|$$

and

$$\lambda_y = \sum_{i=0}^{N-1} \sum_{\substack{j=1 \\ i \neq j}}^{N-1} |R_Y(i, j)|$$

Table 2. Comparison of Complexity Between DCT and MHDCT (Using Lee's Algorithm)

	Additions		Multiplications	
N	DCT	MHDCT	DCT	MHDCT
8	29	25	12	8
16	81	70	32	20
32	209	183	80	52
64	513	456	192	132
128	1217	1097	448	324
256	2817	2570	1024	772
512	6401	5899	2304	1796
1024	14337	13324	5120	4100

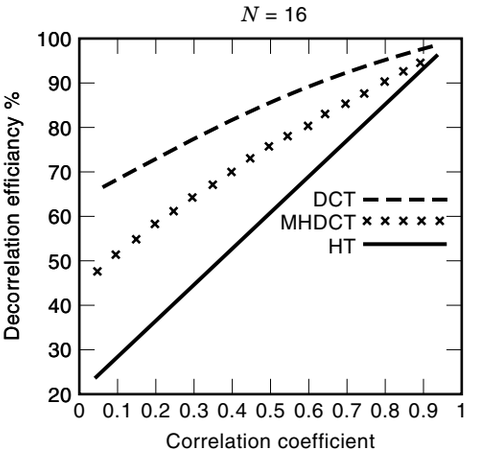

Figure 7. Comparison of the decorrelation efficiency of the HT, MHDCT, and DCT ($N = 16$).

The decorrelation efficiency is defined as

$$\eta_c = 1 - \frac{\lambda_y}{\lambda_x} \tag{21}$$

For completely decorrelated spectral coefficients, $\lambda_y = 0$ and $\eta_c = 1$.

Figures 7 and 8 show the decorrelation efficiency, η_c, of different transforms as a function of the correlation coefficient of the source process, with the transform size as a parameter. It is observed that the performance of MHDCT is between that of HT and DCT, and by increasing the transformation size, the performance of MHDCT approaches that of DCT.

Transformation Gain. The transformation gain G_{TC} of a transform coding (TC) system is defined as the ratio of the measured reconstruction error of PCM to that of the transform coding at the same information bit rate. On the assump-

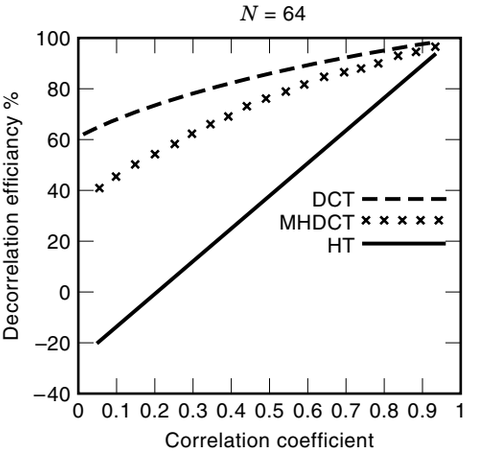

Figure 8. Comparison of the decorrelation efficiency of the HT, MHDCT, and DCT ($N = 64$).

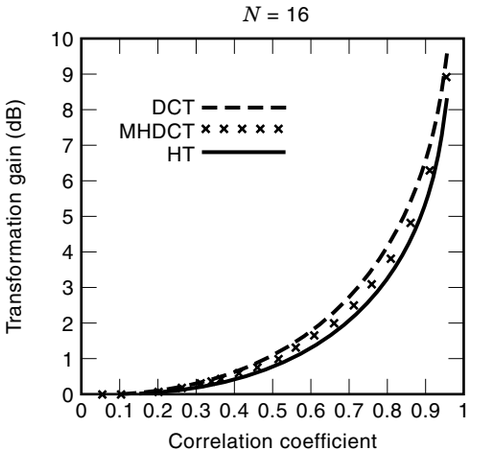

Figure 9. Comparison of the transformation gain of different transforms ($N = 16$).

tion that the error processes have zero mean, G_{TC} is given by

$$G_{TC} = \frac{\sigma_e^2(PCM)}{\sigma_e^2(TC)} = \frac{\frac{1}{N}\sum_{j=0}^{N-1}\sigma_j^2}{\left(\prod_{j=0}^{N-1}\sigma_j^2\right)^{1/N}} \tag{22}$$

Figures 9 and 10 present the transformation gain of DCT, MHDCT, and HT transform codes as a function of the correlation coefficient, for two different transformation size N.

It is observed that the transformation gain of the MHDCT is quite close to that of DCT, and it increases as the transformation size or the correlation coefficient increases.

APPLICATIONS OF HADAMARD MATRICES

Error Correction Coding

Due to the unwanted effects of noise, distortion, and interference, the output of a storage medium or a digital communication channel differs from its input. The theory of error correction coding is concerned with the protection of digital signals against the errors that occur during transmission or storage. In this section a special group of error correcting codes, called Hadamard codes, are discussed. A Hadamard code of rate N/k, where $k = \log_2(2N)$ has a minimum distance of $N/2$. This code is capable of correcting $d_{\min}/2 = N/4$ random errors.

