International Journal of Bifurcation and Chaos, Vol. 26, No. 8 (2016) 1650140 (15 pages)
© World Scientific Publishing Company
DOI: 10.1142/S0218127416501406

Message Embedded Chaotic Masking Synchronization Scheme Based on the Generalized Lorenz System and Its Security Analysis[*]

Sergej Čelikovský[†] and Volodymyr Lynnyk[‡]
Institute of Information Theory and Automation
of the Czech Academy of Sciences,
P.O. Box 18, Prague 8, 182 08, Czech Republic
[†]*celikovs@utia.cas.cz*
[‡]*volodymyr.lynnyk@utia.cas.cz*

Received March 2, 2016

This paper focuses on the design of the novel chaotic masking scheme via message embedded synchronization. A general class of the systems allowing the message embedded synchronization is presented here, moreover, it is shown that the generalized Lorenz system belongs to this class. Furthermore, the secure encryption scheme based on the message embedded synchronization is proposed. This scheme injects the embedded message into the dynamics of the transmitter as well, ensuring thereby synchronization with theoretically zero synchronization error. To ensure the security, the embedded message is a sum of the message and arbitrary bounded function of the internal transmitter states that is independent of the scalar synchronization signal. The hexadecimal alphabet will be used to form a ciphertext making chaotic dynamics of the transmitter even more complicated in comparison with the transmitter influenced just by the binary step-like function. All mentioned results and their security are tested and demonstrated by numerical experiments.

Keywords: Chaotic masking; generalized Lorenz system; message embedded synchronization.

1. Introduction

During recent decades, the idea to use chaotic systems in communication has been attracting many researchers [Pecora & Carroll, 1990; Parlitz *et al.*, 1992; Kocarev *et al.*, 1992; Cuomo & Oppenheim, 1993; Wu & Chua, 1993; Kocarev & Parlitz, 1995; Milanovic & Zaghloul, 1996; Lian & Liu, 2000; Fradkov *et al.*, 2000; Chen *et al.*, 2009; Kaddoum & Shokraneh, 2015; Fradkov *et al.*, 2015; Chen & Dong, 1998]. Famous features of the chaotic systems like strong dependence on the initial conditions, topological transitivity, wide spread spectrum of their signals, etc., directly suggested the idea of using chaotic systems to build up a new generation of the communication methods and to design the novel secure chaos-based communication schemes. Most of them are based on the synchronization of the chaotic systems [Materassi & Basso, 2008; Kocarev *et al.*, 1992; Pecora & Carroll, 1990; Kolumbán *et al.*, 1998]. Unfortunately the majority of the proposed methods are introduced without any cryptanalysis, they have rather weak security and they would be very likely broken later on [Li *et al.*, 2005; Li *et al.*, 2006; Perez & Cerdeira, 1995; Álvarez *et al.*, 2004; Yang *et al.*, 1998a; Short, 1994; Hu & Guo, 2008]. The use of the continuous-time chaotic systems for the encryption of the digital data has been studied briefly [Álvarez & Li, 2006;

[*]This work was supported by the Czech Science Foundation through the research Grant No. 13-20433S.

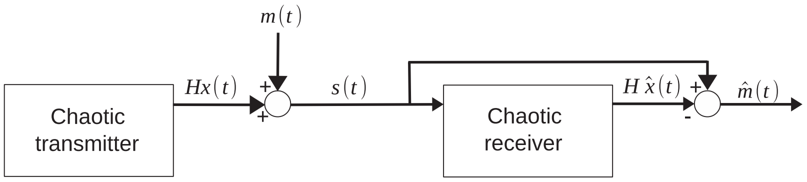


Fig. 1. Block diagram of the conventional (classical) chaotic masking scheme. Here, $m(t)$ is the message; $Hx(t)$ is the output chaotic signal of the transmitter; $s(t)$ is the transmitted signal; $H\hat{x}(t)$ is the output chaotic signal of the receiver; $\hat{m}(t)$ is the recovered message.

Dachselt & Schwarz, 2001; Kocarev, 2001] due to the prevalently used analogue chaotic masking [Alvarez-Ramirez *et al.*, 2002; Lian & Liu, 2000].

The purpose of this paper is to introduce yet another version of the chaotic masking scheme. It is based on the so-called message embedded synchronization of the continuous-time chaotic systems and it will be then used to transmit securely the digital data represented by the hexadecimal waveform. To explain the novelty of this concept, let us first classify the existing and newly introduced chaotic masking schemes:

- **Conventional (Classical) Chaotic Masking Schemes.** These schemes have been developed primarily for the analog communication [Kocarev *et al.*, 1992; Cuomo *et al.*, 1993; Cuomo & Oppenheim, 1993; Lian & Liu, 2000; Liang *et al.*, 2012]. Their main idea is to mask a low-level message signal adding to it a suitable chaotic signal. The diagram of this kind of communication schemes is shown in Fig. 1.

- **Improved Chaotic Masking Schemes.** These schemes [Wu & Chua, 1993; Milanovic & Zaghloul, 1996; Kocarev & Parlitz, 1995; Liao & Huang, 1999; Chen, 2010] use a message signal to modulate the dynamics of the transmitter. More precisely, they combine a conventional chaotic masking algorithm and a chaotic modulation algorithm. The transmitted signal is the sum of the information-bearing signal and the output of the chaotic transmitter. Dynamics of the transmitter is influenced by the same information-bearing signal. The diagram of this kind of the communication schemes is shown in Fig. 2.

- **Message Embedded Chaotic Masking Scheme (MECHMS).** This scheme is introduced in the current paper and it uses the embedded message signal to modulate the dynamics of the transmitter equations to achieve the so-called message embedded synchronization. The diagram of this communication scheme is shown in Fig. 3.

As already noted, the main goal of the current paper is to introduce the chaotic masking scheme based on the message embedded synchronization. Furthermore, the class of systems where the above scheme is possible is characterized and it is shown that the well-known generalized Lorenz system (GLS) [Čelikovský & Vaněček, 1994; Čelikovský & Chen, 2002, 2005a, 2005b] belongs to that class. Thanks to that, the MECHMS will be implemented in detail for the GLS and its security aspects will be analyzed. Finally, it will be shown that it is possible to use this newly proposed chaotic masking scheme to encrypt the digital information.

Digital information secure encryption using continuous-time chaotic systems was already studied in [Čelikovský & Lynnyk, 2012; Lynnyk & Čelikovský, 2010], where the so-called Desynchronization Chaos Shift Keying (DECSK) method was introduced and its security analyzed in detail.

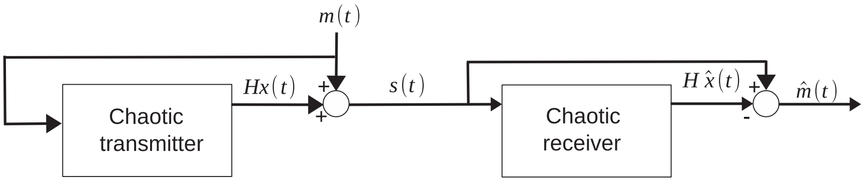


Fig. 2. Block diagram of the improved chaotic masking scheme. Here, $m(t)$ is the message; $Hx(t)$ is the output chaotic signal of the transmitter. Internal dynamics of the chaotic transmitter is influenced by $m(t)$; $s(t)$ is the transmitted signal; $H\hat{x}(t)$ is the output chaotic signal of the receiver; $\hat{m}(t)$ is the recovered message.

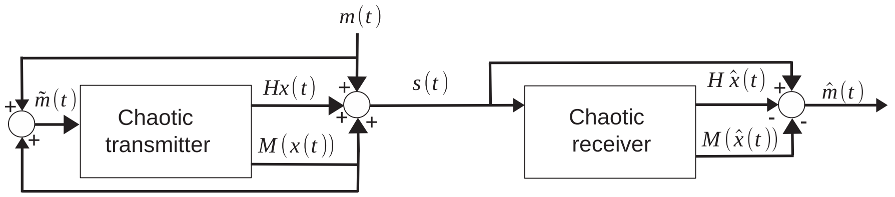


Fig. 3. Block diagram of the MECHMS. Here, $m(t)$ is the message; $Hx(t)$ is the output chaotic signal of the transmitter; $M(x(t))$ is an arbitrary bounded function of the transmitter internal states $x(t)$. Internal dynamics of the chaotic transmitter is influenced by the embedded message $\tilde{m}(t)$; $s(t)$ is the transmitted signal; $H\hat{x}(t)$ is the output chaotic signal of the receiver; $M(\hat{x}(t))$ is an arbitrary bounded function of the receiver internal states $\hat{x}(t)$; $\hat{m}(t)$ is the recovered message.

