Signal Processing: *Image Communication* 35 (2015) 1–8

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

Encryption of medical images based on the cosine number transform

J.B. Lima [a,*], F. Madeiro [b], F.J.R. Sales [c,d]

[a] *Department of Electronics and Systems, Federal University of Pernambuco, Av. da Arquitetura, S/N, CEP 50740-550, Recife/PE, Brazil*
[b] *Polytechnic School of Pernambuco, University of Pernambuco, Rua Benfica, 455, CEP 50720-001, Recife/PE, Brazil*
[c] *Department of Biomedical Engineering, Federal University of Pernambuco, Av. da Arquitetura, S/N, CEP 50740-550, Recife/PE, Brazil*
[d] *Telehealth Center, Hospital das Clínicas, Federal University of Pernambuco, Av. Prof. Moraes Rego, 1235, CEP 50670-901, Recife/PE, Brazil*

ARTICLE INFO

Article history:
Received 29 September 2014
Received in revised form
6 February 2015
Accepted 8 March 2015
Available online 31 March 2015

Keywords:
Medical images
Image encryption
Cosine number transform

ABSTRACT

In this paper, we introduce a novel scheme for encryption of medical images. The technique is based on the cosine number transform, a mathematical tool whose application requires modular arithmetic only. This property avoids rounding-off errors and allows that the image recovered after the encryption/decryption process be identical to the corresponding original image. The proposed scheme is flexible and can be applied to images complying with the DICOM standard, which is frequently employed in medical applications. We show that the technique is capable of resisting the main cryptographic attacks.

1. Introduction

The wide use of medical image, such as computed tomography (CT), magnetic resonance image (MRI), ultrasound and positron emission tomography (PET), has led to intensive research and development concerning compression, processing and security. In particular, medical image security is devoted to provide mainly one or many of the following requirements: confidentiality (only authorized persons can access patient data), integrity (the proof that the medical information has not been modified) and authentication (which is concerned with identification, that is, two communication partners should identify each other–the information origin should be proved) [1–6].

A variety of methods can be applied for providing information security in the scenario of medical images, such as steganography [7], watermarking [8–10] and encryption [11]. Steganography and watermarking are used to imperceptibly embed information in medical images. Encryption involves visual and statistical modification of an image and can be done by employing a plethora of techniques, such as chaos-based methods [12,13]; transforms (such as the fractional Fourier transform [14,15], the finite field cosine transform [16], the Arnold transform [17]); optical systems [18,19]; simultaneous compression and encryption methods [20–22]. In order to be safe, medical image encryption should be robust against a wide variety of attacks, such as statistical and differential attacks.

In this paper, a new medical image encryption scheme based on the cosine number transform (CNT) is proposed [23,24]. Since the CNT is defined over algebraic structures with a finite number of elements (a finite field), only modular arithmetic is needed for computing the transform. Consequently, the computation of a CNT is considerably sensitive to changes in the vector being transformed. In other words, two slightly different vectors may have significantly distinct CNTs, which is desirable for cryptographic applications. This does not occur for real- or complex-valued transforms, such as the ordinary Fourier transform and its variants, which are

* Corresponding author. Tel.: +55 81 2126 7117; fax: +55 81 2126 8215.
E-mail addresses: juliano_bandeira@ieee.org (J.B. Lima), madeiro@poli.br (F. Madeiro), fernando.sales@ufpe.br (F.J.R. Sales).

http://dx.doi.org/10.1016/j.image.2015.03.005
0923-5965/

mainly applied in image encryption techniques implemented in the optical domain [18,25,26]. On the other hand, our approach is suitable for ciphering digital data; it avoids rounding-off errors and assures that the image recovered after an encryption/decryption procedure is identical to the original image, which is very important in the framework of medical images. If a real-valued transform is employed, such a possibility may not be provided, since truncation has to be performed.

More specifically, the method introduced in this work consists in dividing an image into blocks which overlap horizontally and vertically the corresponding adjacent blocks. The blocks are then sequentially taken and submitted to the recursive computation of a two-dimensional CNT. The number of times the CNT is applied to each image block depends on a secret-key, which can be easily encoded as a sequence of bits. The encryption is completed after the whole image is processed twice using the described procedure; the decryption is carried out by applying, in the reverse order, the same steps used in the encryption. The scheme is very flexible and, particularly, simpler than that given in [16], which also employs the CNT; the number of transforms to be computed in the current proposal is less than that required by the method given in [16], and the encoding and the application of the key are more flexible and straight.