Hadamard Codes. An error correcting code with $2N$ codewords can be constructed from a Hadamard matrix of order N as follows:

1. Change all $+1$'s to 0's and all -1's to 1's.
2. Select each row and its complement of the Hadamard matrix as a codeword.

$$H_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$H_4 = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

The complement of H_4 is

$$\overline{H}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

The rows of H_4 and $\overline{H}_4$ form a linear binary code of block length $N = 4$ having $2N = 8$ codewords. The code is also called a first order Reed-Muller error correcting code, an implementation of which is shown in Fig. 11. The minimum dis-

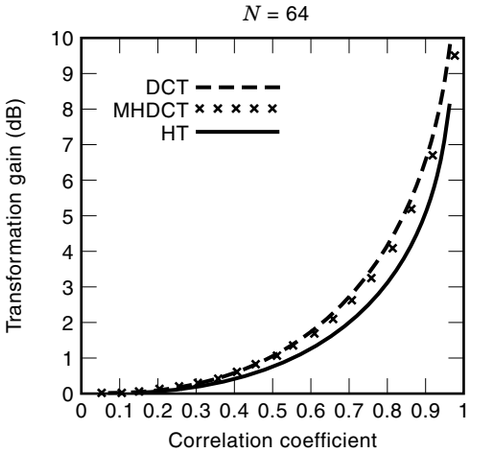

Figure 10. Comparison of the transformation gain of different transforms ($N = 64$).

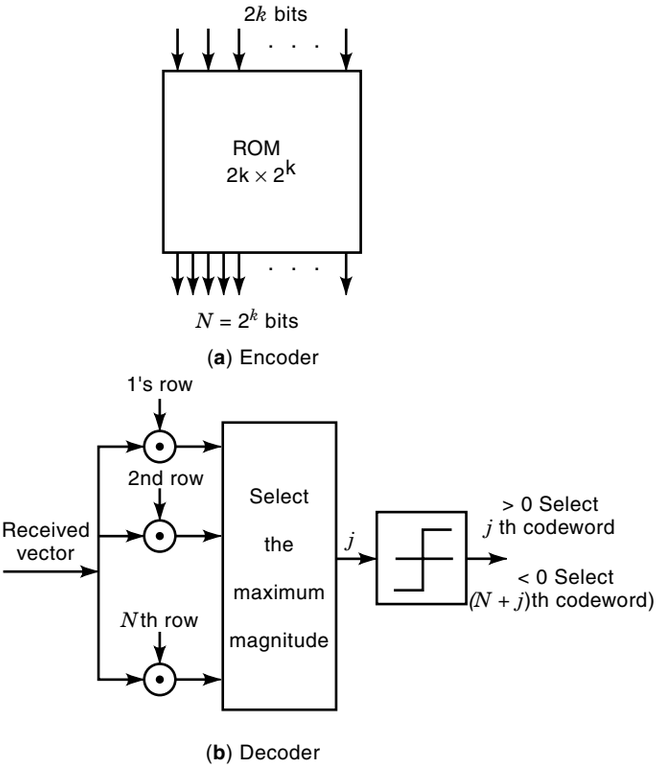

Figure 11. The encoder and decoder of a first-order Reed–Muller code.

tance of the code is

$$d_{\min} = N/2 = 2$$

In general a Hadamard code of size $2N$ codewords is obtained by selecting the N rows and their complement. By selecting $M = 2^k \leq 2N$ of these codewords, we obtain a Hadamard code $H(N, k)$, where each codeword conveys k information bits. The resulting code has constant weight equal to $N/2$ and minimum distance $d_{\min} = N/2$.

Using the above procedure, one can construct a Hadamard error correcting code (n, k, d) with codeword length $N = 2^m$, input block length $k = \log_2 2N = m + 1$, and Hamming distance $d = N/2 = 2^{m-1}$, where m is a positive integer.

The Hadamard error correcting codes with $N = 2^m$ are called *linear*. The *nonlinear* Hadamard codes are those with order $n = p + 1$ for a multiple of 4, and any order $n = p^m + 1$ if the quadratic residues in $GF(p^m)$ are used. They are also called Paley-type Hadamard codes.

Decoding of Hadamard Codes. Hadamard codes are decoded using the following procedure:

1. First, in a transform matrix of order N change all 0's to $+1$'s and all 1's to -1's.
2. Premultiply this transform matrix by the received vector and locate the largest magnitude coefficient of the transformed vector. Assume it is the jth coefficient.
3. If the largest coefficient is positive, decide on the jth codeword; otherwise decide on the $(j + N)$th codeword.

Logical Hadamard Transform and Nonlinear Block Codes. The logical Hadamard transform proposed by Searle (28) is a modification of the arithmetic Hadamard transform for binary inputs. In the logical Hadamard transform, both input and output blocks are binary. The procedure for obtaining the logical Hadamard transform is to take the output of an arithmetic Hadamard transform and threshold each element at zero. The only condition for recovering the input signal is that the first element of the input vector should be 1. Banta (29) has used the logical Hadamard transform to obtain a nonlinear block code with block length $N = 2^n - 1$, data length $K = 2^r - 1$, $r < n - 1$, error correction $t = 2^{n-r} - 1$, and rate $R = K/N \approx 1/t$.