DECSK method uses the transmitter which consists of the chaotic system affected by the selected parameter varying dependingly on the bit to be encrypted (“0” or “1”). The receiver consists of two perfectly synchronized transmitter copies corresponding to those different values of that selected parameter. The transmitter sends a short signal segment generated by one of those parameter values corresponding to the bit value to be sent. It turns out that even a quite short time segment is sufficient to have one of the receiver systems quickly *desynchronized*, which enables to detect the encrypted bit. To make that method realistic, the second derivative error detection was used ensuring that even two iterations only are sufficient to detect the desynchronization. All these ideas were implemented in detail for the GLS. Later on, an introductory study on how to use the GLS to encrypt the digital data using the chaotic masking was presented in [Čelikovský & Lynnyk, 2013]. Nevertheless, as it will be discussed later on, the security of this method is subject to some drawbacks.

The present paper thereby continues this line of the research and uses the GLS to design the message embedded chaotic masking encryption scheme capable to transmit the digital information. To do so, the embedded message signal $\tilde{m}(t)$ is added to the chaotic output generated by the chaotic oscillator whose dynamics depends on the same embedded message $\tilde{m}(t) = m(t) + \mathcal{M}(x(t))$. Here, $\mathcal{M}(x(t))$ is arbitrary bounded function of the transmitter internal state $x(t)$, which should be independent of the transmitted scalar synchronizing signal. Furthermore, it will be shown that it is possible to use this property to implement the chaotic masking for the digital signal modulation (information-bearing waveform). Suitable waveform is to be selected, namely, the hexadecimal digital waveform will be used. This waveform is smoothed by the integration procedure as the nonsmooth message visibly affects the second derivative of the transmitted signal being thereby easily decryptable. Such a signal step-like function may have a small amplitude which makes the integrated signal even more undetectable, unless one has at his/her disposal the correct carrying chaotic signal to subtract it from the encrypted message. All these properties provide a firm basis for the successful security analysis of the newly proposed method.

The rest of the paper is organized as follows. The next section briefly repeats some known facts about the GLS. Section 3 introduces the MECHMS for the GLS, while its security analysis is provided by Sec. 4. Numerical experiments are collected in Sec. 5. The final section draws the conclusions and gives some outlooks for future research.

2. The GLS and Its Synchronization

Definition 2.1. The following nonlinear system in R^3 is called as the generalized Lorenz system (GLS):

$$\dot{x} = \begin{bmatrix} A & 0 \\ 0 & \lambda_3 \end{bmatrix} x + \begin{bmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{bmatrix}, \quad A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}. \tag{1}$$

Here, $x = [x_1, x_2, x_3]^\top$, $\lambda_3 \in R$, and A has eigenvalues $\lambda_1, \lambda_2 \in R$, such that

$$-\lambda_2 > \lambda_1 > -\lambda_3 > 0. \tag{2}$$

The inequality (2) goes back to the well-known Shilnikov’s chaos analysis near the homoclinicity and it can be viewed as the necessary condition for the chaos existence, see a more detailed discussion in [Čelikovský & Chen, 2002]. GLS is said to be *nontrivial* if it has at least one solution that goes neither to zero, nor to infinity, nor to a limit cycle. The following result, enabling the efficient synthesis of a rich variety of the chaotic behaviors for the GLS, was obtained in [Čelikovský & Chen, 2002].

Theorem 2.2 [Čelikovský & Chen, 2002]. *For the nontrivial GLS (1)–(2), there exists a nonsingular linear change of coordinates $z = Tx$, which takes (1) into the following* generalized Lorenz canonical form:

$$\dot{z} = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} z + cz \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 1 & \tau & 0 \end{bmatrix} z, \qquad (3)$$

where $z = [z_1, z_2, z_3]^\top$, $c = [1, -1, 0]$ and $\tau \in (-1, \infty)$.

Actually, the parameter τ plays an important role being the single scalar "nonlinear bifurcation parameter", while the remaining parameters have only a qualitative influence being the eigenvalues of the approximate linearization of the GLS at the origin. These qualitative parameters are required to satisfy the robust condition (2) only, so that a fine tuning may be done using the single scalar parameter τ only. In [Čelikovský, 2004], the GLS was further extended to the so-called hyperbolic-type generalized Lorenz system (HGLS) which has the same canonical form as (4) but with $\tau \in (\infty, -1)$. In such a way, the parameter range to be used in the encryption can be extended even more. In [Čelikovský & Chen, 2005a], the complete and nice classification of all related systems is given showing that many previously introduced classes are actually particular cases of the GLS or the HGLS.

Synchronization of two or more copies of the GLS is based on yet another canonical form, the so-called *observer canonical form of the GLS*, provided by the following theorem.

Theorem 2.3 [Čelikovský & Chen, 2005b]. *Both the nontrivial GLS (1) and its canonical form (3) are state equivalent to the following form, called in the sequel as the observer canonical form of the GLS:*

$$\frac{\mathrm{d}\eta}{\mathrm{d}t} = \begin{bmatrix} (\lambda_1 + \lambda_2)\eta_1 + \eta_2 \\ -\eta_1 \left[\lambda_1\lambda_2 + (\lambda_1 - \lambda_2)\eta_3 + \dfrac{(\tau+1)\eta_1^2}{2} \right] \\ \lambda_3\eta_3 + K(\tau)\eta_1^2 \end{bmatrix},$$

$$K(\tau) = \frac{\lambda_3(\tau+1) - 2\tau\lambda_1 - 2\lambda_2}{2(\lambda_1 - \lambda_2)}, \qquad (4)$$

where $\eta = [\eta_1, \eta_2, \eta_3]^\top$ and the state equivalence coordinate change and its inverse are, correspondingly:

$$\eta = \left[z_1 - z_2, \lambda_1 z_2 - \lambda_2 z_1, z_3 - \frac{(\tau+1)(z_1 - z_2)^2}{2(\lambda_1 - \lambda_2)} \right]^\top, \qquad (5)$$

$$z = \left[\frac{\lambda_1\eta_1 + \eta_2}{\lambda_1 - \lambda_2}, \frac{\lambda_2\eta_1 + \eta_2}{\lambda_1 - \lambda_2}, \eta_3 + \frac{(\tau+1)\eta_1^2}{2(\lambda_1 - \lambda_2)} \right]^\top. \qquad (6)$$

Indeed, the above observer canonical form, when viewing $\eta_1 = x_1 = z_1 - z_2$ as the output, is very similar to the form linearizable by output injection. As a consequence, the following observer-based synchronization of two copies of the GLS is possible.

Theorem 2.4 [Čelikovský & Chen, 2005b]. *Consider system (4) with the output η_1 and its uniformly bounded trajectory $\eta(t)$, $t \geq t_0$. Further, consider the following system having the input η_1^m and the state $\hat{\eta} = (\hat{\eta}_1, \hat{\eta}_2, \hat{\eta}_3)^\top$:*

$$\frac{\mathrm{d}\hat{\eta}}{\mathrm{d}t} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta} + \begin{bmatrix} \lambda_1 + \lambda_2 - l_1 \\ -\lambda_1\lambda_2 - l_2 \\ 0 \end{bmatrix} \eta_1^m + \begin{bmatrix} 0 \\ -(\lambda_1 - \lambda_2)\eta_1^m\hat{\eta}_3 - \left(\dfrac{1}{2}\right)(\tau+1)(\eta_1^m)^3 \\ K(\tau)(\eta_1^m)^2 \end{bmatrix}, \qquad (7)$$

where $l_{1,2} < 0$. For all $\varepsilon \geq 0$, assume $|\eta_1(t) - \eta_1^m(t)| \leq \varepsilon$. Then, it holds exponentially in time that

$$\overline{\lim_{t\to\infty}} \|\eta(t) - \hat{\eta}(t)\| \leq C\varepsilon,$$

for a constant $C > 0$. In particular, for $\eta_1^m \equiv \eta_1$, (7) is the global exponential observer of system (4).

Proofs of Theorems 2.3–2.4 may be found in [Čelikovský & Chen, 2005b]. In the sequel, system (4) will be called as the master while (7) as the slave. Theorem 2.4 can be used for the conventional chaotic masking in the sense of [Cuomo & Oppenheim, 1993] (see Fig. 1). Here, the message to be masked is added to the synchronizing signal which corrupts the synchronization, as claimed by Theorem 2.4, where synchronization error does not go to zero completely. Namely, $\eta_1^m = \eta_1 + m(t)$, where $m(t)$ is the signal representing message to be masked, i.e.

$$\overline{\lim_{t\to\infty}} \|\eta(t) - \hat{\eta}(t)\| \leq C\|m(t)\|.$$

This drawback will be removed in the next section using the message embedded synchronization.

