20

Robustness and Security of H_∞-Synchronizer in Chaotic Communication System

Takami Matsuo, Yusuke Totoki and Haruo Suemitsu
Oita University, Dannoharu, Oita
Japan

1. Introduction

In recent years, a large amount of work on chaos-based cryptosystems has been published (Kocarev (2001); Millérioux et al. (2008)). A general methodology for designing chaotic and hyperchaotic cryptosystems has been developed using the control systems theory (Grassi et al. (1999); Liao et al. (1999); Yang et al. (1997a;b)). The chaotic communication system is closely related to the concept of chaos synchronization. An overview of chaotic secure communication systems can be found in (Yang (2004)). He classified the continuous-time chaotic secure communication systems into four generations. In the third generation, the combination of the classical cryptographic technique and chaotic synchronization is used to enhance the degree of security. Specifically, Yang *et al.* proposed a new chaos-based secure communication scheme in an attempt to thwart the attacks (Yang et al. (1997a;b)). They have combined both conventional cryptographic method and synchronization of chaotic systems. Their cryptographic method consists of an encryption function (the multi-shift cipher), a decryption function (the inverse of the encryption function), a chaotic encrypter that generates the key signal for the encryption function, and a decrypter that estimates the key signal. The approach has a limitation since the cryptosystem design may fail if different chaotic circuits are utilized. So far, this generation has the highest security in all the chaotic communication systems had been proposed and has not yet broken. From the control theoretic perspective, the transmitter and the receiver in the chaotic communication system can be considered as the nonlinear plant and its observer, respectively. Grassi *et al.* proposed a nonlinear-observer-based decrypter to reconstruct the state of the encrypter (Grassi et al. (1999); Liao et al. (1999)). They extended the Chua's oscillator to the observer-based decrypter. The cryptosystem does not require initial conditions of the encrypter and the decrypter belonging to the same basin of attraction. If we can design a decrypter without the knowledge of the parameters of the encrypter, the chaos-based secure communication systems are not secure, because the parameters of the encrypter is selected as static secret keys in the cryptosystem. Parameter identification and adaptive synchronization methods may be effective for intruders in building reconstruction mechanisms, even when a synchronizing system is not available. Therefore, it is important for secure issues to investigate whether adaptive identifiers without the system information of encrypter can be constructed or not.
We have recently designed an observer-based chaotic communication system combining the cryptosystems proposed by Grassi *et al.* (Grassi et al. (1999)) and by Liao *et al.* (Liao et al. (1999)) that allows us to assign the relative degree and the zeros of its encrypter system (Matsuo et al. (2004)). Specifically, we constructed three cryptosystems based on a Chua's circuit by assigning its relative degree and zeros. The cryptosystem consists of

an encryption function (the multi-shift cipher), a decryption function (the inverse of the encryption function), a chaotic encrypter that generates the key signal for the encryption function, and a decrypter that estimates the key signal. The proposed cryptosystem allows us to assign the relative degree and the zeros of the encrypter dynamics by selecting an output vector that generates a transmitted signal as partial states of the encrypter. As in (Fradkov et al. (1997; 2000)), we can design an adaptive decrypter for minimum-phase systems with its relative degree 1. Therefore, the encrypter dynamics should be design such that its relative degree is more than two and its zeros are unstable so as to fail to synchronize the cryptosystem adaptively. At the same time, the designed cryptosystem should be robust with respect to uncertainties of the transmission lines such as a time delay, and noises. Suykens *et al.* (Suykens et al. (1997a;b)) presented a nonlinear H_∞ synchronization method for chaotic Lur'e systems based on the dissipativity of nonlinear systems to minimize the influence of the exogenous input such as the message signal and channel noises.

However, many proposed systems with robustness against parameter uncertainties and signal uncertainties are difficult to implement in practice with a reasonable degree of security. The basic difference between the conventional cryptography and the chaos cryptography is that the conventional encryption is defined discrete sets and the chaos encryption is defined on continuous sets. This makes the keyspace behavior of chaotic systems vary different that of conventional systems. Due to the continuous-value property, keys in chaotic cryptosystems form a key basin around the actual secret key.

When one key is very close to the real one, it could decrypt part or all of the ciphertext (Alvarez et al. (2006)). To avoid brute-force attacks, a secret parameter should be sensitive enough to guarantee the so-called avalanche property: even when the smallest change occurs in the parameter, the ciphertext will change dramatically (Alvarez et al. (2006)).

Various attacks such as the nonlinear forecasting, the return map, the adaptive parameter estimation, the error function attack (EFA), and inverse computation based on the chosen cipher attack, are proposed to recover messages from the chaotic ciphers (Zhou (2005)). Short (Parke et al. (2001); Short (1994; 1996)) and Guojie *et al.* (Guojie et al. (2003)) have proposed the attack strategies against chaotic communication systems. Short analyzed only the encrypter by using the nonlinear forecasting method that belongs to ciphertext-only attack when the attacker does not know the structure of the encryption system. They discussed the secure property of chaos communication based on chaotic parameter modulation from the chosen-ciphertext attack under the Kerckhoff principle (Guojie et al. (2003)). Guojie *et al.* discussed the secure property of chaos communication based on chaotic parameter modulation from the chosen-ciphertext attack under the Kerckhoff principle. We proposed chaotic communication systems using the adaptive control and robust control technologies (Matsuo et al. (2004; 2008)).

Wang *et al.* (Wang et al. (2004)) presented the error function attack to evaluate system security as an efficient cryptanalysis tool based on the public-structure and known-plaintext cryptanalysis. By defining the EFA function, an eavesdropper can scan the whole keyspace to find out the proper key that satisfies the EFA function with zero value. Since keys that are not identical with but are very close to the real one can be used to synchronize the two systems very well, a key basin around the actual secret key is formed. Once the eavesdropper knows the key basin, the correct key can be easily obtained through some optimization algorithms. To evaluate the security performance, Wang *et al.* also defined the key basin width by the distance between two trial keys located on the two sides of the key basin. The narrower than the whole keyspace the key basin width is, the higher the security of the cryptosysytem is. However, a systematic approach to get the key basin width is lacking. The brute-force-like calculations are needed to draw the shape of the EFA function. Thus, a considerable computing time is needed

to get the key basin width. If the EFA function has numerous minima and a needle-like basin, the security level of the cryptosystem is high. In this case, the evolutionary optimization techniques such as the particle swarm optimization cannot find the secret key using the EFA function (Nomura et al. (2011)). Anstett *et al.* proposed a general framework based on identifiability for the cryptanalysis of chaotic cryptosystems (Anstett et al. (2006)). They also pointed out that cryptosystems involving polynomial nonlinearities are weak against a known plaintext attack.

In this chapter, we propose an H_∞ synchronizer in order to improve the robustness of chaotic communication systems with respect to delays in the transmission line based on the standard linear H_∞ control theory. To begin with, we derive an error system between the encrypter and the decrypter and reduce the design problem of the cryptosystem to the stabilization problem of a generalized plant in the robust control theory. Next, we give a synchronizer parameterization and an H_∞ synchronizer based on the robust control theory. Furthermore, the decrypter dynamics is designed via the linear controller parameterization to make the decrypter robust against disturbances in transmission line and/or sensitive to modeling errors of the decrypter. We present two design requirements on the robustness and the security. We need to design the free parameter such that both the requirements are satisfied. Since we cannot get this solution simultaneously, we design the dynamical compensator so as to satisfy the robustness requirement and then check the sensitivity to the key parameter mismatches whether the parameters in encrypter may play the role of the secret key or not, numerically. Finally, the proposed system is compared with that proposed by Grassi et al. using MATLAB simulations.