A series of explicit low-rate binary linear block codes which have relatively low covering radius and can be rapidly recoded is described in Ref. 30. These codes can be derived from higher dimensional analogues of the Gale–Berlekamp switching game.

MHDCT as an Image Coding Scheme

The MHDCT can be used to transform 2-dimensional image signals. The image array is divided into blocks of size $N \times N$. Each block is then transformed using the MHDCT and the transform coefficients are adaptively quantized and sent to the receiver (24).

Two-Dimensional MHDCT Transform. Let T_N be the one-dimensional MHDCT transformation matrix that operates independently on the rows and the columns of the 2-dimensional $N \times N$ image block $[X(m, n)]$. Then the 2-dimensional MHDCT transform $[Y(u, v)]$ of the block image $[X(m, n)]$ is defined as

$$[Y(u, v)] = [T_N(u, m)][X(m, n)][T_N(v, n)]^t \tag{23}$$

where T_N is the one-dimensional MHDCT transform defined by Eq. (6). By the orthogonality property of the MHDCT, the inverse transform can be derived as

$$[X(m, n)] = [T_N(u, m)]^t[Y(u, v)][T_N(v, n)] \tag{24}$$

The 2-dimensional transformation of the images can be considered as an orthogonal projection of the image onto the set of basis pictures. The input image can be reconstructed by a linear combination of the basis pictures, with coefficients being the 2-dimensional transform coefficients. The basis pictures of MHDCT and DCT for $N = 8$ are shown in Figs. 12 and 13, respectively. The efficiency of a transformation for encoding a particular image depends on the shape of both the image and the basis pictures. The basis pictures should be able to represent different patterns of pixel intensities within the image.

For a 2-dimensional image, the N^2 values of $X(m, m)$ are the elements of a subimage of size $N \times N$. In image coding, the typical arrays used are of sizes $N = 4$, 8, 16, or 32. This partitioning into subimages is particularly efficient in cases where the correlations are localized to the neighboring pixels, and where the structural details tend to cluster. Partitioning of an image into subimages reduces the complexity of the transformation. The coding method in Ref. 24 uses 8×8 blocks. This block size yields a good tradeoff between complexity and performance of the transformation. By using the Kolmogorov-Smirnov (KS) test (31), the distribution of the ac coefficients of the MHDCT was found to be Laplacian.

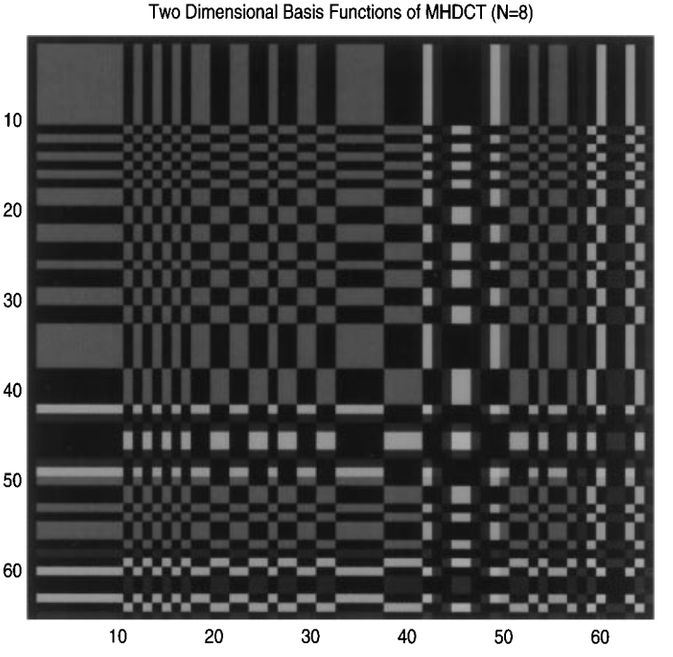

Figure 12. Two-dimensional MHDCT basis pictures ($N = 8$).

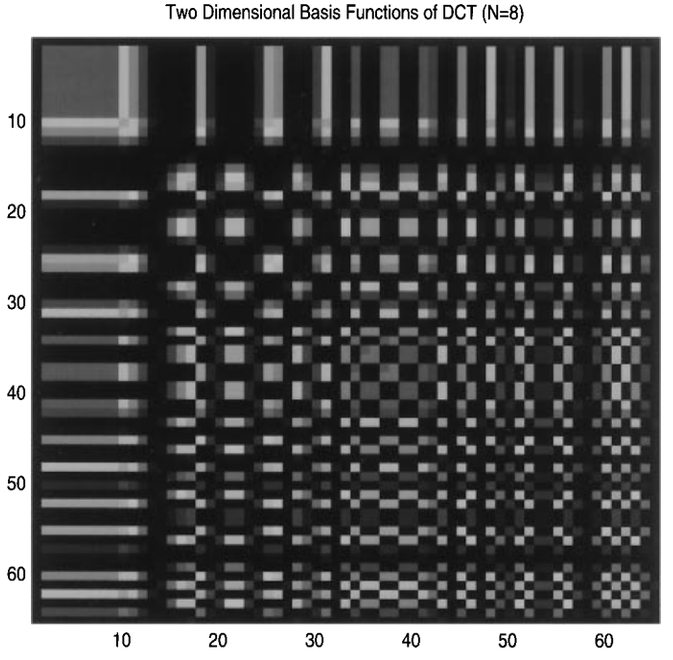

Figure 13. Two-dimensional DCT basis pictures ($N = 8$).