3. Message Embedded Synchronization and Its Use for Chaotic Masking

The message embedded synchronization is proposed in this section. It will be used for the chaotic masking later on. Characterize first a more general class of the systems where the message embedded synchronization is possible. Namely, consider the nonlinear system of the form

$$\begin{bmatrix}\dot{x}^1\\ \dot{x}^2\end{bmatrix} = \begin{bmatrix}F_1 & 0\\ 0 & F_2\end{bmatrix}\begin{bmatrix}x^1\\ x^2\end{bmatrix} + \begin{bmatrix}\varphi^1(Hx^1, x^2)\\ \varphi^2(Hx^1)\end{bmatrix}, \tag{8}$$

where $\begin{bmatrix}x^1\\ x^2\end{bmatrix} = x \in R^n$, $x^1 \in R^{n_1}$, $x^2 \in R^{n_2}$, $n_1 + n_2 = n$, F is $(n \times n)$ matrix, H is $(1 \times n_1)$ matrix, F_1 is $(n_1 \times n_1)$ matrix, F_2 is $(n_2 \times n_2)$ matrix. Further, suppose that (F_1, H) is a detectable pair, F_2 is Hurwitz and nonlinear functions φ^1, φ^2 are such that $\varphi^1 : R^{n_2+1} \to R^{n_1}$, $\varphi^2 : R \to R^{n_2}$. The synchronized copy of (8) can be obtained using the scalar synchronizing signal $Hx(t)$ as follows

$$\begin{bmatrix}\dot{y}^1\\ \dot{y}^2\end{bmatrix} = \begin{bmatrix}F_1 & 0\\ 0 & F_2\end{bmatrix}\begin{bmatrix}y^1\\ y^2\end{bmatrix} + \begin{bmatrix}\varphi^1(Hx^1, y^2)\\ \varphi^2(Hx^1)\end{bmatrix} + \begin{bmatrix}L_1H(y^1 - x^1)\\ 0\end{bmatrix}. \tag{9}$$

Here, L_1 is $(n_1 \times 1)$ matrix such that $F_1 + L_1H$ is Hurwitz and $y^1 \in R^{n_1}$, $y^2 \in R^{n_2}$. Indeed, define $e = (e^1, e^2)^\top = (y^1 - x^1, y^2 - x^2)$. Subtracting (8) from (9) gives

$$\begin{bmatrix}\dot{e}^1\\ \dot{e}^2\end{bmatrix} = \begin{bmatrix}F_1 + L_1H & 0\\ 0 & F_2\end{bmatrix}\begin{bmatrix}e^1\\ e^2\end{bmatrix} + \begin{bmatrix}\varphi^1(Hx^1, y^2) - \varphi^1(Hx^1, x^2)\\ 0\end{bmatrix}. \tag{10}$$

Notice, that $e^2 \to 0$ exponentially since F_2 is Hurwitz. Assuming that the synchronization signal $Hx(t)$ of (8) is bounded, one concludes easily that

$$\varphi^1(H(x(t)), y^2(t)) - \varphi^1(H(x(t)), x^2(t)) \to 0$$

exponentially as $t \to \infty$. Therefore, by Lemma 9.1 of [Khalil, 2002] $e^1(t) \to 0$ exponentially as $t \to \infty$, since $F_1 + L_1H$ is Hurwitz. Summarizing, $e(t) \to 0$ exponentially as $t \to \infty$ and therefore (8) and (9) are exponentially synchronized.

3.1. *Message embedded chaotic masking scheme*

The previously introduced synchronization scheme is adapted here for the case when synchronizing scalar channel is to carry the additive message to be masked as well. Let $\tilde{m}(t)$ denote the masked and thereby securely encrypted message to be transmitted. More precisely, the signal $Hx^1 + \tilde{m}(t)$ will be transmitted through the public scalar channel. To do so, consider the following system

$$\begin{bmatrix}\dot{x}^1\\ \dot{x}^2\end{bmatrix} = \begin{bmatrix}F_1 & 0\\ 0 & F_2\end{bmatrix}\begin{bmatrix}x^1\\ x^2\end{bmatrix} + \begin{bmatrix}\varphi^1(Hx^1 + \tilde{m}(t), x^2)\\ \varphi^2(Hx^1 + \tilde{m}(t))\end{bmatrix} - \begin{bmatrix}L_1\tilde{m}(t)\\ 0\end{bmatrix} \tag{11}$$

and its synchronized copy

$$\begin{bmatrix}\dot{y}^1\\ \dot{y}^2\end{bmatrix} = \begin{bmatrix}F_1 & 0\\ 0 & F_2\end{bmatrix}\begin{bmatrix}y^1\\ y^2\end{bmatrix} + \begin{bmatrix}\varphi^1(Hx^1 + \tilde{m}(t), y^2)\\ \varphi^2(Hx^1 + \tilde{m}(t))\end{bmatrix} + \begin{bmatrix}L_1H\\ 0\end{bmatrix}y^1 - \begin{bmatrix}L_1(Hx^1 + \tilde{m}(t))\\ 0\end{bmatrix}. \tag{12}$$

Indeed, define

$$e = (e^1, e^2)^\top = (y^1 - x^1, y^2 - x^2).$$

Subtracting (11) from (12) gives

$$\begin{bmatrix}\dot{e}^1\\ \dot{e}^2\end{bmatrix} = \begin{bmatrix}F_1 + L_1H & 0\\ 0 & F_2\end{bmatrix}\begin{bmatrix}e^1\\ e^2\end{bmatrix} + \begin{bmatrix}\varphi^1(Hx^1 + \tilde{m}(t), y^2) - \varphi^1(Hx^1 + \tilde{m}(t), x^2)\\ 0\end{bmatrix}. \tag{13}$$

Assuming that the synchronization signal $Hx + \tilde{m}(t)$ is bounded, one has again that $e \to 0$ exponentially as $t \to \infty$.

The message embedded chaotic masking scheme (MECHMS) can be described as follows. Let $m(t)$ be the message to be encrypted and transmitted, e.g. the plaintext waveform representation. Then $\tilde{m}(t) = m(t) + \mathcal{M}(x(t))$ is the encrypted message to be embedded and transmitted. Here, $\mathcal{M}(x(t))$ is an arbitrary bounded function of the internal components of the state $x(t)$, which should be independent from the scalar synchronizing signal Hx^1. Using (11), one generates the transmitted signal as

$$s(t) = \tilde{m}(t) + Hx^1(t) = m(t) + Hx^1 + \mathcal{M}(x(t)).$$

Recovered message $\hat{m}(t)$ will be taken as $\hat{m}(t) = s(t) - Hy^1(t) - \mathcal{M}(y(t))$. Note, that $\hat{m}(t) - m(t) = H(x^1(t) - y^1(t)) + \mathcal{M}(x(t)) - \mathcal{M}(y(t))$, i.e. $\hat{m}(t) - m(t) \to 0$ exponentially as $t \to \infty$.

Remark 3.1. Notice, that the observer canonical form of the GLS (4) is the system in the form (8), with

$$F_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

$$F_2 = [\lambda_3], \quad H = [1, 0],$$

$$x^1 = \begin{bmatrix} \eta_1 \\ \eta_2 \end{bmatrix}, \quad x^2 = [\eta_3],$$

$$\varphi^1 = \begin{bmatrix} (\lambda_1 + \lambda_2)\eta_1 \\ -\lambda_1\lambda_2\eta_1 - (\lambda_1 - \lambda_2)\eta_1\eta_3 - \dfrac{(\tau+1)\eta_1^3}{2} \end{bmatrix},$$

$$\varphi^2 = K(\tau)\eta_1^2.$$

As a consequence, the GLS in its observer canonical form can be used to implement the MECHMS. To be more specific, the transmitter of the GLS implementation of the MECHMS has the following form

$$\frac{\mathrm{d}\eta}{\mathrm{d}t} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \eta - \begin{bmatrix} l_1 \\ l_2 \\ 0 \end{bmatrix} \tilde{m}(t) + \begin{bmatrix} (\lambda_1 + \lambda_2)(\eta_1 + \tilde{m}(t)) \\ -(\eta_1 + \tilde{m}(t)) \left[\lambda_1\lambda_2 + (\lambda_1 - \lambda_2)\eta_3 + \dfrac{(\tau+1)(\eta_1 + \tilde{m}(t))^2}{2} \right] \\ K(\tau)(\eta_1 + \tilde{m}(t))^2 \end{bmatrix}, \tag{14}$$

$$K(\tau) = \frac{\lambda_3(\tau+1) - 2\tau\lambda_1 - 2\lambda_2}{2(\lambda_1 - \lambda_2)}, \quad \eta = [\eta_1, \eta_2, \eta_3]^\top. \tag{15}$$

The corresponding receiver can be constructed as follows

$$\frac{\mathrm{d}\hat{\eta}}{\mathrm{d}t} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta} + \begin{bmatrix} l_1 \\ l_2 \\ 0 \end{bmatrix} \hat{\eta}_1 - \begin{bmatrix} l_1 \\ l_2 \\ 0 \end{bmatrix} (\eta_1 + \tilde{m}(t)) + \begin{bmatrix} (\lambda_1 + \lambda_2)(\eta_1 + \tilde{m}(t)) \\ -(\eta_1 + \tilde{m}(t)) \left[\lambda_1\lambda_2 + (\lambda_1 - \lambda_2)\hat{\eta}_3 + \dfrac{(\tau+1)(\eta_1 + \tilde{m}(t))^2}{2} \right] \\ K(\tau)(\eta_1 + \tilde{m}(t))^2 \end{bmatrix}, \tag{16}$$

where $\hat{\eta} = [\hat{\eta}_1, \hat{\eta}_2, \hat{\eta}_3]^\top$, $K(\tau)$ is described by Eq. (15) and $\eta_1 + \tilde{m}(t)$ is the synchronization signal received from the transmitter via the public channel. Notice, that the amplitude of the message embedded signal $\tilde{m}(t)$ is much smaller than the magnitude of $\eta_1(t)$ and in our numerical experiments[1] it is equal to $\approx \pm 10^{-2}$.