The following notation is used (Doyle et al. (1989)) :

$\mathcal{F}_l(G, Q)$: lower linear fractional transformation

$$\left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] := C(sI - A)^{-1}B + D$$

2. Observer-based chaotic communication system with free dynamics

Grassi *et al.* (Grassi et al. (1999)) proposed a nonlinear-observer-based cryptosystem that is an extension of the cryptosystem proposed by Yang *et al.* (Yang et al. (1997b)). The cryptographic method consists of an encryption function (the multi-shift cipher), a decryption function (the inverse of the encryption function), a chaotic encrypter that generates the key signal for the encryption function, and a decrypter that estimates the key signal. The transmitted signal through a public channel contains the nonlinear function that is equivalent to that of the encrypter. We add a dynamic compensator in the transmitted signal to the observer-based chaotic communication system proposed by Grassi *et al.* Figure 1 shows the relationship among the encrypter, the observer-based decrypter and the adaptive decrypter where we use the adaptive decrypter as a tool for ciphertext-only attacks.

The cryptosystem consists of an encryption function (the multi-shift cipher), a decryption function (the inverse of the encryption function), a chaotic encrypter that generates the key signal for the encryption function, and a decrypter that estimates the key signal.

- **Part 1 : dynamic encrypter**
  The chaotic encrypter is described by the following equations:

$$\dot{x} = Ax + b_2 f(x) + b_2 e_n \tag{1}$$

$$v = P(s)x \tag{2}$$

$$y = v + e_n + f(x) \tag{3}$$

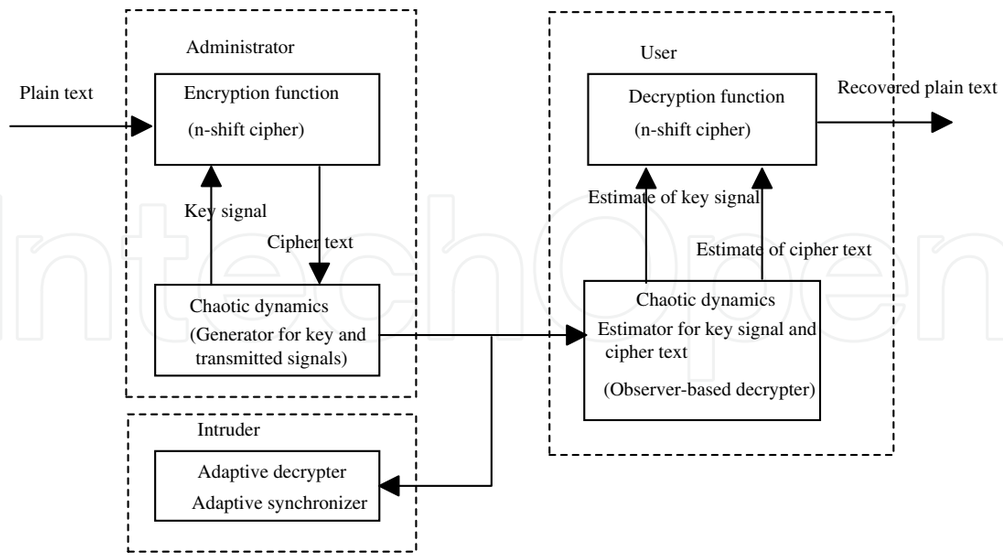


Fig. 1. Chaotic cryptosystem configuration.

where y is the transmitted signal that includes the nonlinear function, $P(s)$ is a transfer function that lets a decrypter synchronize the encrypter, and $s = \frac{d}{dt}$. We call this transfer function $P(s)$ a synchronizer.

- **Part 2 : encryption function**
  Given a plaintext signal $p(t)$, the ciphertext $e_n(t)$ is given by

$$e_n(t) = e_n(p(t), K(t)) \tag{4}$$

where $K(t)$ is a stream key signal that is generated by the encrypter dynamics and is given by the following equation:

$$K(t) = k^T x. \tag{5}$$

The signal e_n is a generic encryption function that makes use of the key signal and we choose a encryption function as the following n-shift cipher:

$$e_n(p(t), K(t)) = q(\cdots q(q(p(t), K(t)), K(t)), \cdots), K(t))$$

$$q(x,k) = \begin{cases} (x+k) + 2h, & -2h \le (x+k) \le -h \\ (x+k), & -h < (x+k) < h \\ (x+k) - 2h & h \le (x+k) \le 2h \end{cases}$$

- **Part 3 : dynamic decrypter with free dynamics**
  Given the encrypter, the decrypter used by an authorized user is the following observer:

$$\dot{\hat{x}} = A\hat{x} + b_2 e_y \tag{6}$$

$$\hat{v} = P(s)\hat{x} \tag{7}$$

$$e_y = y - \hat{v} = P(s)(x - \hat{x}) + e_n + f(x) \tag{8}$$

$$\hat{e}_n = y - (\hat{v} + f(\hat{x})) \tag{9}$$

where $\hat{e}_n$ is a recovered signal of the plain text.

- **Part 4 : decryption function**
  Using the estimated signals $\hat{K}(t)$ and $\hat{e}_n(t)$ by the decrypter, the estimate of the plaintext $\hat{p}(t)$ can be recovered by the following equations:

$$\hat{p}(t) = d(\hat{e}_n(t), \hat{K}(t)) \tag{10}$$

$$\hat{K}(t) = k^T \hat{x} \tag{11}$$

  where $\hat{K}$ is an estimate of the stream key signal and d is the decryption function given by

$$\hat{p}(t) = q(\cdots q(q(\hat{e}_n(t), -\hat{K}(t)), -\hat{K}(t)), \cdots), -\hat{K}(t)).$$

3. Design of H_∞-synchronizer

3.1 Error equations and generalized system

If the transmitted signal is disturbed by an additional disturbance $w(t)$, the signal is rewritten by

$$\tilde{y}(t) = v(t) + e_n(t) + f(x(t)) + \omega(t) \tag{12}$$

When some of parameters of the dynamic encrypter are unknown, the dynamic decrypter constructed by a receiver based on the information of the encrypter has parametric uncertainties. The decrypter used by any receivers including intruders is given by

$$\dot{\hat{x}} = \tilde{A}\hat{x} + \tilde{b}_2 e_y \tag{13}$$

$$\hat{v} = \tilde{P}(s)\hat{x} \tag{14}$$

$$\hat{e}_n = \tilde{y} - (\hat{v} + \tilde{f}(\hat{x})) \tag{15}$$

Denoting the uncertainties of $\tilde{A}, \tilde{b}_2$ in the encrypter dynamics as Δ, the perturbed nonlinear function of $f(x)$ as $\tilde{f}(x)$, and the perturbation of the H_∞ synchronizer as $\tilde{P}(*)$, we assume that the decrypter with the uncertainties is given by

$$\dot{\hat{x}} = A\hat{x} + b_1\Delta + b_2 e_y \tag{16}$$

$$\hat{v} = \tilde{P}(s)\hat{x},\ e_y = \tilde{y} - \hat{v} \tag{17}$$

$$\hat{e}_n = e_y - \tilde{f}(\hat{x}) = \tilde{y} - (\hat{v} + \tilde{f}(\hat{x})). \tag{18}$$

