Information Sciences 291 (2015) 172–183

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Fast Fourier transform using matrix decomposition

Yicong Zhou [a,*], Weijia Cao [a], Licheng Liu [a], Sos Agaian [b], C.L. Philip Chen [a]

[a] Department of Computer and Information Science, University of Macau, Macau 999078, China
[b] Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249, USA

ARTICLE INFO

Article history:
Received 17 July 2013
Received in revised form 10 June 2014
Accepted 5 August 2014
Available online 4 September 2014

Keywords:
Fast Fourier transform
Orthogonal transform
Sparse matrix
Image encryption

ABSTRACT

To reduce both the multiplicative complexity and total number of operations, this paper introduces a modeling scheme of the fast Fourier transform (FFT) to decompose the discrete Fourier transform (DFT) matrix recursively into a set of sparse matrices. Integrating three orthogonal transforms, the Hadamard, Modified Haar and Hybrid transforms, the proposed scheme is able to obtain different FFT representations with less computation operations than state of the arts. To investigate the applications of the proposed FFT scheme, a multi-stage image encryption algorithm is also introduced. Experimental results and security analysis are provided to show its encryption performance.

1. Introduction

As one of the most frequently used operations in digital signal processing, the discrete Fourier transform (DFT) has been widely employed in various fields [11,12,30] such as optical systems [26,29], medical research [8], and image processing [20,28]. However, directly calculating an N-point DFT requires N^2 complex multiplications and $N(N-1)$ complex additions. This extremely slows down the speed of digital signal processing, especially real-time signal processing.

To reduce the computation complexity, various fast Fourier transform (FFT) algorithms have been developed [1,5,11,13,14]. A split-radix-2/8 FFT algorithm [11,22] was proposed to recursively factor a length-N DFT into one length-$\frac{N}{2}$ DFT and four length-$\frac{N}{8}$ DFTs. Including the DFT properties of periodicity and symmetry, several improved algorithms have been also developed such as the recursive FFT [24], fused FFT [21], radix-$2/2^s$ ($4 \leqslant s \leqslant m$) FFT [6], decimation in frequency (DIF) and time (DIT) pruning scheme [17], and mixed-radix FFT [25]. They are effective to reduce the computation complexity of DFT. For example, the recursive FFT scheme was reported to have less computation complexity than the conventional algorithms for computing Fourier-like transforms [24]. In addition, the fused FFT is 15% faster than traditional implementations [21]. Different from these algorithms, this paper proposes a modeling FFT scheme to decompose DFT into a number of sparse matrices. Using different orthogonal transforms, the proposed scheme can obtain various FFT representations. We select the Hadamard, modified Haar, and Hybrid (Hadamard–Haar) transforms as examples to show its effectiveness. The proposed scheme significantly reduces the computation complexity and shows better performance than several state-of-the-art FFT methods.

In addition to low computation complexity, the proposed scheme also shows benefits in data security because it is able to protect data with multiple security levels. As an example, this paper introduces a multi-stage image encryption algorithm (MSIEA) using the proposed FFT scheme. Unlike many image encryption algorithms that protect images using parametric

* Corresponding author. Tel.: +86 853 83978458; fax: +86 853 28838314.
E-mail address: yicongzhou@umac.mo (Y. Zhou).

http://dx.doi.org/10.1016/j.ins.2014.08.022
0020-0255/

DFTs, such as the discrete fractional Fourier transform (DFrFT) [15,16,23] and phase-truncated Fourier transform [19], the proposed MSIEA integrates the image encryption processes with the FFT decomposition. Using different permutation matrices allows MSIEA to encrypt images in different security levels. Experimental results and security analysis are provided.

The rest of this paper is organized as follows. Section 2 introduces the FFT scheme and three examples using orthogonal transforms. Section 3 proposes the multi-stage image encryption algorithm. Its simulation results are provided in Section 4 and its security issues are analyzed in Section 5. Finally, Section 6 reaches a conclusion.

2. Proposed FFT scheme

For an N-point input data sequence $X = (x_0, x_1, \ldots, x_{N-1})^T$, suppose data vector $Y = (y_0, y_1, \ldots, y_{N-1})^T$ is the result of its discrete Fourier transform (DFT). The matrix format of N-point DFT and its inverse transform are defined as

$$Y = F_N X \quad \text{and} \quad X = \frac{1}{N} F_N^{-1} Y \tag{1}$$

where F_N^{-1} is an inverse matrix of the DFT matrix F_N defined by

$$F_N = \begin{pmatrix} W_N^{0\cdot 0} & W_N^{0\cdot 1} & \cdots & W_N^{0\cdot(N-1)} \\ W_N^{1\cdot 0} & W_N^{1\cdot 1} & \cdots & W_N^{1\cdot(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ W_N^{(N-1)\cdot 0} & W_N^{(N-1)\cdot 1} & \cdots & W_N^{(N-1)\cdot(N-1)} \end{pmatrix} \tag{2}$$

where $W_N^{n\cdot k} = e^{-j\frac{2\pi nk}{N}}$ with $n, k \in (0, 1, 2, \ldots, N-1)$ is so-called the twiddle factor.

Here, we introduce an FFT scheme to decompose the DFT matrix F_N into a number of sparse matrices. Its structure is illustrated in Fig. 1.

For an *N-point* ($N = 2^n$) DFT matrix, the general formula of the proposed FFT scheme is defined by

$$F_N = P_N^2 \left(I_{\frac{N}{2^{n-1}}} \oplus F^{sr}_{\frac{N}{2^{n-1}}} \oplus F^{sr}_{\frac{N}{2^{n-2}}} \oplus \cdots \oplus F^{sr}_{\frac{N}{2}} \right) P_N^1 D_N O_N \tag{3}$$

where F_N^{sr} denotes F_N or its deformation (such as being applied with permutation or scaled by factors), P_N is a permutation matrix (including the identity matrix), D_N is a diagonal matrix (including the identity matrix), O_N is the orthogonal matrix and $\oplus$ denotes the direct matrix sum defined in Eq. (4) where $A \in C^{N_1 \times N_2}$ and $B \in C^{N_3 \times N_4}$ are two matrices,

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \tag{4}$$

Utilizing orthogonal transforms with appropriate decompositions, the N-point DFT can be iteratively divided into small DFTs with or without a few number of twiddle factors. In this manner, the proposed FFT scheme significantly reduces the computation complexity. Applying different orthogonal transform matrices to O_N in Eq. (3) yields new FFT representations. Next, we will provide three examples to show the effectiveness of the proposed scheme.

2.1. Hadamard transform based FFT representation (HDT-FFT)

Using the Hadamard transform [1,2] O_N in Eq. (3) can be defined as:

$$O_N = \prod_{i=1}^{\log N} \left(I_{\frac{N}{2^i}} \otimes H_2 \otimes I_{2^{i-1}} \right) \tag{5}$$

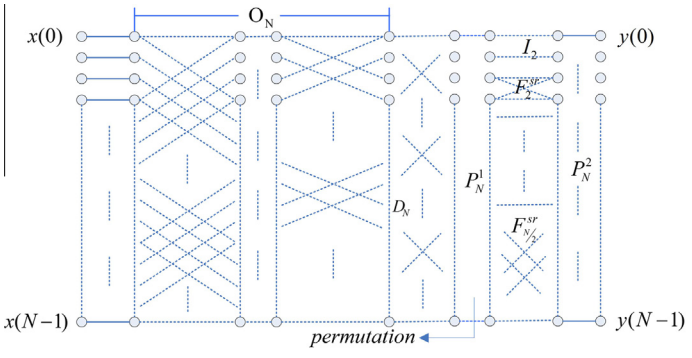

Fig. 1. The structure of the proposed N-point FFT scheme.