4. Security Analysis of the MECHMS

Following [Álvarez & Li, 2006], we will analyze here whether the proposed GLS implementation of the MECHMS used as a cryptosystem can be broken by the chaos-specific attacks.

[1] MATLAB-SIMULINK ode4 Runge–Kutta procedure with the fixed step size equal to 10^{-3} is being used throughout the paper.

4.1. *Message signal extraction*

As a matter of fact, the MECHMS is the digital chaotic cipher implemented via the GLS to transmit securely the digital information. Some kinds of the chaos-specific attacks proposed in the literature have broken many analogue chaotic ciphers, but they are not useful enough against the digital chaotic ciphers. Message signal extraction methods, like the power spectral analysis proposed in [Álvarez *et al.*, 2004; Yang *et al.*, 1998a] and the return-map analysis introduced in [Li *et al.*, 2006; Perez & Cerdeira, 1995; Yang *et al.*, 1998b], are usually performed without any knowledge of the specific structure of the chaotic system used for the message encryption. Furthermore, the power analysis attack is more efficient, since it does not require any knowledge about the structure of the chaotic system used in the transmitter of the cryptosystem. Both these methods can be applied to extract the message signal if the latter is the periodic signal or it consists of periodic frames within the duration long enough. The MECHMS for the GLS is resistive against both kinds of the above attacks as its ciphertext is a digital signal, whose waveform is dependent on the plaintext which affects a ciphertext during each iteration of the computation of the trajectory of the chaotic system in the transmitter. Even if the GLS has some periodic frames, these frames are useless for the intruder, because a single periodic frame has ≈ 2 sec length[2] and each point on the ciphertext waveform represents a bit of the encrypted plaintext. Čelikovský and Lynnyk [2012] provides the security analysis of the DECSK encryption method [Čelikovský *et al.*, 2006] based on the GLS via the power and the return-map analysis. Both these methods are uneffective against the DECSK digital cipher and since the MECHMS has a similar structure of the chaotic generator based on the GLS, one can assume that the MECHMS is cryptographically resistant against the power and the return-map analysis as well.

4.2. *Key space*

The GLS has three initial values and four control parameters. Every algorithm used for the secure encryption must have the key space cardinality of at least 2^{128} to oppose the brute force attack. As the secret key, the combination of the initial values and the bifurcation parameter τ, both with the double precision is proposed here. The key is sensitive to differences equal to or larger than 10^{-14}. Therefore, the total key size is equal to $10^{14} \cdot 10^{14} \cdot 10^{14} \approx 2^{140}$, that makes this secure method resistive against the brute force attack. The key space may be extended using the parameters λ_1, λ_2, λ_3 and the periodical switching of the bifurcation parameter τ, if necessary.

4.3. *Parameter and state estimation of the MECHMS*

As noticed in [Wang *et al.*, 2004], many secure communication schemes based on the chaotic dynamics are not sensitive enough to the parameter mismatch, therefore the intruder can estimate the bifurcation parameter used in the transmitter via approximation of the parameter values. Many methods of the parameter estimation were introduced during the last two decades. Direct calculation of the parameters from the short piece of ciphertext was introduced for the Lorenz chaotic system in [Vaidya & Angadi, 2003] and studied in detail for Chua's circuit in [Liu *et al.*, 2004]. Evolutionary algorithms [Zelinka *et al.*, 2010] were intensively studied both for the chaos synthesis and the parameter identification in the chaotic systems [Chang *et al.*, 2008]. Estimation of the parameters of the transmitter in the Chaos Shift Keying (CSK) scheme [Dedieu *et al.*, 1993] via the adaptation algorithm was provided by the standard gradient (or speed-gradient) techniques in [Fradkov *et al.*, 2000]. State and parameter estimation based on the adaptive observers can be found in [Zhang, 2002; Tyukin *et al.*, 2013; Besancon, 2000]. It was shown in [Liang *et al.*, 2008] that the states of the GLS with unknown bifurcation parameter, used in the secure synchronization proposed in [Čelikovský & Chen, 2005b], can be estimated by the adaptive observer introduced in [Zhang, 2002]. This adaptive observer can be therefore used for the state and bifurcation parameter estimation of the improved chaotic masking synchronization scheme using the GLS. Nevertheless, the quite long time period of the constant unknown parameter value is necessary, so that one can avoid such an attack by reasonable frequent change of the value of τ.

[2] That corresponds to 2000 iterations, since the fixed step size is equal to 10^{-3} in the presented numerical simulations.

To be specific, rewrite first system (4) as follows:

$$\frac{\mathrm{d}\eta}{\mathrm{d}t} = \begin{bmatrix} \lambda_1+\lambda_2 & 1 & 0 \\ -\lambda_1\lambda_2 & 0 & -(\lambda_1-\lambda_2)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix}\eta + \begin{bmatrix} 0 \\ -\dfrac{1}{2}\eta_1^3 \\ K_1\eta_1^2 \end{bmatrix} + \begin{bmatrix} 0 \\ -\dfrac{1}{2}\eta_1^3 \\ K_2\eta_1^2 \end{bmatrix}\tau, \tag{17}$$

where $K_1 = \frac{\lambda_3-2\lambda_2}{2(\lambda_1-\lambda_2)}$, $K_2 = \frac{\lambda_3-2\lambda_1}{2(\lambda_1-\lambda_2)}$, $\eta = [\eta_1, \eta_2, \eta_3]^\top$. Adaptive observer of [Zhang, 2002] for system (17) can be then constructed in the following way:

$$\frac{\mathrm{d}\hat{\eta}}{\mathrm{d}t} = \begin{bmatrix} \lambda_1+\lambda_2 & 1 & 0 \\ -\lambda_1\lambda_2 & 0 & -(\lambda_1-\lambda_2)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix}\hat{\eta} + \begin{bmatrix} l_1 & 0 & 0 \\ l_2 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}(\hat{\eta}-\eta) + \begin{bmatrix} 0 \\ -\dfrac{1}{2}\eta_1^3 \\ K_1\eta_1^2 \end{bmatrix} + \begin{bmatrix} 0 \\ -\dfrac{1}{2}\eta_1^3 \\ K_2\eta_1^2 \end{bmatrix}\hat{\tau} + \Upsilon(t)\dot{\hat{\tau}}, \tag{18}$$

$$\dot{\hat{\tau}} = -\Upsilon^\top(t)C^\top C(\hat{\eta}-\eta), \tag{19}$$

$$\dot{\Upsilon}(t) = \begin{bmatrix} \lambda_1+\lambda_2+l_1 & 1 & 0 \\ -\lambda_1\lambda_2+l_2 & 0 & -(\lambda_1-\lambda_2)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix}\Upsilon(t) + \begin{bmatrix} 0 \\ -\dfrac{1}{2}\eta_1^3 \\ K_2\eta_1^2 \end{bmatrix}, \tag{20}$$

where $\hat{\eta} = [\hat{\eta}_1, \hat{\eta}_2, \hat{\eta}_3]^\top$, $K_1 = \frac{\lambda_3-2\lambda_2}{2(\lambda_1-\lambda_2)}$, $K_2 = \frac{\lambda_3-2\lambda_1}{2(\lambda_1-\lambda_2)}$, $C = [1, 0, 0]$, and $l_i < 0$, $i = 1, 2$, are such that the matrix

$$L = \begin{bmatrix} \lambda_1+\lambda_2+l_1 & 1 \\ -\lambda_1\lambda_2+l_2 & 0 \end{bmatrix} \tag{21}$$

is Hurwitz. The synchronization between (17) and (18) is achieved if $\lim_{t\to\infty}|\eta(t) - \hat{\eta}(t)| = 0$, which means that (18) is the asymptotically stable observer of (17).

