Signal Processing 94 (2014) 521–530

Contents lists available at ScienceDirect

Signal Processing

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

Image encryption based on the fractional Fourier transform over finite fields

J.B. Lima [a,*], L.F.G. Novaes [b]

[a] Department of Mathematics, Federal University of Pernambuco, Av. Jornalista Aníbal Fernandes, S/N, Cidade Universitária, CEP 50740-560 Recife, Brazil

[b] Polytechnic School of Pernambuco, University of Pernambuco, Rua Benfica, 455, CEP 50750-470 Recife, Brazil

ARTICLE INFO

Article history:
Received 16 February 2013
Received in revised form
17 May 2013
Accepted 16 July 2013
Available online 30 July 2013

Keywords:
Fractional Fourier transforms
Finite fields
Image encryption

ABSTRACT

In this paper, we introduce fractional Fourier transforms over finite fields GF(p), where $p \equiv 1 \pmod 4$. Such a definition is based on the approach given in [1], which corresponds to a finite field extension of the commuting matrix method for defining discrete fractional Fourier transforms [2]. The transforms we have constructed are then used as the basis of a novel image encryption scheme. Security aspects of such a scheme are analyzed through computer simulations and specific metrics.

1. Introduction

In recent years, fractional transforms have been studied by researchers originated from several fields of knowledge. Such transforms can be viewed as generalizations of the corresponding ordinary transforms, where an additional parameter is included. This parameter, normally referred to as fractional order, is a noninteger number related to the computation of arbitrary powers of the respective transform operator. The most widely investigated fractional transform is the fractional Fourier transform, which has a well established continuous-time version and also several definitions in the discrete-time framework [2–5]. Fractional Fourier transforms are applied, for example, in signal filtering, image encryption, multiuser communication and watermarking [6–9].

Recently, finite field versions for fractional Fourier transforms were introduced. In [10], such transforms are referred to as fractional number-theoretic transforms and their definition is based on complete generalized Legendre sequences over finite fields. In [1], the finite field fractional Fourier transform is identified by the acronym GFrFT, where "G" alludes to "Galois field"; in this case, the transform is defined by using an extension to the finite field scenario of the commuting matrix method for transform fractionalization [2] and the construction of GFrFT over GF(p), where $p \equiv 3 \pmod 4$, is emphasized.

In the present paper, we extend the definition proposed in [1], showing how to construct GFrFT over GF(p), where $p \equiv 1 \pmod 4$. A specific GFrFT is then constructed and an image encryption scheme based on such a transform is introduced. In the proposed method, blocks of the plain-image are sequentially transformed by the GFrFT. The fractional parameter used in the transformation of each block is obtained from a secret key. Since there is superposition among two consecutive blocks taken from the plain-image, the encryption/decryption of a block affects all subsequent blocks. This property provides good results related to the robustness against differential attack and the key sensitiveness of the method [11]. In the proposed technique, only modular arithmetic is necessary to compute the GFrFT. This avoids rounding and assures that the decrypted image and the corresponding plain-image are identical, if the correct key

* Corresponding author. Tel.: +55 81 2126 7687; fax: +55 81 2126 8410.
E-mail addresses: juliano@dmat.ufpe.br (J.B. Lima), filipe.g.novaes@gmail.com (L.F.G. Novaes).

0165-1684/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.sigpro.2013.07.020

is used. Additionally, the application of the finite field transform leads to the uniformization of the histogram of the ciphered-images, which makes the scheme secure against statistical attacks [11].

This paper is organized as follows. In Section 2, we review the definition of trigonometric functions over finite fields; we also present some definitions and propositions concerning the finite field Fourier transform and its eigenstructure. When compared to the content presented in [1], several results given in Section 2 had to be adjusted, in order to make all concepts valid for finite fields GF(p), where $p \equiv 1 \pmod 4$. In Section 3, we summarize the steps for constructing the GFrFT and, as an example, we construct the transform used in the encryption scheme to be introduced. In Section 4, we introduce the image encryption scheme based on the GFrFT. In Section 5, the main aspects related to the security of the method are discussed and simulation results are shown. The paper closes with some concluding remarks given in Section 6.

2. Preliminaries

In this section, the definition of trigonometric functions over finite fields is reviewed [12]. Definitions and propositions concerning the finite field Fourier transform (FFFT) and its eigenstructure are also shown [1,13]. Differently from previous papers, all results presented here are valid not only for prime finite fields whose characteristic is $p \equiv 3 \pmod 4$, but also for the cases where $p \equiv 1 \pmod 4$. Some adjustments had to be done in order to support such a generalization.