Adaptive MHDCT Transform Coding of Images. The transform coefficients of 8×8 blocks of the images are quantized and transmitted to the receiver through the communication channel. To make efficient use of the available bandwidth with minimum distortion, an adaptive method as in Ref. 32 can be used. The blocks of the image in the transform domain are classified according to their ac energy level. To demonstrate the effectiveness of the coding scheme, choose four classes of blocks, and choose the decision boundaries for the classification such that the number of blocks in each class is the same. The coding of the image is performed on a block-by-block basis. Then the process is made adaptive by assigning more bits to the higher energy blocks. Also, within a block a larger number of bits is allocated to the coefficients in the block with higher variance. The sum of the squared values of ac coefficients in each block of the image in the transform domain is defined as the energy level of the block. The classification map, bit allocation matrices, and the MHDCT coefficients are transmitted to the receiver through the communication channel. In the receiver, image reconstruction is accomplished by inverting the compression operation. Figure 14 shows a block diagram of the adaptive MHDCT coder.

In practice, it is necessary to make two passes on the image data. The first pass generates the subblock classification map and also assigns the bit allocation matrices to different classes. The second pass quantizes the subblock transform coefficients using the bit allocation matrices. We have used the optimal Lloyd-Max (33,34) quantizers designed for Laplacian sources in our coding system. The quantizer can also be designed using the Lloyd-Max algorithm for a suitable training data.

Bit Allocation. A crucial part of transform coding is an efficient bit allocation algorithm that provides the possibility of quantizing some transform coefficients more finely than others. Minimization of the mean-squared reconstruction error can be used as the criterion to derive an optimum bit allocation algorithm. In our case, the bit allocation matrix for each block is constructed after determining the variances of the transform coefficients, as given by

$$N_{B_k}(u,v) = \frac{1}{2}\log_2[\sigma_k^2(u,v)] - \log_2[D] \qquad \forall (u,v) \neq (0,0) \tag{25}$$

where $\sigma_k^2(u, v)$ is the variance of the transform sample and D is a parameter. The value of D is first initialized and then recursively calculated to meet the desired total number of bits.

Experimental Results for Adaptive Encoding of Images. We have used the adaptive MHDCT coding method to compress the 512×512 Lena image with intensity value uniformly quantized to 256 levels (8 bits per pixel). The results of our experiments are summarized in Table 3. The peak signal-to-noise ratio defined in Eq. (26) is used for objective comparison of images.

$$SNR = 10\log_{10}\left(\frac{255^2}{\frac{1}{N^2}\sum_{m=0}^{m=N-1}\sum_{n=0}^{n=N-1}[X(m,n) - \hat{X}(m,n)]^2}\right) \tag{26}$$

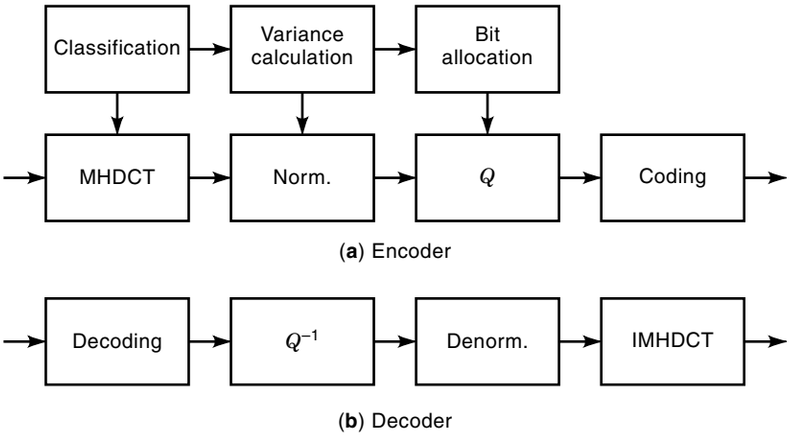

Figure 14. Adaptive MHDCT coding system.

Table 3. Comparison of SNR for Lena Image Using Different Transforms

Bit Rate (bpp)	Hadamard SNR	MHDCT SNR	DCT SNR	Compression Ratio
0.25	28.29	29.08	30.91	32.0
0.50	29.67	30.44	31.77	16.0
0.75	30.81	32.05	32.75	10.6
1	31.91	33.41	33.68	8.0

where the image size is $N \times N$ and $X(m, n)$ and $\hat{X}(m, n)$ are the original and the reconstructed images, respectively.