The observer error $e := (\hat{\eta} - \eta)$ has the dynamics

$$\dot{e} = \begin{bmatrix} \lambda_1+\lambda_2+l_1 & 1 & 0 \\ -\lambda_1\lambda_2+l_2 & 0 & -(\lambda_1-\lambda_2)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix} e + \begin{bmatrix} 0 \\ -\dfrac{1}{2}\eta_1^3 \\ K_2\eta_1^2 \end{bmatrix}\varepsilon - \Upsilon(t)\Upsilon^\top(t)\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} e_1. \tag{22}$$

In the sequel, denote the error of the bifurcation parameter as follows:

$$\varepsilon = \hat{\tau} - \tau. \tag{23}$$

Obviously, it holds

$$\dot{\varepsilon} = \dot{\hat{\tau}} = -\Upsilon_1(t)e_1. \tag{24}$$

Further, introduce the combined error variable $\bar{e}$ as follows

$$\bar{e} = e - \Upsilon(t)\varepsilon, \tag{25}$$

then

$$e = \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix} = \begin{bmatrix} \bar{e}_1 \\ \bar{e}_2 \\ \bar{e}_3 \end{bmatrix} + \begin{bmatrix} \Upsilon_1(t) \\ \Upsilon_2(t) \\ \Upsilon_3(t) \end{bmatrix}\varepsilon \tag{26}$$

and

$$e_1 = \bar{e}_1 + \Upsilon_1(t)\varepsilon. \tag{27}$$

Using the system equation (17) and observer equations (18)–(20) gives

$$\begin{aligned} \dot{\bar{e}} &= \dot{e} - \Upsilon(t)\dot{\varepsilon} - \dot{\Upsilon}(t)\varepsilon \\ &= \begin{bmatrix} \lambda_1+\lambda_2+l_1 & 1 & 0 \\ -\lambda_1\lambda_2+l_2 & 0 & -(\lambda_1-\lambda_2)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix}\bar{e}. \end{aligned} \tag{28}$$

Moreover, (24) becomes

$$\dot{\varepsilon} = -\Upsilon_1(t)(\bar{e}_1 + \Upsilon_1\varepsilon) = -\Upsilon_1^2(t)\varepsilon - \Upsilon_1(t)\bar{e}_1. \tag{29}$$

Summarizing, by (28) one has that $\bar{e} \to 0$ as $t \to \infty$ due to the fact that the matrix (21) is Hurwitz and $\lambda_3 < 0$. Moreover, if $\Upsilon_1^2(t)$ is persistently exciting then $\varepsilon \to 0$ as $t \to \infty$, too. Therefore by (26) $e \to 0$ as $t \to \infty$ and one has both that $\hat{\eta} \to \eta$ and $\hat{\tau} \to \tau$ as

$t \to \infty$. Adaptive observer (18) can be used for the estimation of the bifurcation parameter τ and, consequently, to synchronize two GLSs without parameter τ knowledge provided unknown τ is constant for a suitably long time period. The corresponding numerical results will be described in Sec. 5.4 later on.

5. Numerical Experiments

In this section, the numerical simulations of the various chaotic masking secure communication schemes based on the GLS are demonstrated. The main goal of this section is to demonstrate the effectiveness of the MECHMS (see Fig. 3) in comparison to the improved masking scheme (see Fig. 2) applied to the secure communication. Notice, that the constant bifurcation parameter τ and the initial conditions of the transmitter in improved chaotic masking scheme can be estimated after a certain time period by the adaptive observer (18). Therefore, for more security of the MECHMS, the value of the bifurcation parameter τ will be changed every 1024 iterations (≈ 1 sec). Moreover, the ciphertext of the chaotic masking embedded synchronization method consists of reduced values of the scalar signal η_1 with only eight digits after the decimal point (the numerical experiments with seven digits after the decimal point work quite well, too) and the message embedded signal depends on the reduced value of η_3.

5.1. *Hexadecimal numeral system*

Each hexadecimal digit represents four binary digits (bits) and the primary use of hexadecimal notation is a human-friendly representation of binary-coded values in computing. Hexadecimal digits are also commonly used to represent the computer memory addresses [Borowik *et al.*, 2012]. One hexadecimal digit represents a nibble, which is half of a byte (8 bits). Earlier, in [Čelikovský & Lynnyk, 2006] it was shown that using the multialphabet, it is possible to increase the security and the bit rate in the DECSK communication scheme. Another goal of using the hexadecimal numerical system is that the behavior of the transmitter will be changing according to 16 different chaotic systems in comparison to binary digits use relying on two different chaotic systems only. Table 1 describes the values of the low-level signal with their binary and hexadecimal code representations used in the numerical simulations within the paper.

5.2. *Relation between security of the MECHMS and the signal form of the encrypted message*

Čelikovský and Lynnyk [2013] illustrated the application of the chaotic masking scheme based on the GLS for the encryption and the decryption of the information represented by the binary step-like function. The amplitude of the used binary step-like function expressing the original message $m(t)$ was much smaller than the amplitude of the signal generated by the chaotic system used in the transmitter ("0" = 0, "1" = 0.00001). During the preparation of this paper the detailed analysis of the GLS-based improved chaotic masking scheme shown in Fig. 2 has been performed. It has been revealed that the low-level binary message can be decrypted directly from the openly transmitted ciphertext by the calculation of its second derivation. In the MECHMS the transformation of the original message by its integration before the injection into the transmitter chaotic system was used. Therefore, the transformed message is smoother than the original message and it eliminates the possibility of the decryption of the original message by the second derivation calculation. After the decryption of the original message in the receiver, the decrypted message can be transformed into the original message by the differentiation with respect to time.

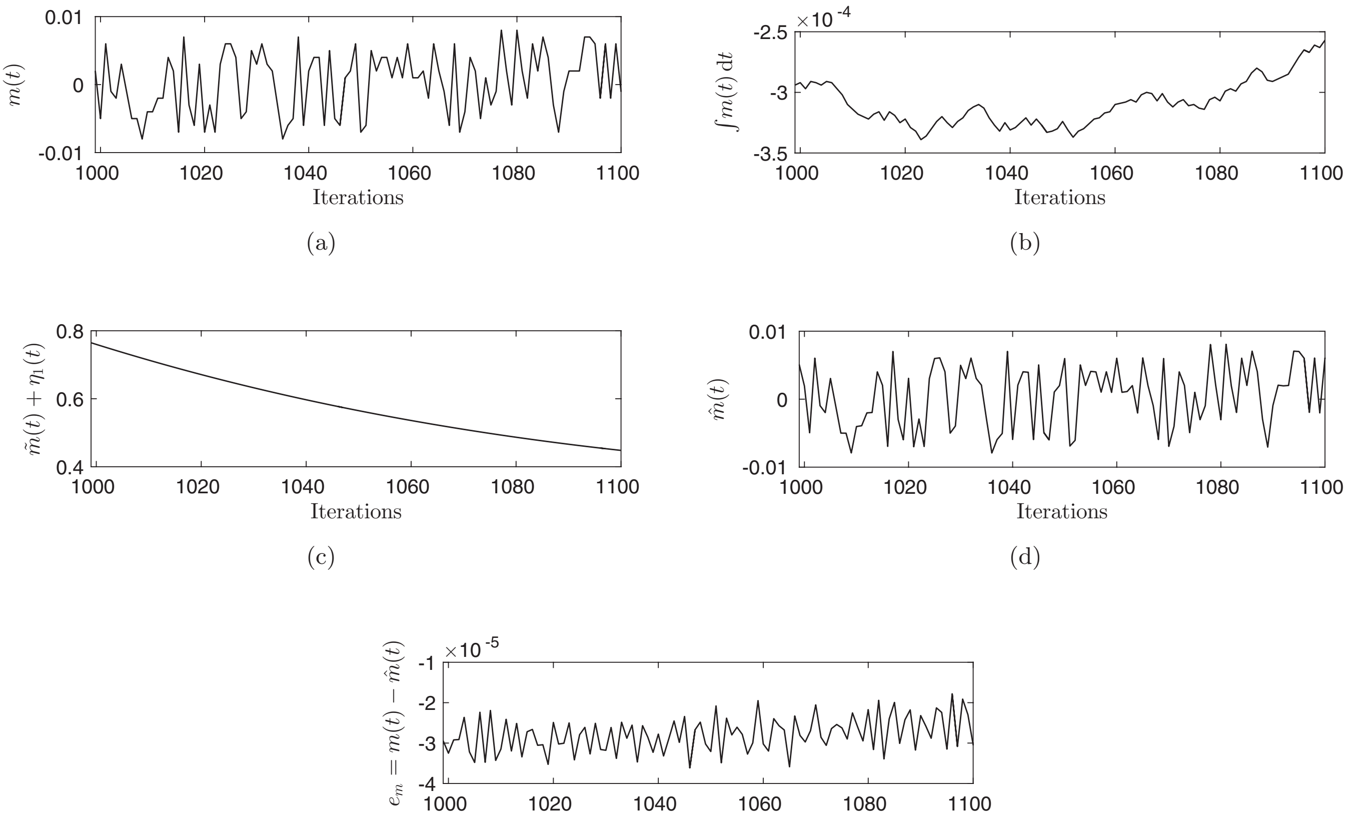
5.3. *Illustrative example of the MECHMS*

Numerical simulations demonstrate the efficiency of the proposed MECHMS. Its diagram is presented

Table 1. Construction of the low-level signal from the hexadecimal information.

Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Binary	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Low-level signal ($\times 10^{-3}$)	-8	-7	-6	-5	-4	-3	-2	-1	1	2	3	4	5	6	7	8

in Fig. 3. Here, $m(t)$ is the original transmitted message and $\hat{m}(t)$ is the recovered message. Finally, $\tilde{m}(t) = m(t) + \eta_3(t) \times 10^{-2}$ is the embeded message. The transmitter generates the output signal $\tilde{m}(t) + \eta_1(t)$ which depends on the message $m(t)$. Figure 4 illustrates the MECHMS GLS implementation for the encryption and the decryption of the digital information. Namely, Fig. 4(a) shows the original message to be encrypted, while Fig. 4(b) shows its integral. The dynamics of the transmitter is affected by the mentioned integral and this integral is added to the chaotic output signal to be sent via communication channel as well. The amplitude of the original message is much smaller than the chaotic signal generated by the transmitter. Figure 4(c) illustrates the signal which is transmitted via the communication channel. Finally, Fig. 4(d) shows the decrypted message while the error of the synchronization is illustrated in Fig. 4(e). Decryption scheme of the MECHMS requires the mutual initial synchronization between the chaotic transmitter and receiver up to the available numerical precision, called in the sequel as the "numerical zero". Therefore, the initial condition is the immediate candidate for the secret key. As our "numerical zero" is 10^{-14}, this key space is naturally discretized in the sense that two initial conditions that are closer to each other than the numerical zero should be represented by the same key. In [Čelikovský & Lynnyk, 2012; Lynnyk & Čelikovský, 2010] the secure encryption system based on the GLS was described by the DECSK method. It used a similar principle for the formation of the secret key. At the same time, the DECSK secure encryption scheme cannot use the full carrier of the generated signal and for the carrier signal at values close to zero the use of more than one iteration per bit is required. The MECHMS does not face the



(e)

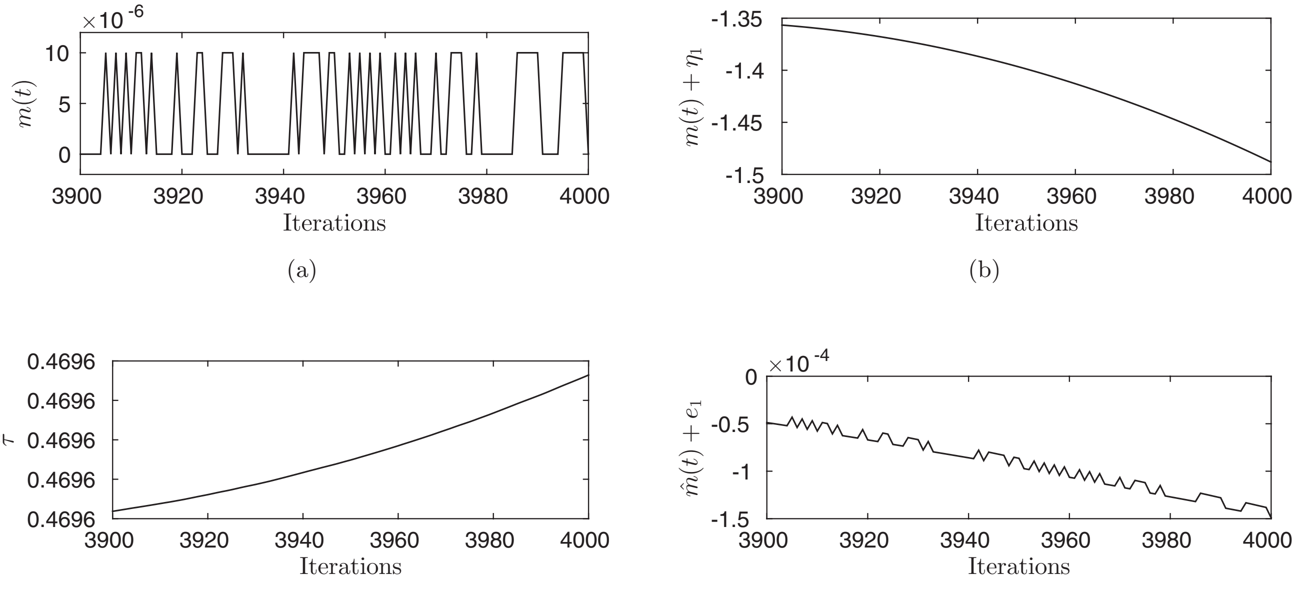
Fig. 4. Time histories related to the encryption and the decryption of the plaintext "93D76A73304466B91E52A151ADD B34CADA95023E29BB2C3289D12C9BB8B8D8896D972D14B93857F95F96D9EB517999EED6D6D7" using the MECHMS. Namely, (a) shows the plaintext time signal $m(t)$, (b) the integral of the plaintext $m(t)$, (c) the ciphertext of the embeded message $\tilde{m}(t)$ and the reduced value of $\eta_1(t)$, (d) the reconstructed plaintext $\hat{m}(t)$ and (e) the error e_m between the original plaintext $m(t)$ and the reconstructed plaintext $\hat{m}(t)$. "Intruder" can see only the third graph from the top.

above mentioned problems and it can be used for the encryption of the digital data using the full carrier of the generated signal. On the other hand, the detailed analysis provided in the next subsection shows that to enhance the security of the message transmission one can change the part of the secret key in the transmitter and the receiver during some suitable selected time intervals.

5.4. *Estimation of the initial condition and the bifurcation parameter by the adaptive observer*

Kerckhoffs's principle was stated by Auguste Kerckhoffs. It proclaims that everything about the cryptosystem is public knowledge, except the secret key. Later on, Claude Shannon reformulated this principle as "the enemy knows the system" [Shannon, 1949]. Therefore, we suppose that the "intruder" knows everything about the proposed secure cryptosystem, except the secret key, which consists of the initial condition and the bifurcation parameter τ of the chaotic system in the transmitter.

Figure 5 illustrates the extraction of the transmitted message generated by the transmitter shown in Fig. 2 without knowledge of the initial condition and the constant bifurcation parameter τ estimation after 3900 of iterations by the adaptive observer (18). Here, Fig. 5(a) shows the original message $m(t)$. Figure 5(b) illustrates the ciphertext $m(t) + \eta_1$ openly transmitted through the communication channel to the receiver. Figure 5(c) shows the estimation of the constant bifurcation parameter $\hat{\tau}$, one can see that the value of the parameter $\hat{\tau} \approx 0.4696$ estimated by the adaptive observer (18) is still quite far from the correct value $\tau = 0.5$ of the bifurcation parameter in the transmitter. Nevertheless, the adaptive observer (18) can reconstruct the original message $m(t)$ with a small error as well [see Fig. 5(d)]. Figure 6 demonstrates the full time histories of the errors between the transmitter of improved chaotic masking scheme and the adaptive observer (18) and the progress of the estimation of the constant bifurcation parameter $\hat{\tau}$. One can see that the states of the adaptive observer and the estimated value of the bifurcation parameter $\hat{\tau}$ converge to the states of the transmitter and the correct value of the constant bifurcation parameter τ during a short time of ≈3.5 sec. Therefore, the secret key component τ of the improved masking scheme (see Fig. 2) must be changed at least



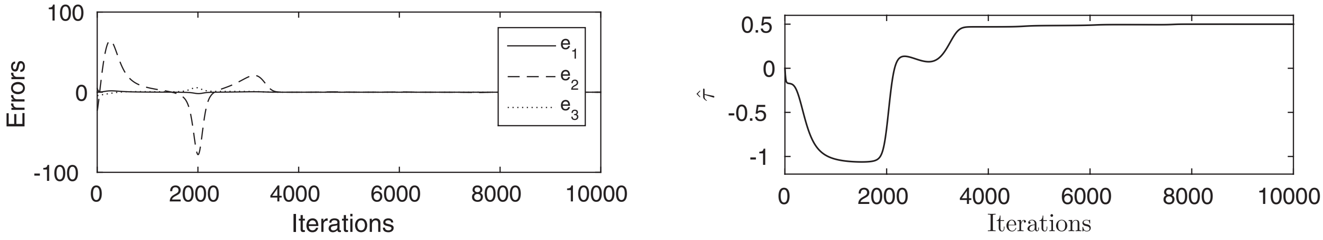
(a)

(b)

(c)