A decrypter used by an authorized user satisfies $\Delta(t) = 0, f(\cdot) = \tilde{f}(\cdot), P(s) = \tilde{P}(s)$ since he knows all parameters of the encrypter. On the other hand, a decrypter used by an intruder has uncertainties in the encrypter dynamics, the nonlinear function, and the synchronizer.
In this chapter, we assume that the intruder knows the H_∞ synchronizer, $P(s) = \tilde{P}(s)$ but does not know the values of A, b_2, *i.e.* $\Delta(t) \neq 0$, and the nonlinear function, *i.e.* $f(\cdot) \neq \tilde{f}(\cdot)$. Defining the estimation error of the decrypter as $e(t) = \hat{x}(t) - x(t)$, we have the following error system:

$$\dot{e}(t) = Ae(t) + b_1\Delta(t) + b_2\omega(t) - b_2\xi(t) \tag{19}$$

$$\xi(t) = P(s)e \tag{20}$$

We assign the estimation error of the key signal e_K or that of cipher text $\tilde{e}_n$ to the controlled output as follows:

$$\begin{aligned} e_K(t) &= \hat{K}(t) = k^T e(t) \\ \tilde{e}_n &= \hat{e}_n - e_n = \tilde{y} - \hat{v} - \tilde{f}(\hat{x}) - e_n \\ &= -\xi + (f(x) - \tilde{f}(\hat{x})) + \omega \end{aligned}$$

If $\lim_{t\to\infty} \omega(t) = 0$,$\lim_{t\to\infty}(f(x) - \tilde{f}(\hat{x})) = 0$ and $\lim_{t\to\infty} e(t) = 0$, then the plaintext can be recovered by the decrypter ,$\lim_{t\to\infty}(e_n(t) - \hat{e}_n(t)) = 0$.
Since $f(\cdot) = \tilde{f}(\cdot)$ for authorized users, we have

$$\begin{aligned} |\tilde{e}_n| &\le |\xi| + |f(x) - f(\hat{x})| + |w| \\ &\le |P(s)e| + \gamma\|e\| + |w|. \end{aligned}$$

Thus, if $\lim_{t\to\infty} w(t) = 0$ and $\lim_{t\to\infty} e(t) = 0$, then we attain the recover the plaintext, *i.e.* $\lim_{t\to\infty}(e_n(t) - \hat{e}_n(t)) = 0$.
For each controlled output, the generalized plant in Fig. 2 is defined as:

- When the controlled output is e_K, the generalize plant is

$$G_1(s) = \left[\begin{array}{c|cc} A & [b_1 \quad b_2] & -b_2 \\ \hline k^T & 0 & 0 \\ I & 0 & 0 \end{array}\right] \tag{21}$$

- When the controlled output is the upper bound of $|\tilde{e}_n|$, the generalize plant is

$$G_2(s) = \left[\begin{array}{c|cc} A & [b_1 \quad b_2] & -b_2 \\ \hline k^T & [0 \;\; 1] & -1 \\ I & 0 & 0 \end{array}\right]. \tag{22}$$

3.2 Synchronizer parameterization

To design the synchronizer based on the static output-feedback-based controller, we rewrite the generalized plant as in Fig.2. Since we can select the input of the synchronizer as arbitrary scalar signal, the signal in Eq.(2) is chosen as $v(t) = P(s)x(t) = P_o(s)c^T x(t)$, where c is an arbitrary vector.
We call a stabilizing compensator $P_o(s)$ for the generalized plant $G(s)$ the synchronizer of the chaotic cryptosystem. The design problem of the synchronizer is summarized as follows:

> Given a generalized plant $G(s)$ as in Fig. 2, parameterize all synchronizer $P(s)$ that internally stabilize $G(s)$.

We consider the n-th order generalized plant in Fig.3, where (A, B_2) is stabilizable and (A, C_2) is detectable;

$$G_o(s) = \begin{bmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{bmatrix} = \left[\begin{array}{c|cc} A & B_1 & B_2 \\ \hline C_1 & D_{11} & D_{12} \\ C_2 & D_{21} & 0 \end{array}\right] \tag{23}$$

and the p-th order dynamic stabilizing compensator,

$$P_o(s) = \left[\begin{array}{c|c} A_c & B_c \\ \hline C_c & D_c \end{array}\right]. \tag{24}$$

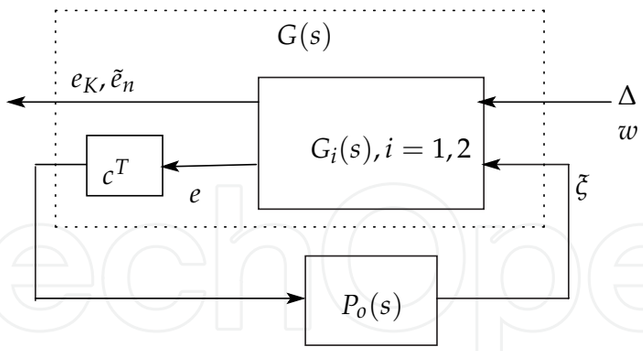


Fig. 2. Generalized plant and synchronizer in the chaotic communication system.

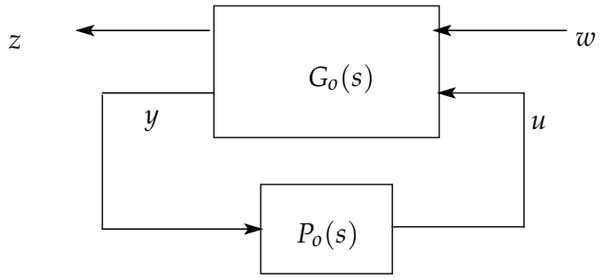


Fig. 3. Generalized plant and controller in the robust control theory.

For any choice of K_0, we can obtain the parameterization of $K(s)$ as follows (Matsuo et al. (1998)):

$$P_o(s) = \mathcal{F}_l(\tilde{P}_o(s), Q(s)) \tag{25}$$

$$\tilde{P}_o(s) = \left[\begin{array}{c|cc} A_K + H_0C_2 + B_2F_0 & -H_0 & B_2 \\ \hline F_0 & K_0 & I \\ -C_2 & I & 0 \end{array}\right] \tag{26}$$

$$Q(s) = \left[\begin{array}{c|c} A_{c22} & B_{c2} \\ \hline C_{c2} & D_{c2} \end{array}\right]$$

$$A_K = A + B_2K_0C_2$$

where

A_{c22} : stable
F_0 s.t. $A_K + B_2F_0$ is stable
H_0 s.t. $A_K + H_0C_2$ is stable.