It is shown that the performance of MHDCT is better than HT and close to that of DCT with less complexity. Figures 15 and 16 provide a visual comparison between the performances of DCT and MHDCT in adaptive coding of the Lena image. The difference in quality of the two pictures is not noticeable. From this figure it is observed that the performance of MHDCT is quite close to the performance of DCT and that the difference in the SNR is very small. No entropy coding has been used in our experiments and using a lossless entropy code will significantly improve the performance of the coding system.

Signal Representation

The Hadamard matrix may be used to design orthogonal and biorthogonal M-ary sequences. To form the signal set, we might use the Hadamard matrix construction. The Hadamard matrix of order 4 is

$$H_4 = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix} = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}$$

These four rows plus their complements form an 8-ary biorthogonal set of linear binary code of block length $N = 4$ having $2N = 8$ codewords. The minimum distance is $d_{\min} = N/2 = 2$. The selected row can be sent as a rectangular pulse train of duration

$$T_s = T_b \log_2 M = 3T_b \quad (M = 8)$$

where T_b is the bit duration.

The Hadamard matrix of order 8 is constructed as

$$H_8 = \begin{bmatrix} H_4 & H_4 \\ H_4 & -H_4 \end{bmatrix} = \begin{bmatrix} +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 \\ +1 & +1 & +1 & +1 & -1 & -1 & -1 & -1 \\ +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\ +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 \end{bmatrix}$$

The eight rows can be used as the signal patterns for the 8-ary orthogonal set. The minimum distance of the code is $d_{\min} = N/2$. The first element of each row is a $+1$, which means that this signal element yields no distinguishing feature to the signal set. Therefore this signal element can be dropped with no loss in performance to lower the entropy per bit to $\frac{7}{8}$ of the former value, while maintaining $d_{\min}$ fixed and thus achieving the same error probability. Although the rows of the Hadamard matrices are mutually orthogonal, for spectral purposes, these are not good for random binary sequences.

Figure 15. MHDCT coding of Lena image, compression ratio = 8.10.

Figure 16. DCT coding of Lena image, compression ratio = 8.10.

Feature Extractions and Pattern Recognition. Features such as shape, motion, pressure details and timing, and transformation methods such as Fourier and Hadamard have been used in handwritten signature recognition with various degrees of success. In Ref. 35 a fast Fourier transform is used to transform normalized signatures into the frequency domain. Fifteen harmonics having the largest magnitude normalized by their corresponding variances were selected and used in a stepwise discriminant analysis.

An approach to the problem of signature verification is described in Ref. 36. This paper considers the signature as a 2-dimensional image and uses the Hadamard transformation as a means of data reduction and feature extraction. The signature image is a 2-dimensional array of 1's and 0's corresponding to light and dark areas on the original image. This method achieves 91% of correct recognition, 11% valid signature rejection, and 41% forgery acceptance.

For handwriter identification, feature extraction was performed by decomposition of the quantized pressure pattern into a set of orthogonal functions. In view of the rectangular nature of the time domain waveforms, Hadamard transform is a logical natural choice (37).

In Ref. 38 the Hadamard transform was used to design a vector classifier for a Predictive Classified Vector Quantizer (PCVQ). The performance of Hadamard transform vector classifier was compared to a spatial vector classifier. The good performance of the Hadamard transform classifier is the unique property of the Hadamard transform, which groups the frequency components within the image vector into distinct coefficients.

The Hadamard transform is used in Ref. 39 to represent image signals in the transformed domain. Compared to the Fourier transform, the Hadamard transform offers an order of magnitude speed increase. Transmitting the Hadamard transform coefficients of an image instead of the spatial representation of the image provides a potential tolerance to channel errors and the possibility of reduced bandwidth requirement. Linear and Gaussian-optimized quantizers are used to quantize the Hadamard transform coefficients. Results with the linear quantizer are poor because of the large quantization errors at high sequences (equivalent to frequencies in Fourier transform).

The coding efficiency of the differential PCM (DPCM) with a 2-dimensional predictor is compared to that of a 2-dimensional Hadamard transform code (HTC) in intrafield coding of the NTSC composite signal in Ref. 40. It is shown that the coding efficiency of the HTC is far lower than that of the DPCM in the case of a signal having high-power level carrier chrominance signal, such as a color-bar signal. In general it was shown that

1. For signals with large values of horizontal and vertical correlation ratios (close to 1), DPCM outperforms HTC, while for smaller values of correlation ratio, the performance of HTC is much better.
2. In the case of high compression ratio (2 bit/pel), HTC shows higher coding efficiency than DPCM.

Special Purpose HT Applications

Spread Spectrum. The basic idea in spread spectrum is to distribute a relatively low-dimensional data signal into a higher dimensional signal. A jammer with finite energy has to either distribute its energy on all dimensions, thereby inducing a small interference on each dimension or put its total energy on a small subspace leaving the remainder of the space interference free. In the time domain, the distribution of the signal is achieved by multiplying the data signal by a member of an orthogonal set.