2.1. Trigonometry in finite fields

Definition 1. The set of Gaussian integers over GF(p) is the set $\mathrm{GI}(p) = \{c + dj, c, d \in \mathrm{GF}(p)\}$, where p is a prime such that j^2 is a quadratic nonresidue over GF(p).

If $p \equiv 3 \pmod 4$, the set GI(p) can be constructed by using $j = \sqrt{-1}$. On the other hand, if $p \equiv 1 \pmod 4$, there is no general rule which gives quadratic nonresidues; in this case, the number j used in the construction of GI(p) can be chosen through a searching procedure or by the use of more restrict rules.[1] A number $\zeta \in \mathrm{GI}(p)$ can be viewed as a "complex" number with "real" and "imaginary" parts given by $\Re\{\zeta\} = c$ and $\Im\{\zeta\} = d$, respectively. In this sense, we can associate an arc to ζ and define the following finite field trigonometric functions.

Definition 2. Let $\zeta \in \mathrm{GI}(p)$ be an element with multiplicative order denoted by $\mathrm{ord}(\zeta)$. The finite field cosine and sine of the arc related to ζ are computed modulo p, respectively, as

$$\cos_\zeta(x) := 2^{-1}(\zeta^x + \zeta^{-x}) \tag{1}$$

and

$$\sin_\zeta(x) := (2j)^{-1}(\zeta^x - \zeta^{-x}), \tag{2}$$

$x = 0, 1, \ldots, \mathrm{ord}(\zeta) - 1$.

The finite field trigonometric functions defined above hold properties similar to those of the standard real-valued ones, such as the *unit circle* and the *addition of arcs*, for instance [12].

2.2. The finite field Fourier transform

Definition 3. The finite field Fourier transform of a vector $\mathbf{x} = x[i]$, $i = 0, 1, \ldots, N-1$, $x[i] \in \mathrm{GI}(p)$ is a vector $\mathbf{X} = X[k]$, $k = 0, 1, \ldots, N-1$, $X[k] \in \mathrm{GI}(p)$, computed modulo p by

$$X[k] = \sqrt{N^{-1}} \sum_{i=0}^{N-1} x[i]\zeta^{-ki},$$

where $\zeta \in \mathrm{GI}(p)$ has multiplicative order N. The inverse transform is given by

$$x[i] = \sqrt{N^{-1}} \sum_{k=0}^{N-1} X[k]\zeta^{ki}.$$

Specially for signal processing applications, it is common to use FFFT defined over fields where p is a Fermat or a Mersenne prime (see Eqs. (3) and (6) of [10], for example). In these cases, which are referred to as Fermat and Mersenne number transforms, respectively, a multiplication can be performed by bit-shifting operations and transforms with length N being a power of two can be obtained [15,16]. These aspects simplify hardware implementations and allow the use of fast algorithms. In the present paper, we emphasize the construction of transforms in fields where $p \equiv 1 \pmod 4$, which include all Fermat number transforms.

The relationship between $\mathbf{x}$ and $\mathbf{X}$ can be expressed by the matrix equation

$$\mathbf{X} = \mathbf{F}\mathbf{x}, \tag{3}$$

where $\mathbf{F}$ is the transform matrix, the $(k+1)$-th row and $(i+1)$-th column element of which is given by $F_{k,i} = \sqrt{N^{-1}}\zeta^{-ki}$.

2.2.1. Eigenstructure of the FFFT

As expressed in Eq. (3), the computation of the FFFT of a vector can be viewed as a matrix multiplication, which represents the application of the linear transformation defined by the matrix $\mathbf{F}$ to the vector $\mathbf{x}$. Since the definition of a fractional transform is closely related to the eigenstructure of the respective ordinary transform matrix [2,17], the study of the eigenvalues and the eigenvectors of $\mathbf{F}$ performs an essential role in developing the finite field fractional Fourier transform. The most relevant properties concerning the eigenstructure of the FFFT are described in the following propositions [13,18–20].

Proposition 1. *The* $\mathbf{F}$ *matrix has, at most, four distinct eigenvalues,* $\{1, -1, \sqrt{-1}, -\sqrt{-1}\}$, *computed in GI*($p$), *the multiplicities of which are presented in Table 1.*

[1] For example, $j^2 = 2$ is a quadratic nonresidue if and only if $p \not\equiv \pm 1 \pmod 8$. Other rules related to quadratic residues can be found in Number Theory books and articles [14].