Since $P_o(s)$ is a stabilizing compensator for each $Q(s) \in RH_\infty$, (25) is one of the parameterization of stabilizing compensators. This LFT form is equal to the Youla parameterization when the static output feedback gain, K_0, is selected as zero. When the generalized plant can be stabilized by a static output feedback gain, *i.e.* there exists an output feedback gain K_0 such that A_K is stable, we can set $H_0 = 0$, $F_0 = 0$. In this case, the

parameterization of all stabilizing compensators is as follows (Matsuo et al. (1998)):

$$P_o(s) = \mathcal{F}_l(\tilde{P}_o(s), Q(s)) \tag{27}$$

$$= K_0 + Q(s)(I + C_2(sI - A_K)^{-1}B_2Q(s))^{-1} \tag{28}$$

where

$$\tilde{P}_o(s) = \left[\begin{array}{c|cc} A_K & 0 & B_2 \\ \hline 0 & K_0 & I \\ -C_2 & I & 0 \end{array}\right]. \tag{29}$$

In Fig. 2, since C_2 is replace to c^T, where c^T can be selected as an arbitrary vector, there exists a scalar k_0 such that $A_k = A - b_2k_0c^T$ is stable, as long as (A, b_2) is stabilizable. In this case, we can set $H_0 = 0,\ F_0 = 0$. The parameterization of all synchronizers in Fig. 2 is obtained as follows (Matsuo et al. (1998)):

$$P_o(s) = \mathcal{F}_l(\tilde{P}_o(s), Q(s)) \tag{30}$$

where $Q(s) \in RH_\infty$ and

$$\tilde{P}_o(s) = \left[\begin{array}{c|cc} A_k & 0 & -b_2 \\ \hline 0 & k_0 & 1 \\ -c^T & 1 & 0 \end{array}\right]. \tag{31}$$

We call this parameterization a synchronizer parameterization. By selecting $P_o(s)$ as constant gain k_0 *i.e.* $Q(s) = 0$, the proposed cryptosystem is equivalent to that proposed by Grassi *et al.*

3.3 Design problem of H_∞ synchronizer

The input-output relation of the generalized plant $G(s) = G_1(s)$ or $G_2(s)$ from the exogenous input $[\Delta\ \ w]$ to the controlled output z is given by

$$z = \mathcal{F}_l(G(s), P(s)) \left[\, \Delta(s)\ w(s) \,\right]^T \tag{32}$$

$$= \left[\, T_1(s)\ T_2(s) \,\right] \left[\, \Delta(s)\ w(s) \,\right]^T \tag{33}$$

The free dynamics $Q(s)$ is designed to make the decrypter robust against the disturbances in the transmission line of sensitive to the modeling errors of the decrypter by intruders. We present two design specifications:

1. **Robustness requirement:** The proposed decrypter can recover the plain text by the transmitted signals when the generalized plant with the synchronizer is internally stable. Moreover, the H_∞ synchronizer has an additional synchronization property with respect to plant uncertainties. To recover plain texts, the decrypter should be robust with respect to time delay uncertainties in the transmission line. Design the free parameter $Q(s)$ such that for a given γ_2,

$$\|T_2(s)\| < \gamma_2. \tag{34}$$

2. **Security requirement:** To attain the secure cryptosystem, the decrypter of the intruder should not synchronize the encrypter. Therefore, The free parameter $Q(s)$ is designed to

the error system sensitive to Δ. Design the free parameter $Q(s)$ such that for a given γ_1,

$$\underline{\sigma}\{T_1(j\omega)\} > \gamma_1, \text{ for } \omega \in [0, \infty). \tag{35}$$

However, since the generalized plant does not have a direct term from the uncertainty Δ to the transmitted signal $\tilde{y}$, (35) cannot be hold for all $\omega \in [0, \infty)$. Therefore, to satisfy the security requirement, we change the transmitted signal $\tilde{y}$ and the feedback term in the decrypter e_y as

$$\begin{aligned} \tilde{y}(t) &= v(t) + e_n(t) + f(x(t)) + \omega(t) + c^T A b_2 \\ e_y &= \tilde{y} - \hat{v} - c^T \tilde{A} \tilde{b}_2 \end{aligned}$$

In this case, the estimation error of the cipher text includes the direct term from the uncertainty to the transmitted signal as follows:

$$\tilde{e}_n' = \xi + (f(x) - \tilde{f}(\hat{x})) + w + \Delta'$$

In particular, when there is a perturbation in the nonlinear function, $f(x) \neq \tilde{f}(\hat{x})$ generates the direct term from the uncertainty to the transmitted signal.

We need to design the free parameter such that both the requirements are satisfied. Since we cannot get this solution, we design the dynamical compensator so as to satisfy the robustness requirement, and then check the security requirement whether the error system is sensitive to the modeling errors of the decrypter, *i.e.* the designed cryptosystem is secure against to attacks by intruders.

4. Simulations

We design a robust cryptosystem via Chua's circuits as in Yang *et al.* (Yang et al. (1997b)) and in Fradkov *et al.* (Fradkov et al. (2000)), and carry out simulations using MATLAB/Simulink.

4.1 Encrypter based on Chua's circuit

The chaotic encrypter based on the Chua's circuit is given by

$$\dot{x} = Ax + b_2 f(x_1) + b_2 e_n \tag{36}$$

$$y = P(s)x + e_n + f(x) \tag{37}$$

$$f(x_1) = G_b x_1 + \frac{1}{2}(G_a - G_b)(|x_1 + 1| - |x_1 - 1|)$$

$$A = \begin{bmatrix} -p_1 & p_1 & 0 \\ 1 & -1 & 1 \\ 0 & -p_2 & -p_3 \end{bmatrix}$$

$$b_2 = \begin{bmatrix} -p_1 \\ 0 \\ 0 \end{bmatrix}, x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

We select the parameters in the Chua's circuit given by Liao *et al.* (Liao et al. (1999)) as $p_1 = 10, p_2 = 13.14, p_3 = 0.07727, G_a = -1.28$, and $G_b = -0.69$. The initial conditions are given by

$$x_1(0) = 1.1, x_2(0) = 0, x_3(0) = 0$$
$$\hat{x}_1(0) = 0, \hat{x}_2(0) = 0, \hat{x}_3(0) = 0$$

The encryption function is 30-shift cipher, the parameter h is equal to 1 and the key signal $K(t)$ is the second state variable x_2, *i.e.*

$$K(t) = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} x(t).$$

Moreover, we select $c^T = -\begin{bmatrix} 0 & 1 & 1 \end{bmatrix}$.
MATLAB has a built-in music file, `handel.mat`, with a short segment of Handel's *Messiah*. We use it as the plaintext signal.

4.2 Grassi-type system

In the encrypter presented by Grassi *et al.* (Grassi et al. (1999)), the dynamic synchronizer is simplified as $P_o(s) = k_0 = 0.8$.