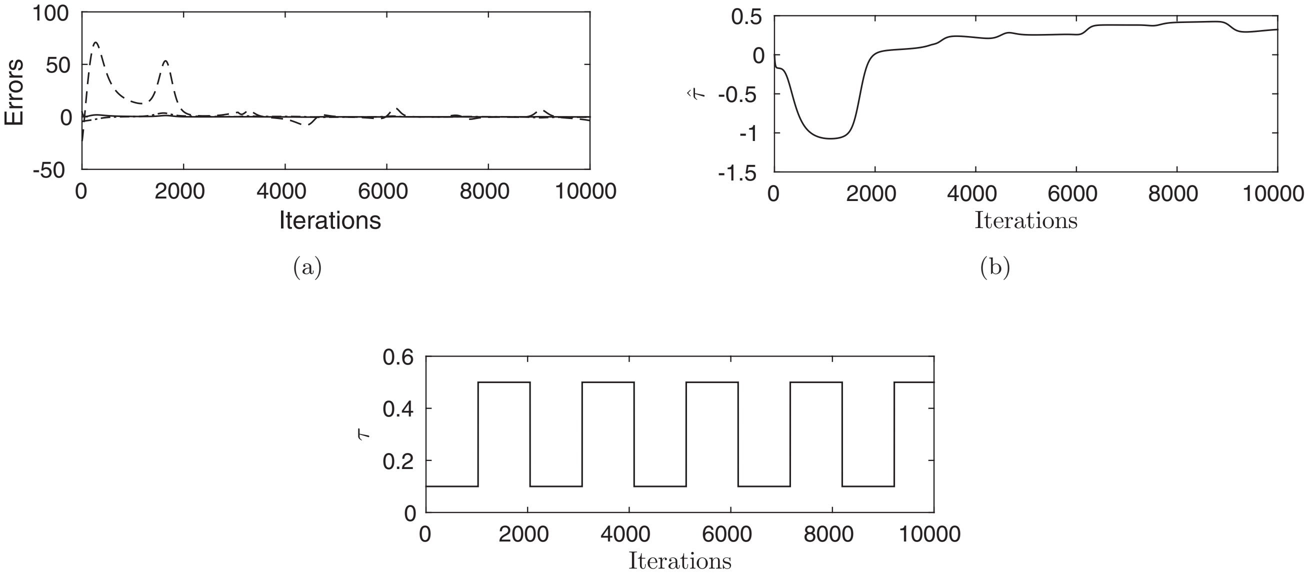
(d)

Fig. 5. Time histories related to the encryption and the decryption of the binary plaintext "0000010101011010000100011 0001110100000000010111101100101010100101010001001110010000000111110000111110" using the adaptive observer (18). Namely, (a) shows the binary plaintext time signal $m(t)$, (b) the ciphertext $m(t) + \eta_1(t)$, (c) the estimated bifurcation parameter $\hat{\tau}$ and (d) the reconstructed plaintext with the error $\hat{m}(t) + e_1$. "Intruder" can see the graph (b) which gives a possibility of the estimation of the bifurcation parameter $\hat{\tau}$ (c) and the reconstruction of the plaintext (a) during quite short time interval. Here, the improved chaotic masking scheme described in Fig. 2 is analyzed.



(a) (b)

Fig. 6. Time histories of (a) the errors e_1, e_2, e_3 between (17) and (18) and (b) the value of the estimated bifurcation parameter $\hat{\tau}$.



(a) (b)

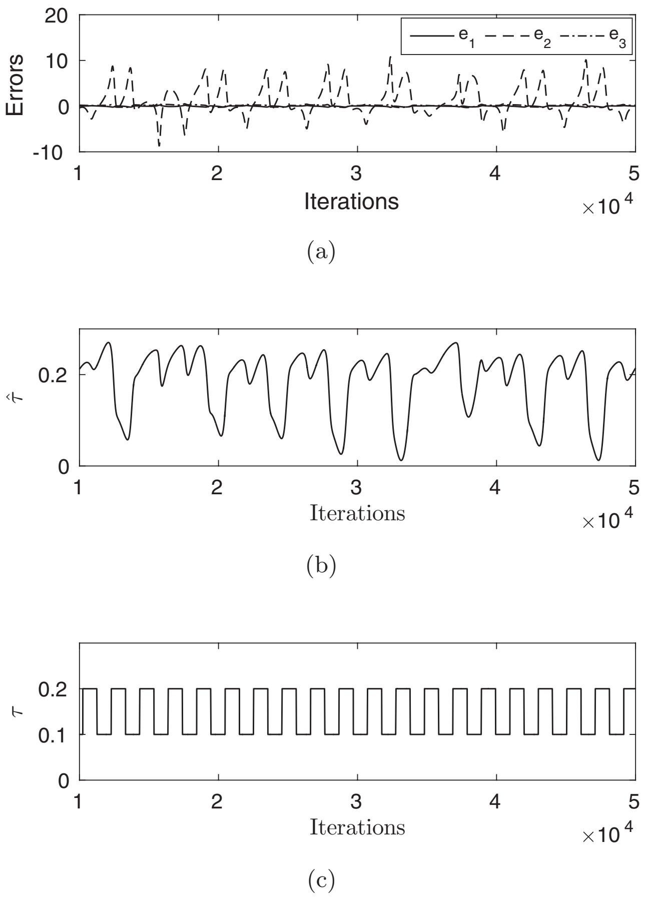
(c)

Fig. 7. Time histories related to estimation of the parameter τ by the adaptive observer (18). Here, (a) shows the errors e_1, e_2, e_3 between (17) and (18), (b) the value of estimated bifurcation parameter $\hat{\tau}$ and (c) the value of the parameter τ in the transmitter (17) which switches every 1024 iterations between values 0.1 and 0.5.

every three seconds, to exclude the possibility of the decryption of the transmitted information by the adaptive observer attack.

Figure 7 illustrates the error dynamics and the estimate of the varying bifurcation parameter $\hat{\tau}$ in the improved chaotic masking scheme. Here, the bifurcation parameter τ is changed every 1024 of iterations (≈ 1 sec) taking two different values. Switching between two bifurcation parameter values during the encryption of the message improves the chaotic masking transmitter shown in Fig. 2 and it prevents to estimate the state and the bifurcation parameter by the adaptive observer (18).

Using the adaptive observer (18) for the estimation of the varying bifurcation parameter τ and transmitter states of the MECHMS are illustrated in Fig. 8. During all the time the synchronization error between the transmitter (14) and the adaptive observer (18) is large. Furthermore, the adaptive observer cannot estimate a varying bifurcation parameter τ. Therefore, decryption of the original message with the adaptive observer (18) is not possible. That actually shows a good strength against very specific adaptive observer attack and demonstrates the possibility of using the proposed MECHMS in the chaos-based security communication.



(a)

(b)

(c)

Fig. 8. Time histories related to the estimation of the parameter τ by the adaptive observer (18) for the MECHMS. Here, (a) shows the errors e_1, e_2, e_3 between (14) and (18), (b) the value of the estimated bifurcation parameter $\hat{\tau}$ and (c) the value of the parameter τ in the transmitter (14) which switches every 1024 iterations between the values 0.1 and 0.2.

6. Conclusions and Outlooks

The GLS family has been analyzed and used for the chaotic masking of the digital information. More precisely, the MECHMS has been used to avoid the corruption of the synchronization by the transmitted message. This enabled to use a digital modulation with a very small amplitude thereby enhancing the security of the chaotic masking. It was shown that the proposed digital communication method has a potential of introducing the high degree of security at the low receiver complexity. At the same time, it requires a reasonable amount of data to encrypt a single bit, thereby making the continuous-time chaotic system for the digital data encryption realistic. The proposed cryptosystem has a good resistance against the adaptive observer attack. Further research will be devoted to the application of the proposed algorithm to encrypt the information transmitted between nodes in the complex networks [Čelikovský *et al.*, 2013]. Another goal of future research is to study the message embedded synchronization in analogue chaotic masking as well.

References

Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [2004] "Breaking parameter modulated chaotic secure communication system," *Chaos Solit. Fract.* **21**, 783–787.

Álvarez, G. & Li, S. [2006] "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation and Chaos* **16**, 2129–2151.

Alvarez-Ramirez, J., Puebla, H. & Cervantes, I. [2002] "Stability of observer-based chaotic communications for a class of Lur'e systems," *Int. J. Bifurcation and Chaos* **12**, 1605–1618.

Besancon, G. [2000] "Remarks on nonlinear adaptive observer design," *Syst. Contr. Lett.* **41**, 271–280.

Borowik, B., Karpinskyy, M., Lahno, V. & Petrov, O. [2012] *Theory of Digital Automata* (Springer Publishing Company).

Čelikovský, S. & Vaněček, A. [1994] "Bilinear systems and chaos," *Kybernetika* **30**, 403–424.

Čelikovský, S. & Chen, G. [2002] "On a generalized Lorenz canonical form of chaotic systems," *Int. J. Bifurcation and Chaos* **12**, 1789–1812.

