Fast Binary Block Inverse Jacket Transform

Moon Ho Lee[1] · Xiao-Dong Zhang[1,2] · Subash Shree Pokhrel[1] · Chang-hui Choe[3] · Gi-Yean Hwang[1]

Abstract

A block Jacket transform and its block inverse Jacket transform have recently been reported in the paper "Fast block inverse Jacket transform". But the multiplication of the block Jacket transform and the corresponding block inverse Jacket transform is not equal to the identity transform, which does not conform to the mathematical rule. In this paper, new binary block Jacket transforms and the corresponding binary block inverse Jacket transforms of orders $N=2^k$, $3^k$and 5^k for integer values k are proposed and the mathematical proofs are also presented. With the aid of the Kronecker product of the lower order Jacket matrix and the identity matrix, the fast algorithms for realizing these transforms are obtained. Due to the simple inverse, fast algorithm and prime based p^k order of proposed binary block inverse Jacket transform, it can be applied in communications such as space time block code design, signal processing, LDPC coding and information theory. Application of circular permutation matrix(CPM) binary low density quasi block Jacket matrix is also introduced in this paper which is useful in coding theory.

Key words : Block Algorithms, Binary Block Inverse Jacket Transform, Fast Algorithms, Kronecker Product, Sparse Matrix Factorization, Low Density Matrix.

Ⅰ. Introduction

Discrete orthogonal transform[2]~[4] have highly practical value for representing signals and images, especially for propose of data compression, for Walsh-Hadamard orthogonal sequence generator in code division multiple access(CDMA), coded modulation and spread spectrum communication[6]~[9]. Specially, Walsh-Hadamard transform is an orthogonal matrix with highly practical values for signal sequence transforms and data processing[2]~[4],[20]. Jacket matrices[10],[13],[18], which are motivated by the center weighted Hadamard matrices[5],[11],[12], is class of matrices with their inverse being determined by the element-wise of the matrix. Mathematically, let $A=(a_{kt})$ be a matrix, if, $A^{-1}=(a_{kt}^{-1})^T$, then the matrix A is a Jacket matrix, where T denotes the transpose and (·) denotes a matrix. Since the inverse of the Jacket matrix can be calculated easily, it is very helpful to employ this kind of matrix in the signal processing[15],[16], encoding[14], mobile communication[7],[8],[18],[19], sequence design[21], cryptography[22],[23] and orthogonal code design[25]. Especially, the interesting matrices, such as Hadamard, DFT matrices, belong to the Jacket matrix family[24]. In addition, the Jacket matrices are associated with many kind of matrices, such as unitary matrices and Hermitian matrices which are very important in communication (e.g., encoding), mathematics and physics.

Recently, Lee and Hou in [1] proposed one dimensional and two dimensional fast algorithms for block inverse Jacket transforms. Their block inverse Jacket transform is, in some sense, not real inverse Jacket transform from mathematical point of view, since their inverse does not satisfy the usual condition, i.e., the multiplication of a matrix with its inverse matrix is not equal to the identity matrix. For example, the equation's (4) and (5) in [1] can be stated as follows:

$$[J]_2=\left(\begin{array}{cc|cc}1&0&1&0\\0&1&0&1\\\hline 1&0&0&1\\0&1&1&0\end{array}\right),\quad [J]_2^{-1}=\left(\begin{array}{cc|cc}1&0&1&0\\0&1&0&1\\\hline 1&0&0&1\\0&1&1&0\end{array}\right)$$

over Galois field GF (2). It is easy to see that

$$[J]_2[J]_2^{-1}=\left(\begin{array}{cc|cc}1&0&1&0\\0&1&0&1\\\hline 1&0&0&1\\0&1&1&0\end{array}\right)\left(\begin{array}{cc|cc}1&0&1&0\\0&1&0&1\\\hline 1&0&0&1\\0&1&1&0\end{array}\right)$$
$$=\left(\begin{array}{cc|cc}0&0&1&1\\0&0&1&1\\\hline 1&1&0&0\\1&1&0&0\end{array}\right)\neq[I]_4$$

It is nature to seek better block Jacket transform and the corresponding block inverse transform which can overcome the problem arising in [1].

Manuscript received November 16, 2006 ; revised December 20, 2006. (ID No. 20061116-032J)
[1]Institute of Information and Communication, Chonbuk National University, Chonbuk, Korea.
[2]Department of Mathematics, Shanghai Jiao Tong University, Shanghai, China.
[3]Department of Information Security, Chonbuk National University, Chonbuk, Korea.

This paper is organized as follows: in section Ⅱ, we present a binary block Jacket and corresponding block inverse transform of order 2^k. Section Ⅲ presents the binary block inverse Jacket transform of orders $N=3^k$ and 5^k for integer value k. Section Ⅳ presents the two dimensional fast algorithms for binary block Jacket transform. In section Ⅴ, application of binary low density quasi block Jacket matrices are introduced. Finally, some conclusions are drawn in section Ⅵ.

Ⅱ. Binary Block Jacket Transform of Order 2^k

An $m\times m$ binary matrix $[B]_m$ over Galois field $GF(2)$, which has only two elements 0 and 1, is called a binary Jacket matrix if $[B]_m$ is invertible $[B]_m^{-1}=[B]^T$, *i.e.*, $[B]_m[B]_m^{-1}=[B]_m[B]^T=[I]_m$ where T is the transpose of the matrix $[B]_m$ and $[I]_m$ is the identity matrix. For example,

$$[B]_2=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ [B]_2[B]_2^T=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=[I]_2. \tag{1}$$

Hence $[B]_2^{-1}=[B]_2^T$ is a binary Jacket matrix. Generally, we may define binary block Jacket matrix as follows:

Definition 2.1 Let

$$[B]_m=\begin{pmatrix}B_{11}&B_{12}&\cdots&B_{1m}\\B_{21}&B_{22}&\cdots&B_{2m}\\\cdots&\cdots&\cdots&\cdots\\B_{m1}&B_{m2}&\cdots&B_{mm}\end{pmatrix}$$

and

$$[B]_m^T\triangleq\begin{pmatrix}B_{11}&B_{21}&\cdots&B_{m1}\\B_{12}&B_{22}&\cdots&B_{m2}\\\cdots&\cdots&\cdots&\cdots\\B_{1m}&B_{2m}&\cdots&B_{mm}\end{pmatrix}. \tag{2}$$

be an $m\times m$ block matrix and the transpose of block matrix B, where B_{ij} is a $k\times k$ matrix for all $i, j=1,\cdots,m$. B is called a binary block Jacket matrix, if $[B]_m^{-1}=[B]_m^T$, *i.e*,

$$[B]_m^{-1}=[B]_m^T, i.e,\ [B]_m[B]_m^T=[B]_m[B]_m^{-1}=[I]_m, \tag{3}$$

where $[I]_m$ is the block identity matrix whose each block is of $k\times k$ order. It is easily checked that if each block is 1×1 then binary block Jacket matrix is coincident with binary Jacket matrix. For example, let

$$\alpha=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \beta=\begin{pmatrix}1&1\\1&1\end{pmatrix}. \tag{4}$$

By a simple calculation, we have $\alpha\alpha+\beta\beta=[I]_2$ and $\alpha\beta+\beta\alpha=0=0$. Hence

$$\begin{pmatrix}\alpha&\beta\\\beta&\alpha\end{pmatrix}\begin{pmatrix}\alpha&\beta\\\beta&\alpha\end{pmatrix}^T=\begin{pmatrix}\alpha\alpha+\beta\beta&\alpha\beta+\beta\alpha\\\alpha\beta+\beta\alpha&\alpha\alpha+\beta\beta\end{pmatrix}=\begin{pmatrix}[I_2]&0\\0&[I_2]\end{pmatrix} \tag{5}$$

Therefore,

$$\begin{pmatrix}\alpha&\beta\\\beta&\alpha\end{pmatrix}^{-1}=\begin{pmatrix}\alpha&\beta\\\beta&\alpha\end{pmatrix}^T=\begin{pmatrix}\alpha&\beta\\\beta&\alpha\end{pmatrix}. \tag{6}$$

Thus,

$$[J]_2=\begin{pmatrix}\alpha&\beta\\\beta&\alpha\end{pmatrix}=\left(\begin{array}{cc|cc}1&0&1&1\\0&1&1&1\\\hline 1&1&1&0\\1&1&0&1\end{array}\right), \tag{7}$$

$$[J]_2^{-1}=\begin{pmatrix}\alpha&\beta\\\beta&\alpha\end{pmatrix}=\left(\begin{array}{cc|cc}1&0&1&1\\0&1&1&1\\\hline 1&1&1&0\\1&1&0&1\end{array}\right), \tag{8}$$

and

$$[J]_2[J]_2^{-1}=[I]_2=\left(\begin{array}{cc|cc}1&0&0&0\\0&1&0&0\\\hline 0&0&1&0\\0&0&0&1\end{array}\right). \tag{9}$$

Hence, 2×2 the binary block matrix is a binary block Jacket matrix $[J]_2$. Next, we introduce the block Kronecker product of two block matrices. For two $m\times m$ block matrices,

$$A=\begin{pmatrix}A_{11}&A_{12}&\cdots&A_{1m}\\A_{21}&A_{22}&\cdots&A_{2m}\\\cdots&\cdots&\cdots&\cdots\\A_{m1}&A_{m2}&\cdots&A_{mm}\end{pmatrix},$$

$$B\triangleq\begin{pmatrix}B_{11}&B_{12}&\cdots&B_{1m}\\B_{21}&B_{22}&\cdots&B_{2m}\\\cdots&\cdots&\cdots&\cdots\\B_{m1}&B_{m2}&\cdots&B_{mm}\end{pmatrix}, \tag{10}$$

where, A_{ij} and B_{ij} are $k\times k$ matrices. The block Kronecker product of A and B[2],[17] is defined to be

$$A\otimes B\equiv\begin{pmatrix}A_{11}*B&A_{12}*B&\cdots&A_{1m}*B\\A_{21}*B&A_{22}*B&\cdots&A_{2m}*B\\\cdots&\cdots&\cdots&\cdots\\A_{m1}*B&A_{m2}*B&\cdots&A_{mm}*B\end{pmatrix}, \tag{11}$$

where

$$A_{ij}*B\equiv\begin{pmatrix}A_{ij}B_{11}&A_{ij}B_{12}&\cdots&A_{ij}B_{1m}\\A_{ij}B_{21}&A_{ij}B_{22}&\cdots&A_{ij}B_{2m}\\\cdots&\cdots&\cdots&\cdots\\A_{ij}B_{m1}&A_{ij}B_{m2}&\cdots&A_{ij}B_{mm}\end{pmatrix}, \tag{12}$$

If each block A_{ij} and B_{ij} of A and respectively is 1×1, then the block Kronecker product of two block matrices is coincident with the conventional Kronecker product of two matrices. For example, from (7),

$$[J]_2 \otimes [J]_2 = \begin{pmatrix} \alpha^2 & \alpha\beta & \beta\alpha & \beta^2 \\ \alpha\beta & \alpha^2 & \beta^2 & \beta\alpha \\ \beta\alpha & \beta^2 & \alpha^2 & \alpha\beta \\ \beta^2 & \beta\alpha & \alpha\beta & \alpha^2 \end{pmatrix}. \tag{13}$$

From now, throughout this paper, we only consider that each block in each block matrix is a 2×2 submatrix. We introduce binary block Jacket transform and binary block inverse Jacket transform. Let $[J]_m$ be a binary block Jacket matrix, for the one dimensional binary Jacket transform, we can transform a temporal or spatial vector x into a transform vector y by

$$y = [J]_m x. \tag{14}$$

and binary block inverse Jacket transforms of y is

$$x = [J]_m^{-1} y = [J]_m^T y. \tag{15}$$

A block permutation matrix $[P]_N=(p_{kl})$ is defined as for $1\le k$, $1\le N$,

$$p_{kl} = \begin{cases} [I]_2 & if\ l \equiv k+1 \pmod N \\ 0 & otherwise \end{cases}, \tag{16}$$

where $[I]_2$ is the 2×2 identity matrix. The block permutation matrices P^h are referred to circulant permutation matrices. Moreover, it is easy to see that $\{I, P, \cdots, P^{N-1}\}$ forms an Abelian group with tradition multiplication which is corresponding to the group of all complex N-roots of unity with tradition multiplication. For example, if N=2,

$$[P]_2^0 = \begin{pmatrix} [I]_2 & 0 \\ 0 & [I]_2 \end{pmatrix},\ [P]_2 = \begin{pmatrix} 0 & [I]_2 \\ [I]_2 & 0 \end{pmatrix}. \tag{17}$$