This paper is organized as follows. In Section 2, we review the main theoretical aspects related to the cosine number transform. The image encryption technique based on the CNT is introduced in Section 3. In Section 4, we show results obtained from computer simulations and characterize the scheme with respect to several security aspects; key space analysis and metrics related to key sensitivity as well as the robustness to statistical attacks reveal the effectiveness of the proposed medical image encryption technique. The paper closes with the main concluding remarks in Section 5.

2. The cosine number transform

In this section, we discuss the main theoretical aspects related to the cosine number transform (CNT). This mathematical tool, which constitutes the basis of the encryption scheme to be introduced in Section 3, was originally proposed by Campello de Souza et al. in [23], where it was named *finite field cosine transform* (FFCT). The approach presented in [23] is more general than that employed in the current work. More specifically, the FFCT can be defined in extension fields [27]; on the other hand, the CNT is defined considering modular arithmetic only and the following concepts related to trigonometry in finite fields.[1]

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).

[1] Usually, transforms which map vectors with elements in GF(p) into vectors with elements lying in the same field are called *number-theoretic transforms* or simply *number transforms*. This is the reason why we have used the nomenclature *cosine number transform* instead of *finite field cosine transform*.

The "complex" structure GI(p), whose elements $\zeta = c+dj$ have a "real" part $c=\Re\{\zeta\}$ and an "imaginary" part $d=\Im\{\zeta\}$, is isomorphic to the extension field GF(p^2). If $p\equiv 3 \pmod 4$, the use of the quadratic nonresidue $j^2=-1$ provides an interesting analogy with the usual complex numbers [24,28]. Gaussian integers over GF(p), where $p\equiv 1 \pmod 4$, can also be constructed by choosing specific quadratic nonresidues.

Definition 2. Let ζ be a nonzero element in GI(p), and p an odd prime. The finite field cosine function related to ζ is computed modulo p by

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

$x=0,1,\ldots,\mathrm{ord}(\zeta)-1$, where $\mathrm{ord}(\zeta)$ denotes the multiplicative order of ζ.

It is remarkable to observe that the finite field cosine holds properties similar to those of the standard real-valued cosine function, such as *unit circle* and *addition of arcs*. Additionally, if $\zeta=c+dj$ is unimodular, i.e., $c^2+d^2\equiv 1 \pmod p$, the corresponding finite field cosine is computed modulo p as

$$\cos_\zeta(x)=\Re\{\zeta^x\},$$

$x=0,1,\ldots,\mathrm{ord}(\zeta)$ [29]. This plays an essential role in the definition of the CNT employed in this work, which represents the number-theoretic version of the FFCT of type 2 (in [24], other types of finite field cosine transforms and also finite field sine transforms are defined). CNT is computed according to the following definition.

Definition 3. Let ζ be an element in GF(p) or an unimodular element in GF(p), whose multiplicative order is $\mathrm{ord}(\zeta)=2N$. The cosine number transform of the vector $\mathbf{x}=[x_0,x_1,\ldots,x_{N-1}]$, $x_i\in\mathrm{GF}(p)$, is the vector $\mathbf{X}=[X_0,X_1,\ldots,X_{N-1}], X_k\in\mathrm{GF}(p)$, of elements

$$X_k := \sqrt{\frac{2}{N}}\sum_{i=0}^{N-1}\beta_k x_i \cos_\zeta\left[k\left(i+\frac{1}{2}\right)\right], \tag{2}$$

where

$$\beta_r=\begin{cases}1/\sqrt{2}, & r=0,\\ 1, & r=1,2,\ldots,N-1.\end{cases}$$

It can be shown that the CNT given in Definition 3 is invertible by the formula [23,24]

$$x_i=\sqrt{\frac{2}{N}}\sum_{k=0}^{N-1}\beta_i X_k \cos_\zeta\left[\left(k+\frac{1}{2}\right)i\right]. \tag{3}$$

The computation of the CNT of a vector $\mathbf{x}$ can be represented by the matrix equation

$$\mathbf{X}=\mathbf{C}\cdot\mathbf{x},$$

where $\mathbf{C}$ corresponds to the transform matrix, whose elements are obtained directly from Eq. (2). By comparing Eqs. (2) and (3), we verify that $\mathbf{C}\mathbf{C}^T=\mathbf{C}^T\mathbf{C}=\mathbf{I}$, where $\mathbf{C}^T$ and $\mathbf{I}$ denote, respectively, the matrix $\mathbf{C}$ transpose and the identity matrix. This means that the inverse CNT is obtained by using the transform matrix $\mathbf{C}^T$ [29]. Using such a matrix notation, the CNT can be extended to two