Čelikovský, S. [2004] "Observer form of the hyperbolic-type generalized Lorenz system and its use for chaos synchronization," *Kybernetika* **40**, 649–664.

Čelikovský, S. & Chen, G. [2005a] "On the generalized Lorenz canonical form," *Chaos Solit. Fract.* **26**, 1271–1276.

Čelikovský, S. & Chen, G. [2005b] "Secure synchronization of a class of chaotic systems from a nonlinear observer approach," *IEEE Trans. Automat. Contr.* **50**, 76–82.

Čelikovský, S. & Lynnyk, V. [2006] "Observer-based chaos synchronization and its application to multi-valued alphabet chaos shift keying secure encryption," *Proc. 6th Asian Control Conf. 2006*, pp. 52–57.

Čelikovský, S., Lynnyk, V. & Šebek, M. [2006] "Observer-based chaos sychronization in the generalized chaotic Lorenz systems and its application to secure encryption," *Proc. 45th IEEE Conf. Decision and Control* (San Diego, USA), pp. 3783–3788.

Čelikovský, S. & Lynnyk, V. [2012] "Desynchronization chaos shift keying method based on the error second derivative and its security analysis," *Int. J. Bifurcation and Chaos* **22**, 1250231-1–11.

Čelikovský, S. & Lynnyk, V. [2013] "Message embedded synchronization for the generalized Lorenz system and its use for chaotic masking," *Adv. Intell. Syst. Comput.* **210**, 313–322.

Čelikovský, S., Lynnyk, V. & Chen, G. [2013] "Robust synchronization of a class of chaotic networks," *J. Franklin Instit. — Engin. Appl. Math.* **350**, 2936–2948.

Chang, J.-F., Yang, Y.-S., Liao, T.-L. & Yan, J.-J. [2008] "Parameter identification of chaotic systems using evolutionary programming approach," *Exper. Syst. Appl.* **35**, 2074–2079.

Chen, G. & Dong, X. [1998] *From Chaos to Order*: *Methodologies*, *Perspectives and Applications* (World Scientific, Singapore).

Chen, G., Čelikovský, S. & Zhou, J. [2009] "On a functional LaSalle principle with application to chaos synchronization," *Int. J. Bifurcation and Chaos* **19**, 4253–4261.

Chen, C.-S. [2010] "Optimal nonlinear observers for chaotic synchronization with message embedded," *Nonlin. Dyn.* **61**, 623–632.

Cuomo, K. M. & Oppenheim, A. V. [1993] "Circuit implementation of synchronized chaos with application to communications," *Phys. Rev. Lett.* **71**, 65–68.

Cuomo, K. M., Oppenheim, A. V. & Strogatz, S. H. [1993] "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst.-II* **40**, 626–633.

Dachselt, F. & Schwarz, W. [2001] "Chaos and cryptography," *IEEE Trans. Circuits Syst.-I*: *Fund. Th. Appl.* **48**, 1498–1509.

Dedieu, H., Kennedy, M. P. & Hasler, M. [1993] "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit," *IEEE Trans. Circuits Syst.-II* **40**, 634–642.

Fradkov, A., Nijmeijer, H. & Markov, A. [2000] "Adaptive observer-based synchronization for communication," *Int. J. Bifurcation and Chaos* **10**, 2807–2813.

Fradkov, A. L., Andrievsky, B. & Ananyevskiy, M. S. [2015] "Passification based synchronization of nonlinear systems under communication constraints and bounded disturbances," *Automatica* **55**, 287–293.

Hu, J. F. & Guo, J. B. [2008] "Breaking a chaotic direct sequence spreading spectrum secure communication system," *Acta Phys. Sin.* **57**, 1477–1484.

Kaddoum, G. & Shokraneh, F. [2015] "Analog network coding for multi-user multi-carrier differential chaos shift keying communication system," *IEEE Trans. Wireless Commun.* **14**, 1492–1505.

Khalil, H. [2002] *Nonlinear Systems*, 3rd edition (Prentice Hall).

Kocarev, L., Halle, K., Eckert, K. & Chua, L. [1992] "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurcation and Chaos* **2**, 709–713.

Kocarev, L. & Parlitz, U. [1995] "General approach for chaotic synchronization with applications to communication," *Phys. Rev. Lett.* **74**, 5028–5031.

Kocarev, L. [2001] "Chaos-based cryptography: A brief overview," *IEEE Circuits and Syst. Mag.* **1**, 6–21.

Kolumbán, G., Kennedy, M. P. & Chua, L. O. [1998] "The role of synchronization in digital communications using chaos-part II: Chaotic modulation and chaotic synchronization," *IEEE Trans. Circuits Syst.-I*: *Fund. Th. Appl.* **45**, 1129–1140.

Li, S., Álvarez, G., Chen, G. & Mou, X. [2005] "Breaking a chaos-noise-based secure communication scheme," *Chaos* **15**, 013703.

Li, S., Chen, G. & Álvarez, G. [2006] "Return-map cryptoanalysis revisited," *Int. J. Bifurcation and Chaos* **16**, 1157–1168.

Lian, K.-Y. & Liu, P. [2000] "Synchronization with message embedded for generalized Lorenz chaotic circuits and its error analysis," *IEEE Trans. Circuits Syst.-I*: *Fund. Th. Appl.* **47**, 1418–1424.

Liang, X., Zhang, J. & Xia, X. [2008] "Adaptive synchronization for generalized Lorenz systems," *IEEE Trans. Automat. Contr.* **53**, 1740–1746.

Liang, H., Wang, Z., Yue, Z. & Lu, R. [2012] "Generalized synchronization and control for incommensurate fractional unified chaotic system and applications in secure communication," *Kybernetika* **48**, 190–205.

Liao, T.-L. & Huang, N.-S. [1999] "An observer-based approach for chaotic synchronization with applications to secure communications," *IEEE Trans. Circuits Syst.-I*: *Fund. Th. Appl.* **46**, 1144–1150.

Liu, L., Wu, X. & Hu, H. [2004] "Estimating system parameters of Chua's circuit from synchronizing signal," *Phys. Lett. A* **324**, 36–41.

Lynnyk, V. & Čelikovský, S. [2010] "On the anti-synchronization detection for the generalized Lorenz system and its application to secure encryption," *Kybernetika* **46**, 1–18.

Materassi, D. & Basso, M. [2008] "Time scaling of chaotic systems: Application to secure communications," *Int. J. Bifurcation and Chaos* **18**, 567–575.

Milanovic, V. & Zaghloul, M. [1996] "Improved masking algorithm for chaotic communications systems," *Electron. Lett.* **32**, 11–12.

Parlitz, U., Chua, L. O., Kocarev, L., Halle, K. S. & Shang, A. [1992] "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurcation and Chaos* **2**, 973–977.

Pecora, L. M. & Carroll, T. L. [1990] "Synchronization in chaotic systems," *Phys. Rev. Lett.* **64**, 821–824.

Perez, G. & Cerdeira, H. [1995] "Extracting messages masked by chaos," *Phys. Rev. Lett.* **74**, 1970–1973.

Shannon, C. E. [1949] "Communication theory of secrecy systems," *Bell Syst. Tech. J.* **28**, 656–715.

Short, M. K. [1994] "Steps toward unmasking secure communications," *Int. J. Bifurcation and Chaos* **4**, 959–977.

Tyukin, I. Y., Steur, E., Nijmeijer, H. & van Leeuwen, C. [2013] "Adaptive observers and parameter estimation for a class of systems nonlinear in the parameters," *Automatica* **49**, 2409–2423.

Vaidya, P. & Angadi, S. [2003] "Decoding chaotic cryptography without access to the superkey," *Chaos Solit. Fract.* **17**, 379–386.

Wang, X., Zhan, M., Lai, C. & Gang, H. [2004] "Error function attack of chaos synchronization based encryption schemes," *Chaos* **14**, 128–137.

Wu, C. & Chua, L. [1993] "A simple way to synchronize chaotic systems with application to secure communication systems," *Int. J. Bifurcation and Chaos* **03**, 1619–1627.

Yang, T., Yang, L. & Yang, C. [1998a] "Breaking chaotic secure communication using a spectrogram," *Phys. Lett. A* **247**, 105–111.

Yang, T., Yang, L. & Yang, C. [1998b] "Cryptanalyzing chaotic secure communications using return maps," *Phys. Lett. A* **245**, 495–510.

Zelinka, I., Chen, G. & Celikovsky, S. [2010] "Chaos synthesis by evolutionary algorithms," *Evolutionary Algorithms and Chaotic Systems*, eds. Zelinka, I., Celikovsky, S., Richter, H. & Chen, G. (Springer, Berlin, Heidelberg), pp. 345–382.

Zhang, Q. [2002] "Adaptive observer for multiple-input-multiple-output (MIMO) linear time-varying systems," *IEEE Trans. Automat. Contr.* **47**, 525–529.