If N=3,

$$[P]_3^0 = \begin{pmatrix} [I]_2 & 0 & 0 \\ 0 & [I]_2 & 0 \\ 0 & 0 & [I]_2 \end{pmatrix},$$
$$[P]_3 = \begin{pmatrix} 0 & [I]_2 & 0 \\ 0 & 0 & [I]_2 \\ [I]_2 & 0 & 0 \end{pmatrix},$$
$$[P]_3^2 = \begin{pmatrix} 0 & 0 & [I]_2 \\ [I]_2 & 0 & 0 \\ 0 & [I]_2 & 0 \end{pmatrix}. \tag{18}$$

$[J]_2$ in [9] may be regarded to the smallest order binary block Jacket transform. Moreover, $[J]_2$ is a circulant block matrix, since it can be written to be

$$[J]_2 = \alpha * [I]_2 + \beta * [P]_2 = \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}. \tag{19}$$

The larger order binary block Jacket matrices can be generated by the following recursive relation:

$$[J]_N = [J]_{N/2} \otimes [J]_2, \quad N \ge 4. \tag{20}$$

Since by (13) and definition of transpose of block matrices, we have

$$[J]_4^T = ([J]_2 \otimes [J]_2)^T = [J]_2^T \otimes [J]_2^T. \tag{21}$$

Then

$$\begin{aligned} [J]_4[J]_4^T &= ([J]_2 \otimes [J]_2)([J]_2^T \otimes [J]_2^T) \\ &= ([J]_2[J]_2^T) \otimes ([J]_2[J]_2^T) \\ &= [I]_2 \otimes [I]_2 = [I]_4. \end{aligned} \tag{22}$$

Therefore, $[J]_4[J]_4^{-1} = [J]_4[J]_4^T = [I]_4$ and $[J]_4$ is a 4×4 binary block Jacket matrix. Generally, we can prove that $[J]_{2^k}$ is a $2^k\times2^k$ binary block Jacket matrix for k is positive integer. In fact,

$$\begin{aligned} [J]_{2^k}[J]_{2^k}^T &= ([J]_{2^{k-1}} \otimes [J]_2)([J]_{2^{k-1}} \otimes [J]_2)^T \\ &= ([J]_{2^{k-1}} \otimes [J]_2)([J]_{2^{k-1}}^T \otimes [J]_2^T) \\ &= ([J]_{2^{k-1}}[J]_{2^{k-1}}^T) \otimes ([J]_2[J]_2^T) \\ &= [I]_{2^{k-1}} \otimes [I]_2 = [I]_{2^k}, \end{aligned} \tag{23}$$

So, $[J]_{2^k}^{-1}[J]_{2^k}^T$ and $[J]_{2^k}[J]_{2^k}^{-1} = [J]_{2^k}[J]_{2^k}^{-T} = [I]_{2^k}$. As to fast algorithms of binary block Jacket transforms may be based on the factorization of binary block Jacket matrices. For the 4×4 binary Jacket matrix, $[J]_4$ can be decomposed to the product of two sparse matrices,

$$\begin{aligned} [J]_4 &= [J]_2 \otimes [J]_2 \\ &= ([J]_2 \otimes [I]_2)([I]_2 \otimes [J]_2) \\ &= \begin{pmatrix} \alpha & 0 & \beta & 0 \\ 0 & \alpha & 0 & \beta \\ \beta & 0 & \alpha & 0 \\ 0 & \beta & 0 & \alpha \end{pmatrix} \begin{pmatrix} \alpha & \beta & 0 & 0 \\ \beta & \alpha & 0 & 0 \\ 0 & 0 & \alpha & \beta \\ 0 & 0 & \beta & \alpha \end{pmatrix}. \end{aligned} \tag{24}$$

Further, from (20) and (24), we can derive a general formula for construction of order $N=2^k$, k=1,2$\cdots$, binary block Jacket matrices as

$$\begin{aligned} [J]_{2^k} &= ([J]_{2^{k-1}} \otimes [J]_2) \\ &= ([J]_{2^{k-1}} \otimes [I]_2)([I]_{2^{k-1}} \otimes [J]_2) \\ &= (([J]_{2^{k-2}} \otimes [J]_2) \otimes [I]_2)([I]_{2^{k-1}} \otimes [J]_2) \\ &= ([J]_{2^{k-2}} \otimes ([J]_2 \otimes [I]_2))([I]_{2^{k-1}} \otimes [J]_2) \\ &= ([J]_{2^{k-2}} \otimes [I]_{2^2})([I]_{2^{k-2}} \otimes ([J]_2 \otimes [I]_2))([I]_{2^{k-1}} \otimes [J]_2) \\ &= \prod_{i=0}^{k-1} ([I]_{2^{k-i-1}} \otimes [J]_2 \otimes [I]_{2^i}) \end{aligned} \tag{25}$$

The factor graph corresponding to (25) is similar to the graph in [1] and omitted.

Ⅲ. Binary Block Inverse Jacket Transform of Orders 3^k and 5^k

In this section, binary block Jacket transform(BJT) and binary block inverse Jacket transform with orders 3^k and 5^k are proposed respectively.