4.3 Design of H_∞-synchronizer

The generalized plant $G_1(s)$ in designing the H_∞ synchronizer is shown in Fig. 4. The weighting function $W(s)$ in the exogenous signal is selected as $W(s) = 10 \times \frac{2.1Ls}{Ls+1}, L = 1 \times 10^{-3}$ and $\gamma = 0.75$ so as to stabilize the error system with time delay uncertainties. The H_∞ synchronizer is obtained by using MATLAB LMI toolbox as follows:

$$P(s) = \left[\begin{array}{c|c} a_k & b_k \\ \hline c_k & d_k \end{array}\right]$$
$$a_k = 10^5 \begin{bmatrix} -0.8762 & 1.9816 & -0.3890 & 0.0685 \\ 2.0890 & -4.7937 & 0.9380 & -0.1581 \\ -0.4425 & 1.0122 & -0.2074 & 0.0331 \\ -2.2132 & 5.3464 & -1.0531 & -0.0258 \end{bmatrix},$$
$$b_k = 10^5 \begin{bmatrix} 2.2024 & -0.0009 & 0.0114 \\ -5.3148 & 0.0046 & 0.0005 \\ 1.1245 & 0.0083 & 0.0008 \\ 5.8935 & 0.0186 & -0.1098 \end{bmatrix},$$
$$c_k = 10^3 \begin{bmatrix} -0.0549 & 0.2164 & -0.4198 & -5.4334 \end{bmatrix},$$
$$d_k = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}.$$

4.4 Nominal performance of H_∞-synchronizer

Figs. 5,6, and 7 show the responses of the Grassi-type decrypter and the H_∞-type decrypter of the nominal system. Fig 5 shows the plaintext and recovered signal for each decrypter. Fig 6 shows the transmitted signal and the estimation error of decrypter for each decrypter. Fig 7 shows the cipher text and the percentage error of the recovered signal for each decrypter. The nominal system means that the communication system has neither time delay nor parameter mismatches between the encrypter and the decrypter. The speed of response of the H_∞-type decrypter is faster than that of the Grassi-type.

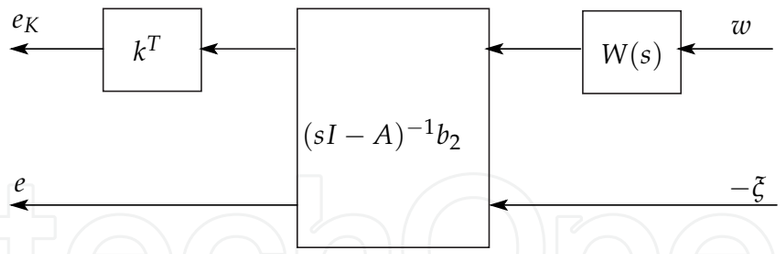


Fig. 4. Generalized plant $G_1(s)$.

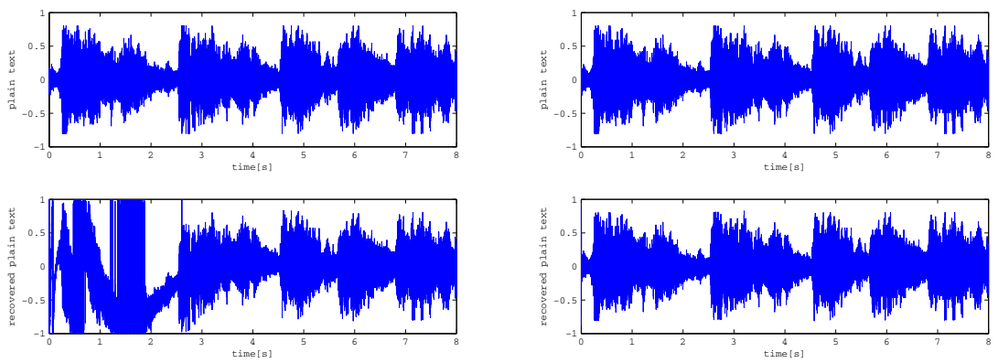


Fig. 5. The plaintext and the recovered plaintext in the nominal transmission line. Above left : the plaintext for the Grassi-type decrypter. Above right : the plaintext for the H_∞-synchronizer. Below left : the recovered plaintext by the Grassi-type decrypter. Below right : the recovered plaintext by the H_∞-synchronizer.

4.5 Robustness of H_∞-synchronizer against time delay in transmission line

Figs. 6 and 7 show the responses of the Grassi-type decrypter and the H_∞-type decrypter for the generalized plant $G_1(s)$in the presence of the time delay $L = 0.1$ in the transmission line, respectively. The responses of the H_∞-type decrypter for the generalized plant $G_2(s)$ in the presence of the time delay $L = 0.1$ in the transmission line is almost same as that for the generalized plant $G_1(s)$. The H_∞-type decrypter has a better robust performance to the time delay than the Grassi-type.

4.6 Security performance of H_∞-synchronizer

We assume that intruders have parameter mismatches in the decrypter. In this simulation, we consider the following parameter mismatches:

$$\hat{v} = P(s)\hat{x},\ \hat{e}_n = y - (\hat{v} + \tilde{f}(\hat{x}))$$

$$\tilde{A} = \begin{bmatrix} -p_1 & p_1 & 0 \\ 1 & -1 & 1 \\ 0 & -\tilde{p_2} & -p_3 \end{bmatrix}$$

$$\tilde{f}(x_1) = \tilde{G_b}x_1 + \frac{1}{2}(\tilde{G_a} - \tilde{G_b})(|x_1 + 1| - |x_1 - 1|)$$

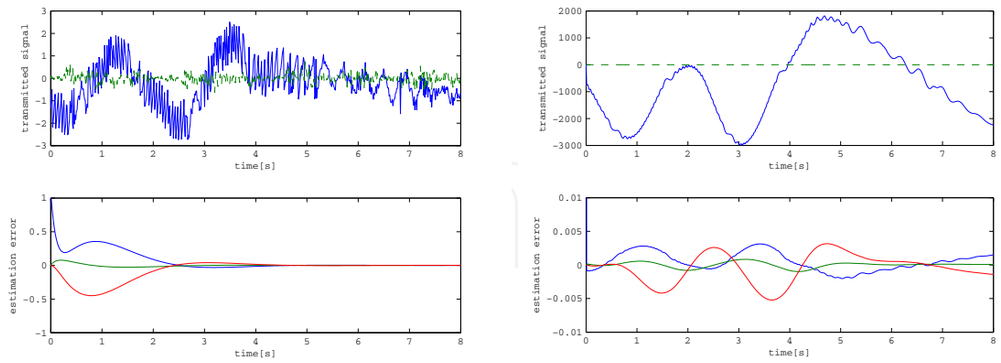


Fig. 6. The transmitted signal and the estimation error of decrypter in the nominal transmission line. Above left : the transmitted signal(solid line) and the plain text(dotted line) of the Grassi-type decrypter. Above right : the transmitted signal(solid line) and the plain text(dotted line) of the decrypter with the H_∞-synchronizer . Below left : the estimation errors of full states of the Grassi-type decrypter. Below right : the estimation errors of full states of the decrypter with the H_∞-synchronizer.

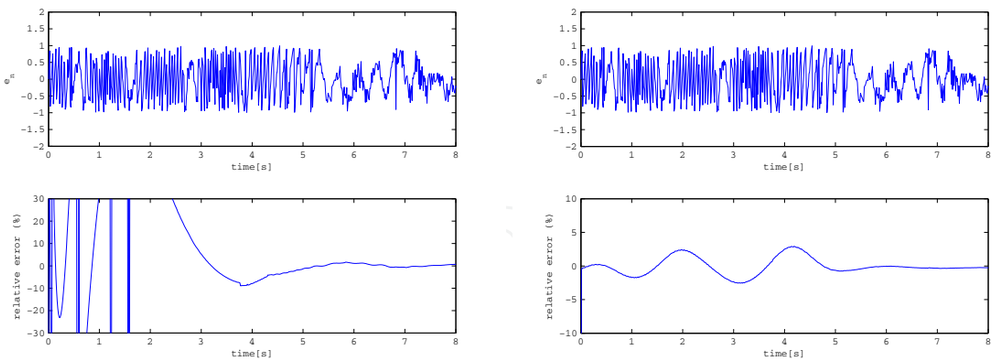


Fig. 7. The cipher text and the percentage error of the recovered signal in the nominal transmission line. Above left : the ciphertext in the Grassi-type decrypter. Above right : the ciphertext in the decrypter with the H_∞-synchronizer. Below left : the percentage error of the recovered signal of the Grassi-type decrypter. Below right : the percentage error of the recovered signal of the decrypter with the H_∞-synchronizer.