Orthogonal sequences can be used as spreading signals in spread-spectrum multiple-access systems. They have zero correlation when they are time synchronized. But in some applications, like multipath fading environments, multiple delays introduce nonzero cross correlation between the otherwise orthogonal signals. One solution to this can be concatenation of a (pseudo-noise) PN sequence with the orthogonal coding to increase the randomness of the orthogonal sequences.

Orthogonal coding was used to spread the information signal in Ref. 41. Each signal is coded with the same orthogonal or biorthogonal code, followed by a modulo-2 addition of a unique signature sequence. With block orthogonal coding, $\log_2 N$ information bits are encoded into an N-bit codeword. An N-bit signature sequence is then modulo-2 added to the codeword before transmission. Thus, orthogonal coding provides the spreading of the information signal, not the signature sequence. From the coding point of view, each signal is assigned a code set, or coset, which is formed by modulo-2 adding the signature sequence to each of N (orthogonal) or $2N$ (bi-orthogonal) codes. Thus the system employs a supercode consisting of codes of orthogonal codes.

A wideband, direct-sequence, code-division multiple access (CDMA) was proposed in Ref. 42. The wideband CDMA system uses PN and Walsh–Hadamard codes for spreading the signal in order to achieve the minimal interference between traffic and control (pilot, sync, and paging) channels. The spreading is done by a combination code, which is generated by PN and orthogonal codes from Walsh–Hadamard sequences to minimize mutual interference between traffic and control signals.

Reference 43 proposes an optimal set of signature sequences for use in a CDMA system where orthogonal or biorthogonal Walsh—Hadamard coding is used to spread the signal. This paper shows that in the special case of a synchronous system with no multipath echoes and use of WH code as the spreading sequence, the product of any two different signature sequences should be a bent sequence of length $N = 2^n$. A sequence with a constant magnitude WH transform is called a bent sequence.

Filter Design in the Hadamard Transform Domain. Adaptive filters have many applications in interference cancellation, linear prediction, spectral estimation, system modeling, and channel equalization in communication systems. The filter parameters can be computed in the time or transform domain. Because of some computational efficiencies observed in the transform domain (44), this subsection discusses the application of Hadamard transform for filter design.

Reference 45 proposes a fast implementation of the LMS error adaptive transversal filter. The fast Walsh–Hadamard transform (FWHT) technique is adopted in this implementation. The error vector is obtained by subtracting the WH transform of the desired output and the filter output. The input vector is also WH transformed before entering the filter. Finally, the output of the filter is inverse WH transformed to obtain the representation in the time domain. This filter provides a significant reduction in computation over both the conventional time domain and the frequency domain adaptive filters. For data blocks of size of N, the proposed filter only requires $2N$ adaptations compared to those of $2N^2$ and $2N + 3N/2 \log_2 N$ for time domain and FFT filters, respectively.

A block implementation of 2-dimensional finite-impulse response (FIR) digital filters using the matrix decomposition approach is described in Ref. 46. The coefficient matrix of the

block realization is decomposed via the Walsh–Hadamard transform without involving any intermediate calculations.

The application of the recursive Walsh–Hadamard transformation to FIR and infinite impulse response (IIR) filtering was investigated in Ref. 47. It was shown that by using a common recursive transform, the usual frequency domain FIR filtering problem was converted into a Walsh sequence-domain filtering problem. A hardware implementation of the filter was also proposed.

Equalizers. Equalizers are used to mitigate the effect of intersymbol interference (ISI) in transmission of digital signals through band-limited communication channels. Different algorithms in the time domain, including the symbol rate linear transversal filter equalizer and the fractionally spaced equilizer (FSE), are proposed for equalizer design. To achieve rapid convergence of the equalizer coefficients, the equalizers are designed in the frequency domain.

Reference 48 considers adaptive equalization for digital data transmitted over discrete linear channels exhibiting intersymbol interference in addition to additive noise. LMS equalization is developed in the discrete sequence (Walsh or Hadamard) domain using a gradient projection method. An adaptive LMS adaptation algorithm in the Hadamard domain is developed, in which the input data sequence is divided into blocks. Each block is Hadamard transformed, passed through an LMS equalizer, and then converted into the time domain again. The performance of time domain and Hadamard transformed domain are comparable, but the latter provides a much faster convergence.

A technique for implementing an echo canceller for full-duplex data transmission was presented in Ref. 49. This article considers the effect of nonlinear distortion in the echo path or in the echo replica. The Hadamard transform was used to add or delete some taps in the equalizer design.

Spectroscopy. Spectroscopy is a branch of physics that studies the production and measurement of the spectra. Conventional spectrometers sort the electromagnetic radiation into rays of different wavelengths and measure the intensity of each ray separately. Hadamard transform optics is a technique in spectroscopy that measures the spectrum of a beam of light using multiplexing. The basic idea is that instead of measuring the intensity of each wavelength separately, the spectral components are multiplexed and the total intensity of each group is measured. This reduces the measurement noise and results in a more accurate measurement of the spectra. Hadamard transform is used for the multiplexing. The same technique can be used for imagers in reconstructing an image or picture.