From the equations (18) and (12), the smallest order 3×3 binary block Jacket transform may be written as

$$[J]_3 = \alpha_0 [P]_3^0 + \alpha_1 [P]_3 + \alpha_2 [P]_3^2, \tag{26}$$

One can obtain the definition of block Jacket matrices,

$$\begin{aligned}[J]_3[J]_3^T &= \left(\alpha_0[P]_3^0 + \alpha_1[P]_3 + \alpha_2[P]_3^2\right) \\ &\times\left(\alpha_0[P]_3^0 + \alpha_1[P]_3 + \alpha_2[P]_3^2\right)^T \\ &= \left(\alpha_0\alpha_0^T + \alpha_1\alpha_1^T + \alpha_2\alpha_2^T\right)[P]_3^0 + \\ &\quad \left(\alpha_0\alpha_2^T + \alpha_1\alpha_0^T + \alpha_2\alpha_1^T\right)[P]_3 + \\ &\quad \left(\alpha_0\alpha_1^T + \alpha_1\alpha_2^T + \alpha_2\alpha_0^T\right)[P]_3^2 \\ &= [I]_3 \end{aligned} \tag{27}$$

if satisfy the following conditions,

$$\begin{aligned}&\left(\alpha_0\alpha_0^T + \alpha_1\alpha_1^T + \alpha_2\alpha_2^T\right) = I_2 \\ &\left(\alpha_0\alpha_2^T + \alpha_1\alpha_0^T + \alpha_2\alpha_1^T\right) = 0 \\ &\left(\alpha_0\alpha_1^T + \alpha_1\alpha_2^T + \alpha_2\alpha_0^T\right) = 0,\end{aligned} \tag{28}$$

For example, let

$$\alpha_0 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},\ \alpha_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ \alpha_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \tag{29}$$

be three 2×2 binary matrices over $GF(2)$ which satisfy the above conditions. Hence $[J]_3[J]_3^{-1} = [J]_3[J]_3^T = [I]_3$. In a similar way, the smallest order 3 binary block Jacket matrix can be written as the following form

$$[J]_3 = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_0 & \alpha_1 \\ \alpha_1 & \alpha_2 & \alpha_0 \end{pmatrix} = \left(\begin{array}{cc|cc|cc} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \tag{30}$$

which is also a circulant binary block Jacket matrix. Using Kronecker product of block Jacket matrices, the larger order 3^k binary block Jacket transform may be governed by the following recursive relation, i.e.,

$$[J]_N = [J]_{N/3} \otimes [J]_3, \quad N \ge 9, \tag{31}$$

where $N=3^k$ for $k=1,2\cdots$. By similar method, it can be proved that $[J]_{3^k}$ is a binary block Jacket transforms of order 3^k. Further, we can also derive a fast algorithm based on factorization of binary block Jacket matrices,

$$[J]_{3^k} = \prod_{i=0}^{k-1}\left([I]_{3^{k-1-i}} \otimes [J]_3 \otimes [I]_{3^i}\right) \tag{32}$$

For example, the binary block matrix of order 9 based on $[J]_3$ may be expressed to

$$[J]_3 \otimes [J]_3 = \left([J]_3 \otimes [I]_3\right)\left([I]_3 \otimes [J]_3\right). \tag{33}$$

The factor graph corresponding to (33) is similar to Fig. 1 in [1]. Now, we next consider how to construct the order 5^k binary block Jacket transform. The smallest order 5 binary blocks Jacket transform can be defined as follows:

$$[J]_5 = \left(\beta_0[P]_5^0 + \beta_1[P]_5 + \beta_2[P]_5^2 + \beta_3[P]_5^3 + \beta_4[P]_5^4\right) \tag{34}$$

where $[P]_5^0$ is 5×5 the block identity matrix and others $[P]_5$ are the 5×5 block permutation matrices. So we can get,

$$\begin{aligned}[J]_5[J]_5^T &= \left(\beta_0[P]_5^0 + \beta_1[P]_5 + \beta_2[P]_5^2 + \beta_3[P]_5^3 + \beta_4[P]_5^4\right) \\ &\times\left(\beta_0[P]_5^0 + \beta_1[P]_5 + \beta_2[P]_5^2 + \beta_3[P]_5^3 + \beta_4[P]_5^4\right)^T \\ &= \left(\beta_0\beta_0^T + \beta_1\beta_1^T + \beta_2\beta_2^T + \beta_3\beta_3^T + \beta_4\beta_4^T\right)[P]_5^0 + \\ &\quad \left(\beta_0\beta_4^T + \beta_1\beta_0^T + \beta_2\beta_1^T + \beta_3\beta_2^T + \beta_4\beta_3^T\right)[P]_5 + \\ &\quad \left(\beta_0\beta_3^T + \beta_1\beta_4^T + \beta_2\beta_0^T + \beta_3\beta_1^T + \beta_4\beta_2^T\right)[P]_5^2 + \\ &\quad \left(\beta_0\beta_2^T + \beta_1\beta_3^T + \beta_2\beta_4^T + \beta_3\beta_0^T + \beta_4\beta_1^T\right)[P]_5^3 + \\ &\quad \left(\beta_0\beta_1^T + \beta_1\beta_2^T + \beta_2\beta_3^T + \beta_3\beta_4^T + \beta_4\beta_0^T\right)[P]_5^4 = [I]_5\end{aligned} \tag{35}$$

if satisfy the following conditions

$$\begin{aligned}&\left(\beta_0\beta_0^T + \beta_1\beta_1^T + \beta_2\beta_2^T + \beta_3\beta_3^T + \beta_4\beta_4^T\right) = I_2 \\ &\beta_0\beta_4^T + \beta_1\beta_0^T + \beta_2\beta_1^T + \beta_3\beta_2^T + \beta_4\beta_3^T = 0 \\ &\beta_0\beta_3^T + \beta_1\beta_4^T + \beta_2\beta_0^T + \beta_3\beta_1^T + \beta_4\beta_2^T = 0 \\ &\beta_0\beta_2^T + \beta_1\beta_3^T + \beta_2\beta_4^T + \beta_3\beta_0^T + \beta_4\beta_1^T = 0 \\ &\beta_0\beta_1^T + \beta_1\beta_2^T + \beta_2\beta_3^T + \beta_3\beta_4^T + \beta_4\beta_0^T = 0\end{aligned} \tag{36}$$