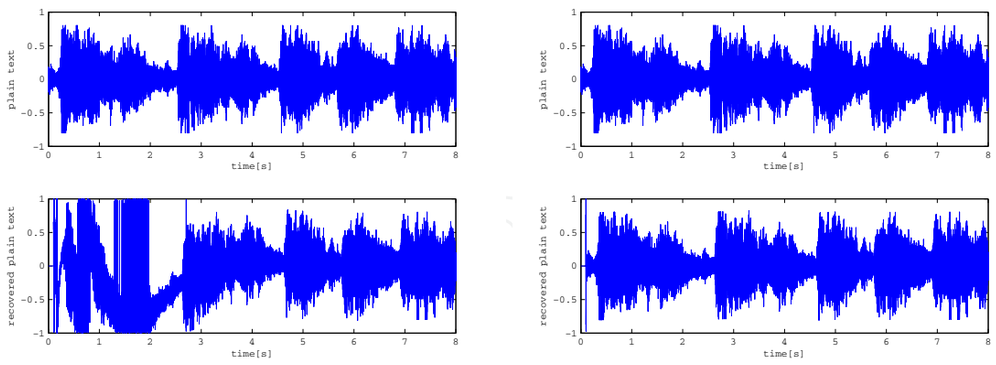


Fig. 8. The plaintext and the recovered plaintext in the transmission line with delay time. Above left : the plaintext for the Grassi-type decrypter. Above right : the plaintext for the H_∞-synchronizer. Below left : the recovered plaintext by the Grassi-type decrypter. Below right : the recovered plaintext by the H_∞-synchronizer.

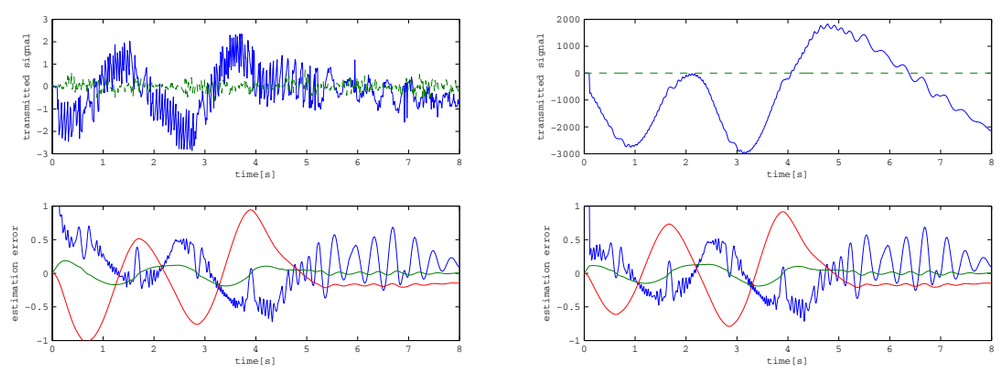


Fig. 9. The transmitted signal and the estimation error of the decrypter in the transmission line with delay time Above left : the transmitted signal(solid line) and the plain text(dotted line) of the Grassi-type decrypter. Above right : the transmitted signal(solid line) and the plain text(dotted line) of the decrypter with the H_∞-synchronizer . Below left : the estimation errors of full states of the Grassi-type decrypter. Below right : the estimation errors of full states of the decrypter with the H_∞-synchronizer.

In this simulation, we select the candidates of the static secret keys as the parameters p_2,G_a,G_b, and $P(s)$. Intruder A has the following parameter mismatch:

$$\tilde{p}_2 = 13.15, p_2 = 13.14$$
$$\tilde{G}_a = G_a = -1.28, \tilde{G}_b = G_b = -0.69$$
$$\tilde{P}(s) = P(s).$$

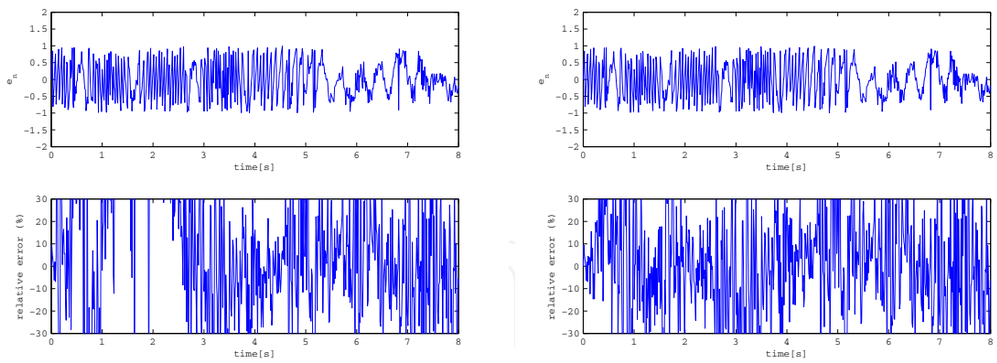


Fig. 10. The cipher text and the percentage error of the recovered signal in the transmission line with delay time. Above left : the ciphertext in the Grassi-type decrypter. Above right : the ciphertext in the decrypter with the H_∞-synchronizer. Below left : the percentage error of the recovered signal of the Grassi-type decrypter. Below right :the percentage error of the recovered signal of the decrypter with the H_∞-synchronizer.

Intruder B has the following parameter mismatches:

$$\tilde{p}_2 = p_2 = 13.14,$$
$$\tilde{G}_a = -1.3, \tilde{G}_b = -0.65$$
$$\tilde{P}(s) = P(s).$$

Figs. 11,12, and 13 show the responses of the H_∞-type decrypter used by the intruders A and B, respectively. The proposed synchronizer is sensitive to the parameter mismatches caused by Intruder A. The parameters in the dynamic encrypter may play the role of the secret key. However, Intruder A can identify the recovered `wav` file as the Handel's *Messiah* in spite of noisy sound. Fig. 14 shows the EFA function of the proposed H_∞-type decrypter. Since the width of the key basin in EFA function is not so narrow, the cryptosystem is not so secure.

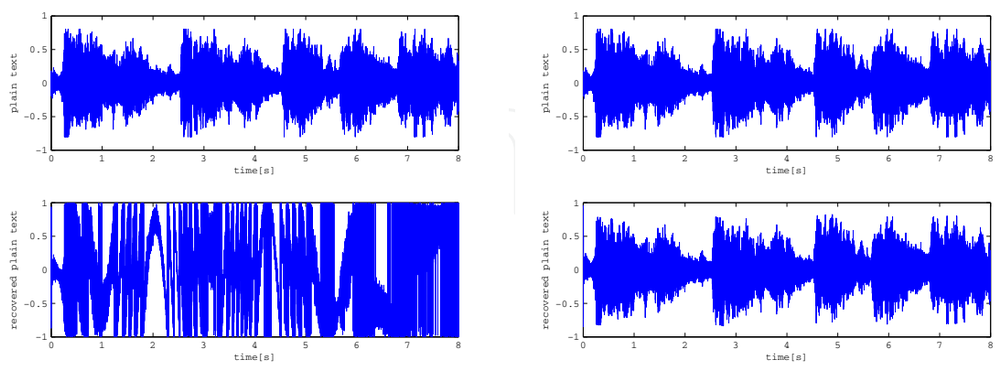


Fig. 11. The plaintext and the recovered plaintext by the intruders A and B. Above left : the plaintext. Above right : the plaintext. Below left : the recovered plaintext by Intruder A. Below right : the recovered plaintext by Intruder B.

