Applied Mathematical Modelling 38 (2014) 961–973

Contents lists available at SciVerse ScienceDirect

Applied Mathematical Modelling

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

On the fractional-order extended Kalman filter and its application to chaotic cryptography in noisy environment

Hoda Sadeghian, Hassan Salarieh, Aria Alasty *, Ali Meghdari

Center of Excellence in Design Robotics and Automation, Department of Mechanical Engineering, Sharif University of Technology, PO Box 11155-9567, Tehran, Iran

ARTICLE INFO

Article history:
Received 13 October 2012
Received in revised form 28 May 2013
Accepted 2 July 2013
Available online 24 July 2013

Keywords:
Kalman filter
Stochastic system
Fractional-order system
Chaos synchronization
Cryptography

ABSTRACT

In this paper via a novel method of discretized continuous-time Kalman filter, the problem of synchronization and cryptography in fractional-order systems has been investigated in presence of noisy environment for process and output signals. The fractional-order Kalman filter equation, applicable for linear systems, and its extension called the extended Kalman filter, which can be used for nonlinear systems, are derived. The result is utilized for chaos synchronization with the aim of cryptography while the transmitter system is fractional-order, and both the transmitter and transmission channel are noisy. The fractional-order stochastic chaotic Chen system is then presented to apply the proposed method for chaotic signal cryptography. The results show the effectiveness of the proposed method.

1. Introduction

In the recent two decades, synchronization of chaotic dynamical systems has received considerable interest among scientists in various fields [1]. The first idea of synchronizing two identical chaotic systems with different initial conditions was introduced by Pecora and Carrols [2], and the method was realized in electronic circuits. Synchronization techniques have been improved in recent years, and many different methods have been applied theoretically and experimentally to synchronize chaotic systems [3–5]. One of the interesting topics in chaos synchronization is the cryptography or secure communication [6]. The era of scientific cryptography has been started by Shannon [7] and continued with the works of Diffie and Hellman [8]. The works of Pecora and Carrols [2] triggered the way of chaotic cryptography and after that considerable amount of researches have been published noting the secure communication and the cryptography through chaotic systems [9–14] which declare to be better than classical methods by increasing the level of complexity of the transmitted signal due to chaotic behavior of transmitters [6]. Most of the works in chaotic communication have modeled the chaotic systems in deterministic form [10,12], but in real world applications due to random uncertainties such as stochastic forces on physical systems and noisy measurements caused by environmental uncertainties, a stochastic chaotic behavior is produced instead of a deterministic one. In this case the deterministic differential equation of a system must be substituted by a stochastic one. There are a few works in the field of stochastic chaos synchronization [3,14].

As to increase the complexity of the transmitter, one may use a fractional-order stochastic chaotic system as transmitter. A chaotic fractional-order dynamical equation produces a complex behavior which makes the masked signal more encrypted and consequently hard to decipher. The complexity of fractional-order systems is due to dealing with integration and derivation of non-integer orders [15,16]. The fractional calculus has been used increasingly in variety of fields of sciences and

* Corresponding author. Tel.: +98 21 6616 5504; fax: +98 21 6600 0021.
E-mail addresses: hsadeghian@mech.sharif.edu (H. Sadeghian), salarieh@sharif.edu (H. Salarieh), aalasti@sharif.edu (A. Alasty), meghdari@sharif.edu (A. Meghdari).

0307-904X/$ - see front matter
http://dx.doi.org/10.1016/j.apm.2013.07.011

engineering [17–23]. The history of fractional Calculus returns back to 18th century in the very basic works of Euler and Lagrange and also systematic studies of Liouville, Riemann and Holmgren in the 19th Century. Nowadays this tool is used to model so many systems in variety of fields; viscoelastic structures [24], vibration and suspensions [25], fractional conservation of mass [26] and diffusion wave [27].

The problem of synchronization in fractional-order chaotic systems has been investigated in the literature [28–31] where there is no significant work on stochastic fractional-order chaotic systems has been addressed in literature. In [31] the problem of secure communication in chaotic fractional-order systems has been investigated. The paper [31] used the discretizing method for a deterministic chaotic fractional-order system as chaotic transmitter and then used the fractional-order extended Kalman filter developed for discrete systems in [32] as the receiver while the transmission channel is assumed noisy. Although that paper has been indicated having the process noise; the noise never comes up explicitly in the equations.