For example, let

$$\begin{aligned}&\beta_0 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \beta_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \beta_2 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \\ &\beta_3 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \beta_4 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.\end{aligned} \tag{37}$$

be five 2×2 binary matrices over $GF(2)$ which satisfy the above conditions. Hence $[J]_5[J]_5^{-1} = [J]_5[J]_5^T = [I]_5$ and the order 5 binary block Jacket transform can be written as

$$[J]_5 = \begin{pmatrix} \beta_0 & \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \beta_4 & \beta_0 & \beta_1 & \beta_2 & \beta_3 \\ \beta_3 & \beta_4 & \beta_0 & \beta_1 & \beta_2 \\ \beta_2 & \beta_3 & \beta_4 & \beta_0 & \beta_1 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_0 \end{pmatrix}$$

$$= \left(\begin{array}{cc|cc|cc|cc|cc} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ \hline 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right) \quad (38)$$

Clearly, $[J]_5$ is also circulant binary block Jacket matrix. Using the Kronecker product of two matrices, we can generate higher order binary block Jacket transform, i.e.,

$$[J]_{5^k} = [J]_{5^{k-1}} \otimes [J]_5, \quad \text{for } k = 1,2,\ldots \quad (39)$$

The fast algorithm for order 5^k binary block Jacket matrix can derive similar fashion as (32).

$$[J]_{5^k} = \prod_{i=0}^{k-1} \left([I]_{5^{k-1-i}} \otimes [J]_5 \otimes [I]_{5^i}\right) \quad (40)$$

where $[I]_{5^0} = 1$. Further, it is easy for us to construct orders 6, 10, 15, 25, etc. binary block Jacket matrices.

Similarly as in equations (25), (32), and (40), we can derive the order p^k fast binary block Jacket transform, where p is the prime number.

If the matrix of order -6, then the binary block Jacket transform can be written as $[J]_6 = ([J]_2 \otimes [J]_3)$. The block Jacket matrix of order $[J]_6$ will be,

$$[J]_6 = ([J]_2 \otimes [I]_3)([I]_2 \otimes [J]_3) \quad (41)$$

Further, with the aid of recursive relation, the matrix $[J]_{6^k} = ([J]_{6^{k-1}} \otimes [J]_6)$ is order of 6^k binary block Jacket transform. The fast algorithm depends on the following sparse factorization.

$$[J]_{6^k} = ([J]_{6^{k-1}} \otimes [I]_2)([J]_{6^{k-1}} \otimes [J]_2) \quad (42)$$

If the matrix is of order 15, we can write

$$[J]_{15} = [J]_3 \otimes [J]_5 . \quad (43)$$

The signal flow graph corresponding (44) is shown in Fig. 1 and its factorization will be

$$[J]_{15} = \left([I]_3 \otimes [J]_5\right)\left([J]_3 \otimes [I]_5\right). \quad (44)$$

$$= \left([I]_3 \otimes \begin{pmatrix} \beta_0 & \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \beta_4 & \beta_0 & \beta_1 & \beta_2 & \beta_3 \\ \beta_3 & \beta_4 & \beta_0 & \beta_1 & \beta_2 \\ \beta_2 & \beta_3 & \beta_4 & \beta_0 & \beta_1 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_0 \end{pmatrix} \right) \times \left([J]_3 \otimes [I]_5\right) \quad (45)$$

Table 1. Computational complexity of the fast algorithms with directed computation(DC) and proposed(P) of the block Jacket transform. In the Table ADD and MUL are the abbreviations of additions and multiplications.

	DC	Proposed $N=2^k$	Proposed $N=3^k$	Proposed $N=3^k$
ADD	$N(N-1)$	$N\log_2 N$	$2N\log_3 N$	$4N\log_5 N$
MUL	$N\times N$	$1/2N\log_2 N$	$4/3N\log_3 N$	$16/5N\log_5 N$

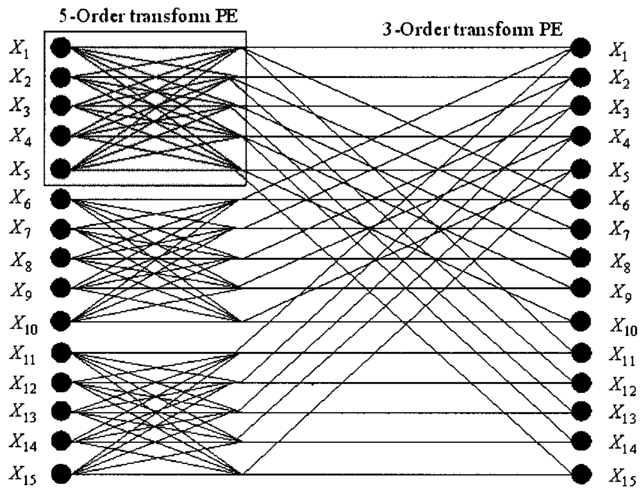


Fig. 1. Jacket transform signal flow graph of order-15.

It can be seen that the computation of order-15 matrix is the combination of three times of order 5 and five times of order 3. In general, the computational complexity of the proposed fast algorithm and higher order binary block Jacket transform implementations inverse are similar to those in [1]. For example, for binary block Jacket transform of order $N=2^k$ requires $N\log_2 N$ additions and $1/2N\log_2 N$ multiplications. For binary block Jacket transform of order $N=3^k$ requires $2N\log_3 N$ additions and $4/3N\log_3 N$ multiplications. For binary block Jacket transform of order $N=5^k$ requires $4N\log_5 N$ additions and $16/5N\log_5 N$ multiplications. These results summed up as in the Table 1.

Ⅳ. Two Dimensional Fast Algorithm for Binary Block Jacket Transform

The two dimensional matrix transforms a temporal/spatial matrix into a transformed matrix as

$$Y = [J]_N X \left([J]_N\right)^T . \quad (46)$$

Generally, the linear transform of matrix X shown as $A\times B=Y$ can be expressed by the transformation of the column-wise stacking vector of X as[1],[5],[17].

$$\left([J]_N \otimes [J]_N\right).vec(X) = vec(Y) \tag{47}$$

Thus, the two dimensional binary block Jacket matrix in (46) can be expressed by

$$vec(Y) = \left([J]_N \otimes [J]_N\right) vec(X). \tag{48}$$

Hence, the two dimensional fast algorithm for binary block Jacket transform decomposition based on one dimensional fast algorithm may be described as follows:

$$[J]_N = [J]_{N_2} \otimes [J]_{N_1} = \left([I]_{N_2} \otimes [J]_{N_1}\right)\left([J]_{N_2} \otimes [I]_{N_1}\right) \tag{49}$$

For example, $N_1=N_2=4=2^2$, then

$$\begin{aligned} [J]_4 \otimes [J]_4 &= \left([I]_{2^2} \otimes [J]_{2^2}\right)\left([J]_{2^2} \otimes [I]_{2^2}\right) \\ &= \left([I]_{2^2} \otimes \left([J]_2 \otimes [J]_2\right)\right)\left(\left([J]_2 \otimes [J]_2\right) \otimes [I]_{2^2}\right) \\ &= \left([I]_{2^2} \otimes [I]_2 \otimes [J]_2\right)\left([I]_{2^2} \otimes [J]_2 \otimes [I]_2\right) \\ &\quad \left([I]_2 \otimes [J]_2 \otimes [I]_{2^2}\right)\left([J]_2 \otimes [I]_2 \otimes [I]_{2^2}\right) \end{aligned} \tag{50}$$

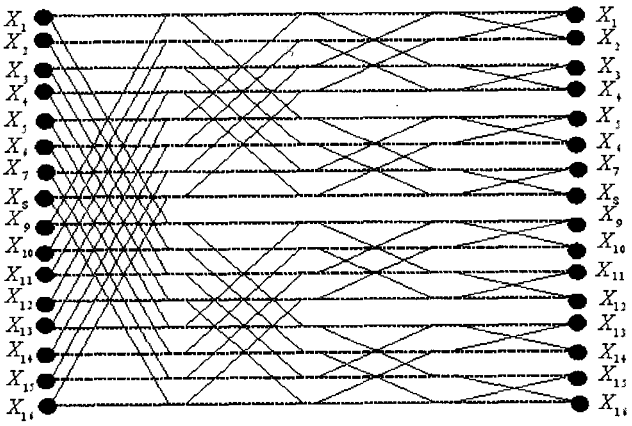


Fig. 2. 2-D 4×4 signal flow graph of Jacket transform.

V. Application of Binary Low Density Quasi Block Jacket Matrices(LDQBJ)

In this section, we present low density quasi block Jacket matrices which are over $GF(2)$, i.e., binary matrices.

Let p be a prime, and let

$$E^h = \left[e_{i,j}\right]_{p \times p}, \tag{51}$$

where

$$\begin{cases} 1 & for\ i = \langle j+h \rangle \\ 0 & otherwise \end{cases} \tag{52}$$

where

$\langle j+h \rangle = j+h \bmod p \ and\ 0 \le i, j, h \le p-1.$

The matrices E^h, for $0 \le h \le p-1$ are refer to circulant permutation matrices(CPM). It can be easily seen that $\{I, E, \cdots, E^{p-1}\}$ from an Abelian group with traditional matrix multiplication and $I=E^p$.

For example, let $p=5$, we have

$$I = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad E = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$E^2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \quad E^3 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$E^4 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{53}$$

Let

$$\Lambda \triangleq \begin{bmatrix} I & O \\ E^h & I \end{bmatrix}, \quad \Omega \triangleq \begin{bmatrix} I & E^{-h} \\ O & I \end{bmatrix} \tag{54}$$

$$\Lambda^2 = \begin{bmatrix} I & O \\ E^h & I \end{bmatrix} \times \begin{bmatrix} I & O \\ E^h & I \end{bmatrix} = I_{2p}$$

$$= \begin{bmatrix} I & E^{-h} \\ O & I \end{bmatrix} \times \begin{bmatrix} I & E^{-h} \\ O & I \end{bmatrix} = \Omega^2, \tag{55}$$

$$(\Lambda\Omega + \Omega\Lambda) =$$

$$\begin{bmatrix} I & O \\ E^h & I \end{bmatrix} \times \begin{bmatrix} I & E^{-h} \\ O & I \end{bmatrix} + \begin{bmatrix} I & E^{-h} \\ O & I \end{bmatrix} \times \begin{bmatrix} I & O \\ E^h & I \end{bmatrix} =$$

$$\begin{bmatrix} I & I \\ I & O \end{bmatrix} + \begin{bmatrix} O & I \\ I & I \end{bmatrix} = I_{2p}, \tag{56}$$

and

$$(\Lambda\Omega) \times (\Omega\Lambda) = \begin{bmatrix} I & I \\ I & O \end{bmatrix} \times \begin{bmatrix} O & I \\ I & I \end{bmatrix} = \begin{bmatrix} I & O \\ O & I \end{bmatrix} = I_{2p}, \tag{57}$$

i.e.

$$\begin{cases} \Lambda = \Lambda^{-1}, \Omega = \Omega^{-1}, \Lambda^2 = \Omega^2 = I_{2p}, \\ \Lambda\Omega + \Omega\Lambda = I_{2p} \\ (\Lambda\Omega)^{-1} = \Omega\Lambda, (\Omega\Lambda)^{-1} = \Lambda\Omega \end{cases} \tag{58}$$

Furthermore,

$$\begin{bmatrix} \Lambda & \Omega \\ \Omega & \Lambda \end{bmatrix} \times \begin{bmatrix} \Omega & \Lambda \\ \Lambda & \Omega \end{bmatrix} = \begin{bmatrix} \Lambda\Omega + \Omega\Lambda & \Lambda^2 + \Omega^2 \\ \Omega^2 + \Lambda^2 & \Omega\Lambda + \Lambda\Omega \end{bmatrix} = \begin{bmatrix} I & O \\ O & I \end{bmatrix} \tag{59}$$

i.e

$$\begin{bmatrix} \Lambda & \Omega \\ \Omega & \Lambda \end{bmatrix}^{-1} = \begin{bmatrix} \Omega & \Lambda \\ \Lambda & \Omega \end{bmatrix} \tag{60}$$

Let,

$$J \triangleq \begin{bmatrix} \Lambda & \Omega \\ \Omega & \Lambda \end{bmatrix} = \begin{bmatrix} I & O & I & E^{-h} \\ E^{h} & I & O & I \\ I & E^{-h} & I & O \\ O & I & E^{h} & I \end{bmatrix} \tag{61}$$

It can be easily checked that

$$J \times J^{-1} = I_{2p} \tag{62}$$

where

$$J^{-1} \triangleq \begin{bmatrix} \Omega & \Lambda \\ \Lambda & \Omega \end{bmatrix} = \begin{bmatrix} I & E^{-h} & I & O \\ O & I & E^{h} & I \\ I & O & I & E^{-h} \\ E^{h} & I & O & I \end{bmatrix} \tag{63}$$

or

$$J^{-1} = \begin{bmatrix} O_2 & I_2 \\ I_2 & O_2 \end{bmatrix} \times \begin{bmatrix} \Lambda & \Omega \\ \Omega & \Lambda \end{bmatrix} = \begin{bmatrix} O_2 & I_2 \\ I_2 & O_2 \end{bmatrix} \times \begin{bmatrix} \Lambda^{-1} & \Omega^{-1} \\ \Omega^{-1} & \Lambda^{-1} \end{bmatrix} \tag{64}$$

We can decompose this order-2 binary block Jacket matrix as equation (25). The proposed hardware implementation is shown in Fig. 3. The shift register provides the basic identity matrix which is circularly permuted by circular permutation block, and fast algorithm products the whole matrix by using proper processing element construction.

Now we consider the density of 0's and 1's in $4p \times 4p$ binary matrix denoted by

$$S_{4p} = \frac{N}{N_0 + N} \tag{65}$$

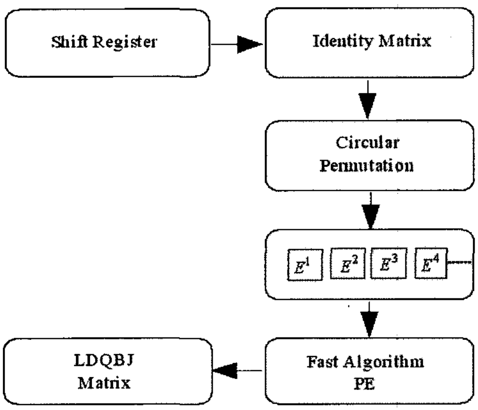


Fig. 3. LDQBJ architecture of the fast encoding algorithm for the matrix decomposition.

where N_a the N_1 numbers of 0's and 1 are respectively. The total number of 0's and 1's in $4p \times 4p$ binary matrix is $16p^2$. There are $12I$, E^{-h}, and E^{h}. Each of I, E^{-h}, and E^{h} contains only p 1's. The total number of 1's is 12p. Thus the density of 1's in J is

$$S_{4p} = \frac{12p}{16p_2} = \frac{3}{4p} \tag{66}$$

It means that this quasi Jacket-matrix is low density matrix.

For example, let p=5 and h=2, then, size of the matrix well be 20×20, which can be factorize like,

$$\begin{aligned} [J]_{20} &= [J]_5 \otimes [J]_4 \\ &= \left([I]_4 \otimes [J]_5\right)\left([J]_4 \otimes [I]_5\right) \end{aligned} \tag{67}$$

Remark: J is a (3,3)-low density matrix, i.e., each row and each column of J contains exactly three 1's.

$$J_{20} = \left[\begin{array}{ccccc|ccccc|ccccc|ccccc}
1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0\\
0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0\\ \hline
0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0\\
1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0\\
0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1\\ \hline
1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0\\
0&0&0&1&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0\\ \hline
0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&0\\
0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1
\end{array}\right]$$

$$J_{20}^{-1} = \left[\begin{array}{ccccc|ccccc|ccccc|ccccc}
1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0\\
0&0&0&1&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0\\ \hline
0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&0\\
0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1\\ \hline
1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0\\
0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0\\ \hline
0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0\\
1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0\\
0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1
\end{array}\right]$$

Ⅵ. Conclusion

Fast binary block Jacket transforms and binary block inverse transforms are proposed, which overcome the mathematical problem in [1] and also satisfy the relation $[J]_N[J]_N^{-1}=[I]_N$. The orders 2^k, 3^k and 5^k binary block Jacket transforms are constructed and their binary block inverse transforms are easily obtained by the transpose of binary block transforms. The one and two dimensional fast algorithm for binary block transforms is proposed and valid, which are based on the recursive forms and the Kronecker product of the identity matrix and lower order binary block matrix. These block inverse Jacket transform and binary low density quasi block Jacket matrices can be applied to signal processing, coding theory and orthogonal code design[1],[7],[8],[18],[19],[20],[25].

This work was supported in part by Minister of Information and Communication(MIC) under IT Foreign Specialist Inviting Program(ITFSIP) supervised by IIFA and ITRC supervised by IITA, ITSOC and International Cooperative Research Program of the Ministry of Science and Technology and KOTEF, 2^{nd} stage BK21, Korea; and supported in part by National Natural Science Foundation of China (No. 10371075).

References

[1] M. H. Lee, J. Hou, "Fast block inverse Jacket transform", *IEEE Signal Processing Letters*, vol. 13, no. 8, pp. 461-464, Aug. 2006.

[2] N. Ahmed, K. R. Rao, *Orthogonal Transforms for Digital Signal Processing*, New York, Springer-Verlag, 1975.

[3] Yang Yi Xian, *Theory and Application of Higher-Dimensional Hadamard Matrices*, Kluwer Academic Publishers, 2001.

[4] V. Anthony, Geramita Jenifer Seberry, *Orthogonal Designs, Quadratic forms and Hadamard Matrices*, Marcel Dekker, Inc., 1979.

[5] C. P. Fan, J. F. Yang, "Fast center weighted Hadamard transform algorithms", *IEEE Trans. Circuits Syst. II*, vol. 45, no. 3 pp. 429-432, Mar. 1998.

[6] Ian Oppermann, "Orthogonal complex-valued spreading sequences with a wide range of correlation properties", *IEEE. Trans. Commun.*, vol. 45, no. 11, pp. 1379-1380, Nov. 1997.

[7] J. Hou, M. H. Lee, "Construction of the dual OV SF codes with lower correlations", Accepted by *IEICE Trans.*, 2006.

[8] J. Hou, M. H. Lee, "Enhancing data throughput and lower correlations quasi orthogonal functions for 3G CDMA systems", *International Journal of Communicational Systems*, John Wiley and Sons, published online, Jan. 2006.

[9] A. J. Goldsmith, S. G. Chua, "Adaptive coded mo dulation for fading channels", *IEEE Trans. On Communications*, vol. 46, no. 5, pp. 595-602, May 1998.

[10] M. H. Lee, "A new reverse Jacket transform and its fast algorithm", *IEEE Trans. Circuits and Systems-II*, vol. 47, no. 1, pp. 39-47, Jan. 2000.

[11] K. W. Schmidt, E. T. H. Wang, "The weighted of Hadamard matrices", *Journal of Combinatorial Theory, Ser. A 23*, pp. 257-263, 1977.

[12] M. H. Lee, "The center weighted Hadamard transform", *IEEE Trans. Circuits Syst.*, vol. 36, no. 9, pp. 1247-1249, Sep. 1989.

[13] S. R. Lee, J. Y. Yi, "Fast reverse jacket transform as an alternative representation of the A-point fast fourier transform", *Journal of Mathematical Imaging and Vision*, vol. 16, pp. 31-39, Jan. 2002.

[14] M. H. Lee, K. Finalayson, "A simple element inverse jacket transform coding", appeared *IEEE Signal Processing Letters*, Mar. 2007.

[15] K. Finlayson, M. H. Lee, J. Seberry, and M. Yamada, "Jacket matrices constructed from Hadamard matrix and generalized Hadamard matrices", *The Australasian Journal of Combinatorics*, vol. 35, no. 1, pp. 83-88, Jun. 2006.

[16] K. J. Horadam, "A generalized Hadamard transform", *IEEE International Symposium on Information Theory(ISIT)*, Sep. 2005.

[17] R. A. Horn, C. R. Johnson, *Topics in Matrix Analysis*, New York, Cambridge Univ., 1991.

[18] D. C. Park, M. H. Lee, and E. A. Choi, "Revisited DFT matrix via the reverse Jacket transform and its applications to communications", *22nd Symposium on Information Theory and its Applications(SITA 99)*, Yuzawa, pp. 427-430, Nov. 1999.

[19] J. Hou, M. H. Lee, "QPSK differential space time coding on different unitary matrices sets and initialization", *International Journal of Communicational Systems*, John Wiley and Sons, published online, Jan. 2006.

[20] Mrityunjoy Chakraborty, R. Shaik, and M. H. Lee, "A block-floating-point based realization of the block LMS algorithm", *IEEE Trans. on Circuits and Systems-II*, vol. 53, no. 9, Sep. 2006.

[21] M. G. Parker, M. H. Lee, "Optimal bipolar sequences for the complex reverse-jacket transform",

International Symposium on Information Theory and Its Applications, Honolulu, Nov. 2000.

[22] W. P. Ma, *The Jacket Matrix and Cryptography*, Technical Report, Chonbuk National University, 2004.

[23] J. Hou, M. H. Lee, "Cocyclic jacket matrices and its application to cryptography systems", Springer Berlin/Heidelberg, LNCS, 2005.

[24] M. H. Lee, B. S. Rajan, and J. Y. Park, "A generalized reverse jacket transform", *IEEE Trans. Circuits Syst. II, Analog Digital Signal Processing*, vol. 48, no. 7, pp. 684-691, Jul. 2001.

[25] Jia Hou, M. H. Lee, "Matrices analysis of quasi orthogonal space time block codes", *IEEE Communication. Letters*, vol. 7, no. 8, Aug. 2003.

Moon-Ho Lee

He received the B.S. and M.S. degree both in electrical engineering from the Chonbuk National University, Korea, in 1967 and 1976, respectively, and the Ph. D. degree in electronics engineering from the Chonnam National University in 1984 and the University of Tokyo, Japan, in 1990. From 1970 to 1980, he was a chief engineer with Namyang Moonhwa Broadcasting. Since 1980, he has been a professor with the department of information and communication and a director with the Institute of Information and Communication, both at Chonbuk National University. From 1985 to 1986, he was also with the University of Minnesota, as a Postdoctoral Feller. He has held visiting positions with the University of Hannover, Germany, during 1990, the University of Aachen, Germany, during 1992 and 1996, and the University of Munich, Germany, during 1998. His research interests include the multidimensional source and channel coding, mobile communication, and image processing.

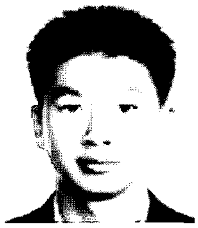
Xiao-Dong Zhang

He received the B.S. degree in Mathematics from Huaiyin Normal College, China in 1984, M.S. degree in Mathematics from Anhui University, China in 1992 and received the Ph.D. degree in Mathematics from University of Science and Technology, China, in 1998. He is currently full time professor in Shanghai Jiao Tong University, China. His research interest includes the Combinatorics and its Applications.

Subash Shree Pokhrel

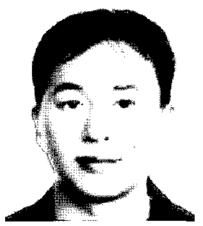
He received the B.S. degree from Tribhuvan University, Nepal in 2000 and M.S. degrees in Information Technology from Manipal University, India in 2004. He is currently in Ph.D. course at Chonbuk National University. His research interests include the areas of mobile communications and channel coding.

Chang-hui Choe



He received the B.S. degree from Korea Advanced Institute of Science and Technology, Korea in 1999 and M.S. degree in Chonbuk National University in 2006. He is currently in Ph.D. course at Chonbuk National University. His research interests include the areas of information security, cryptography, and mobile communications.

Gi-Yean Hwang



He received the B.S. degree in electrical engineering from Seonam University, Korea in 1998 and M.S. degree in computer and information from Seonam University in 2001. Now he is a Ph.D. candidate in information and communication at the Chonbuk National University. His research interests include the MIMO-OFDM and mobile communications.