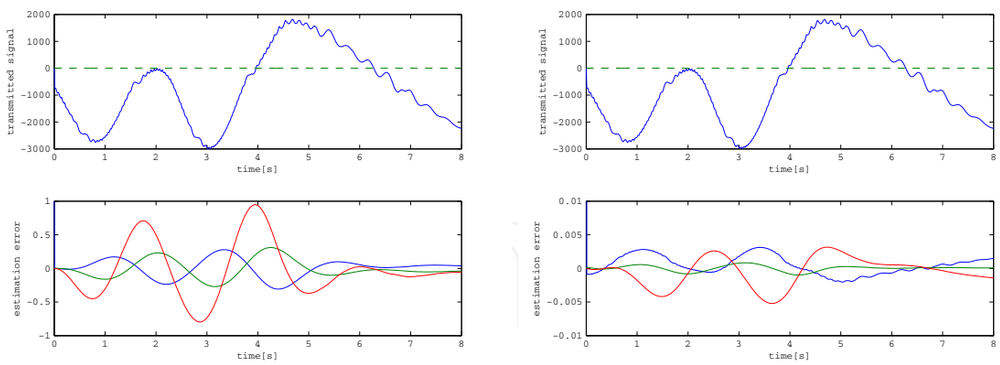


Fig. 12. The transmitted signals and the estimation errors of the intruders' decrypters. Above left : the transmitted signal(solid line) and the plain text(dotted line). Above right : the transmitted signal(solid line) and the plain text(dotted line). Below left : the estimation errors of full states by Intruder A. Below right : the estimation errors of full states by Intruder B.

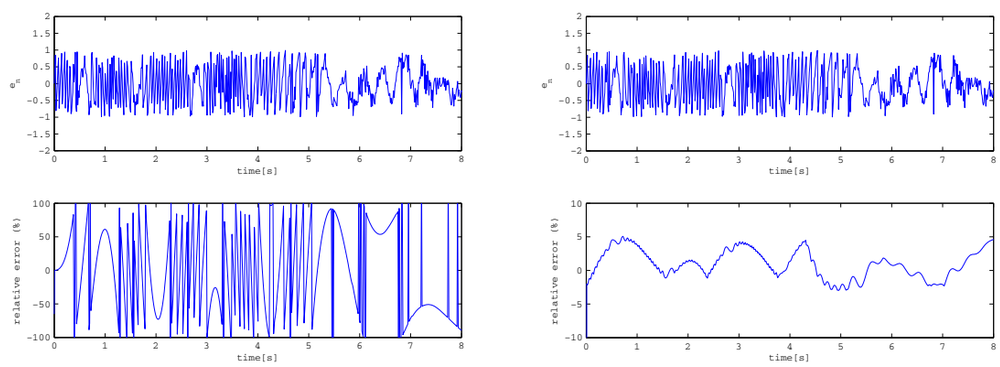


Fig. 13. The cipher text and the percentage error of the recovered signal in the transmission line with delay time. Above left : the ciphertext. Above right : the ciphertext. Below left : the percentage error of the recovered signal by Intruder A. Below right : the percentage error of the recovered signal by Intruder B.

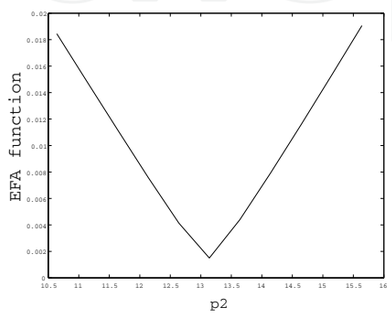


Fig. 14. The key basin of p_2 in EFA function for H_∞ synchronizer.

To improve the security of the H_∞ synchronizer, we select the secret key as a element of $P(s)$. Intruder C has the following parameter mismatch in the H_∞ synchronizer:

$$\tilde{p}_2 = p_2 = 13.14$$
$$\tilde{G}_a = G_a = -1.28, \tilde{G}_b = G_b = -0.69$$
$$\tilde{P}(s) = \left[\begin{array}{c|c} \tilde{a}_k & b_k \\ \hline c_k & d_k \end{array}\right]$$
$$\tilde{a}_k(1,1) = a_k(1,1) + 450$$

The parameter mismatch of the element $a_k(1,1)$ is about 0.51%, because $a_k(1,1) = -0.8762 \times 10^5$.
Figs. 15,16, and 17 show the responses of the H_∞-type decrypter used by Intruder C. In this case, the decrypter with the parameter mismatch causes instability. The parameters in the H_∞ synchronizer $\tilde{P}(s)$ may play the role of the secret key.

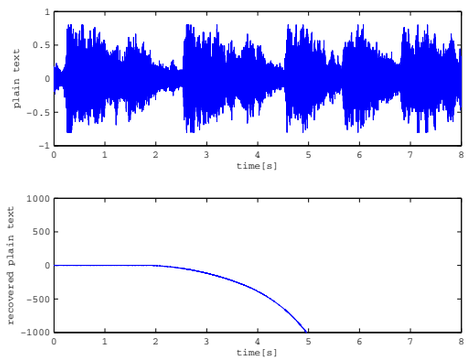


Fig. 15. The plaintext (top) and the recovered plaintext by Intruder C (bottom).

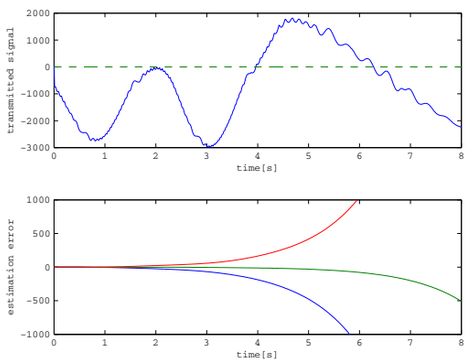


Fig. 16. The transmitted signal (top) and the estimation error of decrypter by Intruder C (bottom).

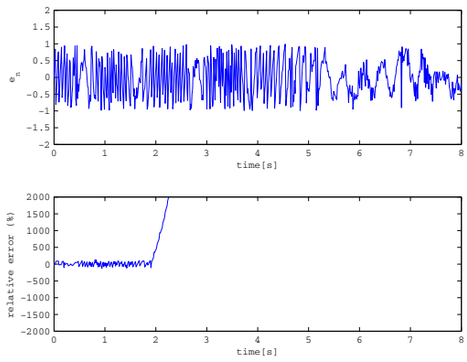


Fig. 17. The cipher text (top) and the percentage error of the recovered signal by Intruder C (bottom).

5. Conclusion

In this chapter, we added an observer-based chaotic communication system proposed by Grassi *et al.* to a dynamical compensator in its transmitted signal to improve the robustness of the cryptosystem with respect to delays in the transmission line. The proposed chaotic system has a good robust performance with respect to the time delay in the transmission line. Moreover, we checked the security in a point of parameters mismatch by an intruder.