The basic Hadamard transform instrument consists of an optical separator, an encoding mask, a detector, and a processor. The separator may be a lens that produces a focused image at the mask or a prism that spears different frequency components of the beam and focuses them at different locations on the mask. Different parts of the mask pass the light to the detector, or absorb it or refect it towards a reference detector. If we record the difference between readings of the main detector and the reference detector, the intensity of this element of the beam is multiplied by $+1$, 0, or -1, respectively. Sometimes masks are only made up of two types of elements, open and closed slots that pass or obstruct the light when the reference detector is removed. The best mask for minimizing the measurement error is the Hadamard mask for the first configuration and the S-matrix mask for the second one (50).

Encryption. Hadamard transform was used in Ref. 51 to encrypt analog speech signals. In the analog speech encryption, speech samples are first converted into a transform domain like DCT, DFT, or discrete Hadamard transform (DHT). The encryption is achieved by permuting the transform coefficients. The encrypted transform samples are then converted back into the time domain and transmitted. The application of the analog speech encryption is in both narrowband and wideband systems (speech transmission over a bandlimited telephone channel and speech storage and retrieval). As a comparison for using different transforms, the DCT, DFT, and (Discrete Prolate Spherical transform) DPST can be used in narrowband systems. The KLT (Karhunen–Loeve transform) and DHT are more suitable for wideband systems. Based on subjective and objective measures (such as LPC, cepstral, SNR distance measures), DCT turned out to be the best transform with respect to both residual intelligibility of the encrypted speech and the recovered speech quality. The DFT produced results that are inferior to the DCT. The DCT implementation would also offer speed advantages over FFT.

ACKNOWLEDGMENTS

This work was supported by the Natural Sciences and Engineering Research Council of Canada under Grant No. A7779.

BIBLIOGRAPHY

1. J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign-succesions, and tesselated properties in two or more colors with application to Newton's rule, ornamental tile-work and the theory of numbers, *Philos. Magazine,* **Series 4**: 461–475, 1967.
2. J. Sylvester, *Mathematical Recreation and Essays,* New York: Macmillan, 1947, pp. 108–111.
3. J. Hadamard, Resolution d'une question relative aux determinants, *Bull. Sci. Math. (2),* **17**: I, 240–246, 1893.
4. M. Vitterli, Tree structure for orthogonal transforms and application to the Hadamard transform, *Sig. Proc.,* **5**: 473–484, 1983.
5. S. G. Wilson and M. Lakshman, Autocorrelation and power spectrum of Hadamard signalling, *Proc. IEEE,* **135** (3): 258–261, 1968.
6. E. R. Berlekamp, *Algebric Coding Theory,* New York: McGraw-Hill, 1968.
7. F. J. MacWillimas and N. J. A. Sloane, *The Theory of Error Correcting Codes,* Amsterdam, The Netherlands: North-Holland, 1977.
8. A. V. Oppenheim and R. W. Schaffer, *Digital Signal Processing,* Englewood Cliffs, NJ: Prentice-Hall, 1975.
9. N. S. Jayant and P. Knoll, *Digital Coding of Waveforms,* Englewood Cliffs, NJ: Prentice-Hall, 1984.
10. W. K. Pratt, W. H. Chen, and L. R. Welch, Slant transform image coding, *IEEE Trans. Commun.,* **22**: 1075–1093, 1974.
11. K. G. Beauchamp, *Applications of Walsh and Related Functions,* New York: Academic Press, 1984.

