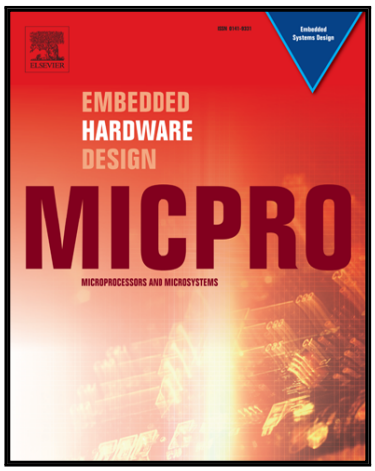

A portable embedded system for point-to-point secure signals transmission

M. Jiménez , M.E. Cano , O. Flores , J.C. Estrada

PII: S0141-9331(17)30577-X
DOI: 10.1016/j.micpro.2018.05.019
Reference: MICPRO 2700

To appear in: *Microprocessors and Microsystems*

Received date: 20 December 2017
Revised date: 25 April 2018
Accepted date: 31 May 2018

Please cite this article as: M. Jiménez , M.E. Cano , O. Flores , J.C. Estrada , A portable embedded system for point-to-point secure signals transmission, *Microprocessors and Microsystems* (2018), doi: 10.1016/j.micpro.2018.05.019

A portable embedded system for point-to-point secure signals transmission

M. Jiménez, M. E. Cano, O. Flores and J. C. Estrada
Centro Universitario de la Ciénega, Universidad de Guadalajara, Guadalajara, México

***Abstract*— In this work, an embedded system for point-to-point secure transmission of encrypted signals was developed. This portable system, which is also experimentally analyzed includes, includes a pair of digital signal controllers dsPIC33FJ128MC802 and the algorithm is based on the Rössler oscillator with constant and chaotic parameters. Therefore, the synchronization between both devices was analyzed via the measurement of the synchronization error and the transient time. The viability of the complete system was experimentally studied, by sending encrypted signals by wired and wireless methods from the master device to the slave, where these are decrypted. As the originally acquired signals show some contamination of white noise, the transmitted and decoded signals are filtered through a Kalman filter embedded in the same algorithm, reaching -8 dB of noise diminution approximately. Afterwards, the decoded signals are compared with the initial ones by the Pearson correlation coefficient. When a synchronization error is fixed at 1×10^{-5}, the experimental results exhibit transient times of 4.45 s and 2.69 min for the wired and wireless transmitting methods, respectively. However, as the estimated correlation coefficients are ranging in the interval $0.99963 < R <$ to 0.999999. Hence, the initial encrypted signal is entirely received by the slave device. The system is able to works in real-time, nevertheless, the determined sampling frequency is drastically diminished when the point-to-point communication is carried out via wireless**.

Keywords: **Chaos, dsPIC33FJ128MC802, Rössler attractor.**

1. INTRODUCTION

Chaos theory is a tool of informatics security that can be employed by the structuration of chaotic maps [1, 2]. These maps are useful for multiple applications, such as compression and encryption of several types of signals via hardware or software [3-7]. Additionally, chaotic synchronization is another technique to shield information, where two identical oscillating systems are coupled by a common signal. After a transitional period, both systems follow the same trajectory, converging in the same series of values [8-10]. This chaotic synchronization technique can be used to hack systems, detecting the secret cipher keys [11]. Many studies have focused on solving the vulnerability of chaotic synchronization, by combining several cryptographic techniques [12], iteratively varying the secret keys [13] or adding authentication methods [14].

The Rössler attractor [15] is one of the oscillating systems more commonly used to synchronize chaotic systems. **The synchronizing and stability of this kind of oscillators have been widely analyzed theoretically and experimentally by Pecora [8] and Pisarchik [9], then they have been employed in other previous works [12,14].** In the field of signal transmission, this can be handled to analogically transmit chaotic signals using a modulated chaotic oscillator [16]. Within the scope of the embed systems, the encoding of data via chaotic maps in a network of ZigBee digital transmitters has been successful, guaranteeing high security with low computing resources [17]. Likewise, employing Arduino technology, a logistic mapping was successfully performed to encrypt/decrypt signals modulated by a delta analogic system [18]. This system utilizes an external signal as an encryption key. Furthermore, a generator of chaotic random bits was designed employing an Arduino-board including an Atmel microcontroller [19]. This type of low-performance microcontroller has also been employed in instrumentation works, in order to develop digital chaotic sequence generators and modify the carrier signal of another transmitted signal, via the logistic map [20]. Another application was conducted to send and receive encrypted data using the chaotic generalized Henon map [21]. On the other hand, the microcontrollers of the PIC family have been successfully utilized in embedded systems based on chaos. For example, the PIC12F6F29 was employed to develop a source of digital chaotic signals [22]. With another more advanced (PIC18F4550), a chaotic oscillator was implemented. For this purpose, an algorithm to generate the Rössler and Chen oscillators separately was developed [23]. Even more, ColdFire technology has been used in embedded devices for encryption and real-time applications, in highly secure systems [24]. **Also, FPGA technology was recently used for applications of chaotic systems [25], which employs an elegant system (because it considers only one parameter) for the synchronization of two chaotic oscillators. This device is able to encrypt and decode images, exhibiting correlations from 0.1804 and up to 0.1952 between the chaotic and recovered images. Another interesting prototype using FPGA to transmit ciphered images (indoor range), using the Lorentz attractor was developed in [26]. In this device, only small circuits and RF transmitters (Xbee) are used, this is one of the few published systems that do not use a bulky PC.**