Signal Processing: Image Communication 58 (2017) 35–48

Contents lists available at ScienceDirect

Signal Processing: Image Communication

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

Cubature Kalman filter-based chaotic synchronization and image encryption

Komeil Nosrati [a], Christos Volos [b,*], Asad Azemi [c]

[a] Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran
[b] Physics Department, Aristotle University of Thessaloniki, GR-54124, Greece
[c] Department of Electrical Engineering, Penn State University, USA

ARTICLE INFO

Keywords:
Chaos synchronization
Cubature Kalman filter
Secure communication
Image encryption

ABSTRACT

In this paper, a chaotic communication method based on the Cubature Kalman Filter (CKF) is presented. Using CKF, state estimation of a chaotic dynamical system and synchronization, in the presence of processing noise and measurement noise, are presented. The proposed method is then applied to a private secure communication setup, and an image encryption algorithm is introduced, where the original image is encoded by a chaotic state. Simulation results show that the original image is well masked in the cipher texts and is recovered successfully from the chaotic signals. Further, the cryptanalysis is conducted in detail through histogram, correlation of two adjacent pixels, differential analysis, information entropy, key and computational complexity analysis to demonstrate the high security, sensitivity and speed of the proposed encryption scheme.

1. Introduction

During the last two decades, there have been significant interests in using chaotic systems to secure communications. There are several features in these systems that make them so attractive in communication systems. Their noise-like broadband power spectra is a good candidate to remedy narrow-band effects such as frequency-selective fading or narrow-band disturbances. Also, dependency on initial conditions makes them more difficult to be predicted over a longer time interval. Even small changes in the initial conditions will lead to an exponential divergence of orbits which is particularly attractive in cryptography.

Moreover, chaotic signals are aperiodic in the sense that no state ever repeats itself. Chaotic output streams will be completely uncorrelated, and the auto-correlation of a chaotic signal has a large peak at zero and decays rapidly. Thus, a chaotic system shares many properties of a stochastic process, which are the basic requirements of the spread spectrum communications. Most of the work in this area has been focused on synchronization of chaotic systems to recover the information signals [1–9]. Pecora and Carroll [1] addressed the synchronization of chaotic system using a drive-response conception. Their idea was to use the output of the driving system to control the response system so that the trajectories of the response's outputs could synchronize those of drive system, and they oscillated in a synchronous manner.

Thereafter, many synchronization schemes have been developed such as inverse system approach [2], system approach [3], linear and nonlinear feedback control [4,5], and system decomposition approach [6]. There are also a number of research publications that have focused on the use of observer-based design approach to show that the synchronization problem of chaotic systems could be solved through observer design approach [7–9], in which only the input and output information of drive system are used to construct part or all of the state information of drive system.

In some research, Extended Kalman Filter (EKF), as an optimal observer [10], was applied to synchronization of chaotic systems, and synchronization was obtained of transmitter and receiver dynamics in case the receiver is given via an EKF driven by a noisy drive signal from the transmitter [11]. However, the main drawback of this filter is the error in function approximation since it uses first order Taylor series for approximating the nonlinearities. Therefore, the EKF is not applicable for many practical applications as it works well only in a mild nonlinear environment, and hence, can degrade the performance. For overcoming the drawbacks associated with the approximation errors, many alternatives to EKF have been offered. Unscented Kalman Filter (UKF) could improve upon the EKF for state estimation since linearization is avoided by an Unscented Transformation (UT), and at least second order accuracy is provided [12]. As a result, the UKF is

[*] Corresponding author.
E-mail address: chvolos@gmail.com (C. Volos).

http://dx.doi.org/10.1016/j.image.2017.06.005
Received 1 February 2017; Received in revised form 17 May 2017; Accepted 21 June 2017
Available online 28 June 2017
0923-5965/© 2017 Elsevier B.V. All rights reserved.

capable of estimating the posterior mean and covariance accurately to a high order compared with the EKF, and consequently, could be applied for the synchronization of the chaotic system [13].

The Cubature Kalman Filter (CKF) is another Gaussian filter that is applicable to nonlinear systems with a better estimation results than the EKF and the UKF, and the ability to solve a wider range of nonlinear problems [14]. Unlike the EKF, this filter does not require the evaluation of Jacobians during the estimation process, and therefore, avoids the possibility of divergence. Also, it provides superior estimation accuracy with minimal computational effort rather than the UKF. To the best of the author's knowledge, the CKF has not been considered to synchronization of chaotic systems which will be provided in this study.

Recently, chaos-based cryptography schemes have attracted more attention from researchers, and mainly was applied in encrypting the analog and digital signals, like sound waves, text messages, and so on [13,15,16]. Due to the special nature of an image and its special encoding features such as strong correlation between adjacent pixels and great capacity of data, image encryption is also considered as different applications from classical data encryption. There are many interesting proposals of image encryption based on chaotic systems in different ways such as total shuffling [17,18], bidirectional diffusion [19], circular substitution box [20], DNA encoding techniques [21,22], FPGA-based implementation with higher dimensional digital chaotic system (HDDCS) [23] and so on. However, there are a few research on image encryption based on chaos synchronization and its security analysis [24–28].

Based on the above-mentioned discussions, this paper considers a novel chaotic synchronization method and image encryption scheme, and pursues the following objectives:

1. Formulating three nonlinear Kalman filters (EKF, UKF and CKF) in a new state of the art to be compared in a simple way.
2. Synchronization of two chaotic systems in master slave configuration by the Cubature Kalman Filter for the first time.
3. Comparison of new CKF-based method of synchronization with other Kalman-based methods in performance, MSE, time execution and complexity.
4. Proposing an image encryption design based on new chaos synchronization method in a noisy environment.
5. Verifying the effectiveness of the presented scheme security based on cryptanalysis.