12. J. Pearl, Optimal dyadic methods of time-invariant systems, *IEEE Trans. Comput.,* **24**: 598–603, 1975.
13. D. F. Elliot and K. R. Rao, *Fast Transforms; Algorithms, Analysis, Applications,* New York: Academic Press, 1982, p. 301.
14. J. L. Walsh, A closed set of orthogonal functions, *Amer. J. Math.,* **55**: 5–24, 1923.
15. P. J. Shlichta, Higher dimensional Hadamard matrices, *IEEE Trans. Inf. Theory,* **25**: 566–572, 1979.
16. S. Boussakta and A. Holt, Fast algorithms for calculation of both Walsh–Hadamard and Fourier transforms, *Electron. Lett.,* **25**: 1352–1354, 1989.
17. S. S. Wang, LMS algorithm and discrete orthogonal transforms, *IEEE Trans. Circuits Syst.,* **38**: 949–951, 1991.
18. B. Widrow et al., Fundamental relations between the LMS algorithm and the DFT, *IEEE Trans. Circuits Syst.,* **34**: 614–820, 1987.
19. M. H. Lee and Y. Yasuda, Simple systolic array algorithm for Hadamard transform, *Electron. Lett.,* **26**: 1478–1480, 1990.
20. D. Coppersmith, E. Feig, and E. Linzer, Hadamard transforms on multiply/add transforms, *IEEE Trans. Sig. Process.,* **42**: 969–970, 1994.
21. Y. A. Geaddah and M. J. G. Corinthios, Natural dyadic and sequency-order algorithms and processors for the Walsh–Hadamard transform, *IEEE Trans. Comput.,* **C-26**: 435–442, 1977.
22. M. J. Corinthios, A time-series analyzer, *Proc. Symp. Comput. Process. Commun.,* April 8–10, 1969, pp. 47–60.
23. W. Kou and J. W. Mark, A new look at DCT transform, *IEEE Trans. Acoust. Speech Signal Process.,* **37**: 1899–1907, 1989.
24. M. Barazande-Pour and J. W. Mark, Adaptive MHDCT coding of images, *Proc. 1994 1st Int. Conf. Image Process.,* 1994, pp. 90–94.
25. R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis,* New York: Cambridge University Press, 1991.
26. W. H. Chen, C. Smith, and S. C. Fralick, A fast computational algorithm for the discrete cosine transform, *IEEE Trans. Commun.,* **COM-25**: 1004–1009, 1977.
27. B. G. Lee, A new algorithm to compute the discrete cosine transform, *IEEE Trans. Acoust. Speech Signal Process.,* **ASSP-32**: 1243–1245, 1984.
28. N. H. Searle, A logical Walsh-Fourier transform, *n Applications of Walsh functions, 1970 Proc.-Symp. Workshop,* Naval Research Laboratory, Washington, DC, 1970, pp. 95–98.
29. E. D. Banta, A class of nonlinear block codes using the logical Hadamard transform to achieve virtually identical encoding and decoding, *IEEE Trans. Inf. Theory,* **24**: 761–763, 1978.
30. J. Pach and J. Spencer, Explicit codes with low covering radius, *IEEE Trans. Inf. Theory,* **34** (5): 1281–1285, 1988.
31. S. D. Silvey, *Statistical Inference,* London: Chapman Hall, 1975.
32. Wen-Hsiun Chen and C. H. Smith, Adaptive coding of monochrome and color images, *IEEE Trans. Commun.,* **COM-25**: 1285–1292, 1977.
33. J. Max, Quantizing for minimum distortion, *IEEE Trans. Inf. Theory,* **6**: 7–12, 1960.
34. S. P. Lloyd, Least squares quantization in PCM, *IEEE Trans. Inf. Theory,* **IT-28**: 127–135, 1982.
35. C. F. Lam and D. Kamins, Signature recognition through spectral analysis, *Pattern Recognition,* **22**: 39–44, 1989.
36. W. F. Nemeck and W. C. Lin, Experimental investigation of automatic signature verification, *IEEE Trans. Syst. Man Cybern.,* **4**: 121–126, 1974.
37. K. P. Zimmerman and M. J. Varady, Handwriter identification from one bit quantized pressure patterns, *Pattern Recognition,* **18**: 63–72, 1985.
38. K. N. Ngan and H. C. Koh, Predictive classified vector quantization, *IEEE Trans. Image Process.,* **1**: 269–280, 1992.
39. W. K. Pratt, J. Kane, and H. C. Andrews, Hadamard transform image coding, *Proc. IEEE,* **57**: 58–68, 1969.
40. H. Murakaami, Y. Yatori, and H. Yamamoto, Comparison between DPCM and Hadamard transform coding in the composite coding of the NTSC color TV signal, *IEEE Trans. Commun.,* **30**: 469–479, 1982.
41. G. E. Bottomley, Signature sequence selection in a CDMA system with orthogonal coding, *IEEE Trans. Veh. Technol.,* **42**: 62–68, 1993.
42. F. Atsushi et al., Wideband CDMA system for personal communication systems, *IEEE Commun. Mag.,* **34**: 116–123, 1996.
43. P. K. Enge and D. V. Sarwate, Spread spectrum multiple access performance of orthogonal codes: linear receivers, *IEEE Trans. Commun.,* **COM-35**: 1309–1318, 1987.
44. M. Dentino, J. McCool, and B. Widrow, Adaptive filtering in the frequency domain, *Proc. IEEE,* **66**: 1658–1659, 1978.
45. R. N. Boules, Adaptive filtering using the fast Walsh–Hadamard transformation, *IEEE Trans. Electromagn. Compat.,* **31**: 125–128, 1989.
46. B. Mertzios and A. Venetsanopoulos, Fast block implementation of 2-dimensional FIR digital filters via the Walsh–Hadamard decomposition, *Int. J. Electron.,* **68**: 991–1004, 1990.
47. G. Peceli and B. Feher, Digital filters based on recursive Walsh–Hadamard transformation, *IEEE Trans. Circuits Syst.,* **37**: 150–152, 1990.
48. M. Maqusi and O. Natour, Adaptive equalization in the discrete-time discrete frequency and Hadamard domains, *Int. J. Electron.,* **72**: 197–212, 1992.
49. O. Agazzi, D. G. Messerschmitt, and D. A. Hodges, Nonlinear echo cancellation of data signals, *IEEE Trans. Commun.,* **30**: 2421–2433, 1982.
50. M. Harwit and N. J. A. Sloane, *Hadamard Transform Optics,* New York: Academic Press, 1979.
51. S. Sridharan, E. Dawson, and B. Goldburg, Speech encryption in the transform domain, *Electron. Lett.,* **26**: 655–657, 1990.

JON W. MARK
M. BARAZANDE-POUR
University of Waterloo