To overcome this problem, in this paper a novel discretized continuous-time Kalman Filter for fractional-order discretized continuous-time systems has been introduced as an extension of discrete version presented in [23]. Then this method is used to solve the problem of chaotic synchronization in noisy environment, assuming the transmitter to be stochastic, chaotic, and fractional-order, and transmission channel to be noisy. The receiver is considered as the extended fractional-order Kalman filter. The method has been applied to stochastic fractional-order chaotic Chen system and the results show the effectiveness of the method for cryptography.

2. Kalman filter derivations

In this section the discretized continuous-time Kalman Filter for fractional discretized continuous-time systems applicable to a class of stochastic fractional-order equation will be investigated.

Lemma 1. *Consider the following continuous-time stochastic linear fractional-order differential equation;*

$$ {}_0^C D_t^{\alpha} x_t = A x_t + \Theta z_t, \tag{1}$$

where $x_t : \mathbb{R} \to \mathbb{R}^n$ is a continuous stochastic process, z_t is zero mean stationary noise and Θ is real valued constant matrix. Assume that the time vector $\{t_k\}_{k=1}^{\infty}$ are positive with properties of,

$$ t_{k+1} - t_k = T_k > 0. \tag{2}$$

Thus,

$$ \begin{aligned} x_{t_{k+1}} &= E_{\alpha,1}\left(At_{k+1}^{\alpha}\right)\left[E_{\alpha,1}\left(At_k^{\alpha}\right)\right]^{-1} x_{t_k} \\ &\quad + \int_0^{t_{k+1}} e_{\alpha}^{A(t_{k+1}-\tau)} \Theta z_\tau d\tau - E_{\alpha,1}\left(At_{k+1}^{\alpha}\right)\left[E_{\alpha,1}\left(At_k^{\alpha}\right)\right]^{-1} \int_0^{t_k} e_{\alpha}^{A(t_k-\tau)} \Theta z_\tau d\tau, \end{aligned} \tag{3}$$

where the Mittag–Leffler function $E_{\alpha,\beta}(z)$ with two parameters is defined as,

$$ E_{\alpha,\beta}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(k\alpha+\beta)} \tag{4}$$

and the α-exponential function $e_{\alpha}^{\lambda z}$ is defined as,

$$ e_{\alpha}^{\lambda z} = z^{\alpha-1} E_{\alpha,\alpha}(\lambda z^{\alpha}). \tag{5}$$

Proof. One may write for steps k and $k+1$ respectively, the solution of Eq. (1) as [16],

$$ x_{t_{k+1}} = E_{\alpha,1}\left(At_{k+1}^{\alpha}\right) x_0 + \int_0^{t_{k+1}} e_{\alpha}^{A(t_{k+1}-\tau)} \Theta z_\tau d\tau, \tag{6}$$

$$ x_{t_k} = E_{\alpha,1}\left(At_k^{\alpha}\right) x_0 + \int_0^{t_k} e_{\alpha}^{A(t_k-\tau)} \Theta z_\tau d\tau. \tag{7}$$

Finding x_0 from Eq. (7) and substituting in Eq. (6) yields to Eq. (3). □

Theorem 1 (Kalman Filter for Linear Fractional-order Stochastic Systems). *Consider the following continuous-time stochastic linear fractional-order differential equation with discrete measurement;*

$$ \begin{aligned} {}_0^C D_t^{\alpha} x_t &= A x_t + \Theta z_t, \\ y_{t_k} &= C x_{t_k} + \upsilon_{t_k}, \end{aligned} \tag{8}$$

where $x_t : \mathbb{R} \to \mathbb{R}^n, y_t : \mathbb{R} \to \mathbb{R}^p$ are continuous-time stochastic processes, and $A \in \mathbb{R}^{n\times n}, \Theta \in \mathbb{R}^{n\times q}, C \in \mathbb{R}^{p\times n}$ are time invariant real matrices. ${}_0^C D_t^{\alpha}$ is the Caputo fractional derivative of order $0 < \alpha \leqslant 1. z_t, t \in \mathbb{R}$ and υ_{t_k}, which is also depicted by υ_k, indexed by parameter $k \in \mathbb{N}$ are two different independent, respectively, continuous-time and discrete-time, zero-mean independent stationary noise with properties of