6. References

Anstett,F.; Millerioux,G. & Bloch,G. (2006). Chaotic Cryptosystems : Cryptanalysis and Identifiability, *IEEE Trans. Circuits Syst. I*, Vol.53, No.12, pp.2673–2680

Alvarez,G. & Li, S. (2006). Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems, *Int. J. of Bifurcation and Chaos*, Vol.16, No.8, pp.2129-2151

Cuomo,K.M. & Oppenheim,A.V. (1993). Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications, *IEEE Trans. Circuits Syst. I*, Vol.40, pp.626-633

Dedieu,H. & Ogorzalek,M.J. (1997). Identifiability and Identification of Chaotic Systems Based on Adaptive Synchronization, *IEEE Trans. Circuits Syst. I*, Vol.44, pp.948-962

Doyle,J.C.; Glover,K.; Khargonekar,P.P. & Francis,B. A. (1989). State-Space Solutions to Standard H_2 and H_∞ Control Problems, *IEEE Trans. Automat. Contr.*, Vol.34, No.8, pp.831-846

Fradkov,A.L. & Markov,A.Y. (1997). Adaptive Synchronization of Chaotic Systems Based on Speed Gradient Method and Passification, *IEEE Trans. Circuits Syst. I*, Vol.44, No.10, pp.905–912.

Fradkov,A.L., Nijmeijer,H., & Markov,A.Y. (2000). Adaptive Observer-Based Synchronization for Communication, *Int. J. of Bifurcation and Chaos*, Vol.10. No.12, pp.2807-2813

Grassi,G. & Mascolo,S. (1999). A System Theory Approach for Designing Cryptosystems Based on Hyperchaos, *IEEE Trans. Circuits Syst. I*, Vol.46, No.9, pp.1135-1138

Guojie,H. Zhengjin,F., & Ruiling,M. (2003). Chosen Cipher Attack on Chaos Communication Based on Chaotic Synchronization, *IEEE Trans. Circuits Syst. I*, Vol.50, No.2, pp.275-279

Kocarev,L. (2001). Chaos-Based Cryptography: a Brief Overview, *IEEE Circuits and Systems Magazine*, Vol.1, No.3, pp.6-21

Liao,T.L. & Huang,N.S. (1999). An Observer-Based Approach for Chaotic Synchronization with Applications to Secure Communications, *IEEE Trans. Circuits Syst. I*, Vol.46, No.9, pp.1144-1149

Matsuo,T. & Nakano,K. (1998). Robust Stabilization of Closed-Loop Systems by PID+Q Controller, *Int. J. of Control*, Vol.70, No.4, pp.631-650

Matsuo,T., Suemitsu,H., & Nakano,K. (2004). Zeros and Relative Degree Assignments of Adaptive Chaotic Communication Systems, *Int.J. of Bifurcation and Chaos*, Vol.14, No.12, pp.4233-4247

Matsuo,T.; Toshimitsu,Y.; & Suemitsu,H. (2008). H_∞-Synchronizer for Chaotic Communication Systems, *Int.J. of Bifurcation and Chaos* Vol.18, No.4, pp.1175-1187

Millérioux,G.; Amigó,J. M. & Daafouz,J. (2008). A Connection between Chaotic and Conventional Cryptography, *IEEE Trans. on CAS–I*, Vol.55, No.6, pp.1695-1703

Nomura,T.; Irie,T.; Suemitsu,H. & Matsuo,T. (2011). Stochastic Security Testing for Chaotic Communication Systems against Error Function Attack, *IEEJ Trans. on Electrical and Electronic Engineering*, Vol.6, No.5, in press

Parker,A.T. & Short,K.M. (2001). Reconstructing the keystream from a chaotic encryption scheme, *IEEE Trans. on CAS–I*, Vol.48, No.5 pp.624-630

Short,K.M. (1994). Steps toward unmasking secure communications, *Int. J. Bifurcation and Chaos* Vol.4, No.44, pp.959-977

Short,K.M. (1996). Unmasking a modulated chaotic communications scheme, *Int. J. Bifurcation and Chaos*, Vol.6-, No.2, pp.367-375

Suykens,J.A.K.; Vandewalle,J. & Chua, L.O. (1997a). Nonlinear H_∞ Synchronization of Chaotic Lur'e Systems, *Int.J. of Bifurcation and Chaos*, Vol.7, No.6, pp.1323-1335

Suykens, J.A.K.; Curran, P.F.; Vandewalle, J. & Chua, L.O. (1997b). Robust Nonlinear H_∞ Synchronization of Chaotic Lur'e Systems, *IEEE Trans. Circuits Syst. I*, Vol.44, No.10, pp.891-904

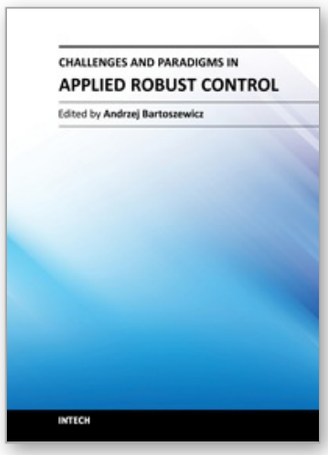
Wang,X; Zhan,M.; Lai,C.-H. & Gang,H. (2004). Error Function Attack of Chaos Synchronization Based on Encryption Schemes, *Chaos*, Vol.14, No.1, pp.128-137

Yang,T. & Chua,L.O. (1997a). Impulsive Control and Synchronization of Nonlinear Dynamical Systems and Application to Secure Communication, *Int. J. of Bifurcation and Chaos*, Vol.7, No.3, pp.645-664

Yang,T.; Wu,C.W. & Chua,L.O. (1997b). Cryptography Based on Chaotic Systems, *IEEE Trans. Circuits Syst. I*, Vol.44, pp.469-472

Yang,T. (2004). A Sruvey of Chaotic Secure Communication Systems, *Int.J. of Comput. Cogn.*, Vol.2, No,2, pp.81-130

Zhou,J.; Pei,W.; Huang,J.; Song,A. & He,Z. (2005). Differential-like Chosen Cipher Attack on A Spatiotemporally Chaotic Cryptosystem, nlin.CD/0506026



Challenges and Paradigms in Applied Robust Control

Edited by Prof. Andrzej Bartoszewicz

ISBN 978-953-307-338-5
Hard cover, 460 pages
Publisher InTech
Published online 16, November, 2011
Published in print edition November, 2011

The main objective of this book is to present important challenges and paradigms in the field of applied robust control design and implementation. Book contains a broad range of well worked out, recent application studies which include but are not limited to H-infinity, sliding mode, robust PID and fault tolerant based control systems. The contributions enrich the current state of the art, and encourage new applications of robust control techniques in various engineering and non-engineering systems.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Takami Matsuo, Yusuke Totoki and Haruo Suemitsu (2011). Robustness and Security of H∞-Synchronizer in Chaotic Communication System, Challenges and Paradigms in Applied Robust Control, Prof. Andrzej Bartoszewicz (Ed.), ISBN: 978-953-307-338-5, InTech, Available from: http://www.intechopen.com/books/challenges-and-paradigms-in-applied-robust-control/robustness-and-security-of-h-synchronizer-in-chaotic-communication-system

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen