www.elsevier.com/locate/image

Cosine Transforms over Fields of Characteristic 2: Fast Computation and Application to Image Encryption

J.B. Lima, E.S. da Silva, R.M. Campello de Souza

PII: S0923-5965(17)30042-5
DOI: http://dx.doi.org/10.1016/j.image.2017.03.007
Reference: IMAGE15191

To appear in: *Signal Processing : Image Communication*

Received date: 24 June 2016
Revised date: 12 January 2017
Accepted date: 14 March 2017

Cite this article as: J.B. Lima, E.S. da Silva and R.M. Campello de Souza Cosine Transforms over Fields of Characteristic 2: Fast Computation and Application to Image Encryption, *Signal Processing : Image Communication* http://dx.doi.org/10.1016/j.image.2017.03.007

Cosine Transforms over Fields of Characteristic 2: Fast Computation and Application to Image Encryption

J. B. Lima[a,*], E. S. da Silva[a], R. M. Campello de Souza[a]

[a]*Department of Electronics and Systems, Federal University of Pernambuco*
Av. da Arquitetura, S/N, 4º andar - Cidade Universitária - Recife, PE - Brazil - 50740-550
Tel.: +55-81-91140396 - Fax: +55-81-21267117

Abstract

In this paper, we introduce a fast algorithm for computing cosine transforms over fields of characteristic 2 (FFCT). Such transforms, which were recently proposed in the literature, are analogous to real-valued discrete cosine transforms in the same sense in which the finite field Fourier transform (FFFT) is analogous to the discrete Fourier transform. The referred algorithm is based on fast algorithms for computing cyclic convolutions over fields of characteristic 2. In particular, we present an algorithm for an 8-point FFCT over GF(2^8) and show how such a transform can be used as the basis of an image encryption scheme. We highlight the advantages of this scheme compared to that based on cosine transforms over fields of odd characteristic and perform computer simulations to demonstrate its resistance against the main cryptographic attacks.

Keywords: Finite field cosine transform, fields of characteristic 2, fast algorithms, image encryption

1. Introduction

Since their introduction in the 1970's, finite field transforms have been used in different application scenarios [22]. In signal processing, where such mathematical tools are commonly known as number-theoretic transforms, they are mainly used for efficient computation of linear convolutions [1, 4, 24, 12]. This avoids rounding-off errors and provides advantages related to the algebraic structures where the transform is defined [4, 13]. In error-correcting codes, finite field transforms are used, for instance, to achieve interesting interpretations of the encoding and decoding processes [3, 26, 19].

In most cases, the finite field transforms are Fourier-like transforms. This means that, for an N-point transform, the kernel is an N-th root of unity in the field where the transform is defined. However, other types of finite field transforms have also been defined. This includes cosine, sine, Hartley and wavelet transforms, which have encountered applications in cryptography, error-correcting codes, information hiding and multiuser communication, for example [6, 15, 9, 18, 8]. With respect to the finite field cosine transform, it is remarkable the fact that, originally, such a transform had been defined only over fields of odd characteristic. This restriction came from

*Corresponding author
Email address: juliano_bandeira@ieee.org (J. B. Lima)