This paper is organized as follows: In Section 2, a brief review of chaotic systems is given, and Lorenz chaotic system is presented. Kalman filtering, principles and algorithms of EKF, UKF and CKF are presented in Section 3. The proposed chaos-based image encryption scheme is provided in Section 4. In Section 5, simulation results for a Lorenz chaotic system using EKF, UKF, and CKF are presented and compared. Image encryption using the proposed method is also presented in this section, and eventually, the cryptanalysis is conducted in detail to verify the high security, sensitivity and speed of the proposed encryption scheme.

2. Chaotic system

In this paper, the synchronization problem of a Lorenz chaotic system with additive noise using Cubature Kalman Filter is considered. The Lorenz system can be described by the following differential equations:

$$\begin{cases} \dfrac{dx_1}{dt} = -\sigma(x_1 - x_2), \\ \dfrac{dx_2}{dt} = -x_1x_2 + \rho x_1 - x_2, \\ \dfrac{dx_3}{dt} = x_1x_2 - \beta x_3. \end{cases} \tag{1}$$

When $\sigma = 10$, $\beta = \frac{8}{3}$ and $\rho = 25$, the dynamical system (1) behaves chaotically. In Fig. 1, the attractor of the chaotic Lorenz system for these parameters is plotted.

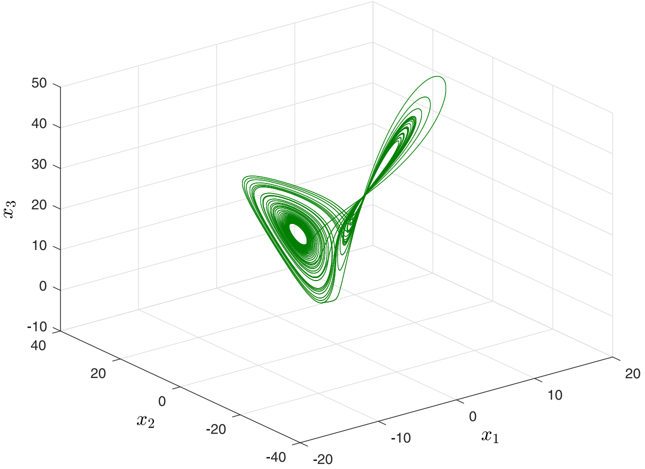

Fig. 1. Attractor of Lorenz dynamical system.

3. Kalman filter

Kalman filter, as an optimal state vector estimator, is a closed form solution to the Bayesian filtering equations for the filtering model, where the state-space model is defined by the pair of difference equations in discrete time as follows [29]:

$$Process\ equation: \qquad x_k = f(x_{k-1}) + w_{k-1} \tag{2a}$$

$$Measurement\ equation: \qquad y_k = h(x_k) + v_k \tag{2b}$$

where $x_k \in \mathbb{R}^n$ and $y_k \in \mathbb{R}^q$ are the state vector and the measurement at time k, respectively, process model $f : \mathbb{R}^n \to \mathbb{R}^n$ and measurement model $h : \mathbb{R}^n \to \mathbb{R}^q$ are some known functions of the class C^∞,[1] w_k and v_k are independent process and measurement Gaussian noise sequences with zero means and covariance Q_k and R_k, respectively. In the Bayesian filtering, the posterior distribution of the state provides a complete statistical description of the state at that time. By obtaining of a new measurement at time k, the old posterior distribution of the state will be updated at time $k-1$ in two basic steps:

1. Computing the predictive distribution equation (*time update*):

$$p(x_k|\{y_i\}_{i=1}^{k-1}) = \int_{\mathbb{R}^n} p(x_{k-1}|\{y_i\}_{i=1}^{k-1}) \times p(x_k|x_{k-1})\mathrm{d}x_{k-1}, \tag{3}$$

where $p(x_{k-1}|\{y_i\}_{i=1}^{k-1})$ is the old posterior distribution at time $k-1$ in which $\{y_i\}_{i=1}^{k-1}$ denotes the measurement sequence up to time $k-1$, and the prior distribution $p(x_k|x_{k-1})$ is obtained from (2a).

2. Computing the updated posterior distribution of the current state (*measurement update*):

$$p(x_k|\{y_i\}_{i=1}^{k}) = p(x_k|\{y_i\}_{i=1}^{k-1}, y_k) = \frac{1}{c_k}p(x_k|\{y_i\}_{i=1}^{k-1})p(y_k|x_k), \tag{4}$$

where the right hand side is derived using Bayes rule. $p(y_k|x_k)$ is the measurement Likelihood function obtained from (2b), and the normalizing constant c_k is given by

$$c_k = p(y_k|\{y_i\}_{i=1}^{k-1}) = \int_{\mathbb{R}^n} p(x_k|\{y_i\}_{i=1}^{k-1}) \times p(y_k|x_k)\mathrm{d}x_k. \tag{5}$$

The multidimensional integrals involved in (3) and (5) may often become harmful in high dimensional state space models, and the divergence may occur because of inaccurate or incomplete model, information loss in capturing the true evolving posterior distribution completely, high degree of nonlinearities and numerical errors. The

[1] The function f is said to be of class C^∞ if the derivatives $f', f'', \ldots, f^{(k)}, \ldots$ exist and are continuous for all orders.