Synchronizing chaotic PDE system using backstepping and its application to image encryption

Sano, Hideki

Wakaiki, Masashi

(Citation)
SICE Journal of Control, Measurement, and System Integration,15(2):182-190

(Issue Date)
2022-09-02

(Resource Type)
journal article

(Version)
Version of Record

SICE JOURNAL OF CONTROL, MEASUREMENT, AND SYSTEM INTEGRATION
2022, VOL. 15, NO. 2, 182–190
https://doi.org/10.1080/18824889.2022.2112528

Synchronizing chaotic PDE system using backstepping and its application to image encryption

Hideki Sano and Masashi Wakaiki

Department of Applied Mathematics, Graduate School of System Informatics, Kobe University, Kobe, Japan

ABSTRACT

This paper is concerned with the observer design problem for a nonlinear hyperbolic system with a modified van der Pol boundary condition in which an integral term is included. The observer plays a role of a chaotic synchronizing system when applying it to secure communication. In our previous work (Sano et al. Secure communication systems using distributed parameter chaotic synchronization. SICE Trans. 2021;57(2):78–85), a nonlinear hyperbolic system without the integral term was treated and a simple synchronizing system was constructed, where the constant coefficients of system played a role of encryption keys. But the keys were vulnerable from a safety standpoint. On the other hand, in the case where the integral term is included in the boundary condition, we need to construct observers. The weighted function contained in the integral term gives a new encryption key of distributed type. An application to image encryption is also discussed and numerical simulation results are given.

ARTICLE HISTORY
Received 17 January 2022
Revised 18 May 2022
Accepted 4 August 2022

KEYWORDS
Nonlinear hyperbolic system; van der Pol boundary condition; backstepping observer; synchronization; image encryption

1. Introduction

We shall consider the nonlinear hyperbolic system with a modified van der Pol boundary condition

$$\begin{cases} u_t(t,x) = u_x(t,x), & t>0,\ x\in(0,1),\\ v_t(t,x) = -v_x(t,x), & t>0,\ x\in(0,1),\\ u(t,1) = \phi(v(t,1)) + \displaystyle\int_0^1 \gamma(x)u(t,x)\,\mathrm{d}x, & t>0,\\ v(t,0) = \kappa u(t,0), & t>0,\\ u(0,x) = u_0(x), \quad v(0,x) = v_0(x), & x\in[0,1], \end{cases} \tag{1}$$

where $\gamma(x)$ is a real-valued function such that $\gamma\in C^1[0,1]$ and $\gamma(0)=0$, and κ is a real constant. For a given $z\in\mathbf{R}$, $\phi(z)$ expresses a solution y to the equation

$$\beta(y-z)^3 + (1-\alpha)(y-z) + 2z = 0. \tag{2}$$

That is, $\phi(z)=y$. For each $z\in\mathbf{R}$, Equation (2) has a unique solution $y\in\mathbf{R}$, if the conditions $0<\alpha\le 1$ and $\beta>0$ are satisfied (e.g. [1]). Hereafter, it is assumed that α and β are chosen such that $0<\alpha\le 1$ and $\beta>0$. If $\gamma(x)\equiv 0$, then we obtain the nonlinear hyperbolic system (1) from a wave equation with a van der Pol boundary condition, and u, v are the Riemann invariants of the wave equation; see, e.g. [1].

Using the method of characteristic lines, we can characterize the solution of system (1). First, we express the boundary condition of (1) as

$$u(t,1) = \phi(v(t,1)) + f(u(t,\cdot)), \quad v(t,0) = \psi(u(t,0)),$$

where

$$f(\varphi) := \int_0^1 \gamma(x)\varphi(x)\,\mathrm{d}x, \quad \varphi\in L^2(0,1),$$
$$\psi(x) := \kappa x, \quad x\in\mathbf{R},$$

with $\gamma(x)$ and κ being the same function and constant as in (1). Considering the reflection of wave at $x=0,1$, the solution (u,v) of (1) is determined as follows (see Appendix 1): For $x\in[0,1]$ and $t=2k+\tau$ $(k=0,1,2,\dots,\ 0\le\tau<2)$,

$$u(t,x) = \begin{cases} u_k(x+\tau), & \text{for } \tau\le 1-x,\\ \phi(v_k(2-x-\tau)) & \\ \quad +f(u(2k-1+x+\tau,\cdot)), & \text{for } 1-x<\tau\\ & \le 2-x,\\ (\phi\circ\psi)(u_k(x+\tau-2)) & \\ \quad +f(u(2k-1+x+\tau,\cdot)), & \text{for } 2-x\\ & <\tau\le 2, \end{cases}$$

$$v(t,x) = \begin{cases} v_k(x-\tau), & \text{for } \tau\le x,\\ \psi(u_k(\tau-x)), & \text{for } x<\tau\le 1+x,\\ (\psi\circ\phi)(v_k(x-\tau+2)) & \\ \quad +(\psi\circ f) & \\ \quad (u(2k-1+\tau-x,\cdot)), & \text{for } 1+x<\tau\le 2, \end{cases}$$

where $u_k(x)$ and $v_k(x)$ are defined as

$$u_k(x) := (\phi\circ\psi)(u_{k-1}(x)) + f(u(2k-1+x,\cdot)),$$

CONTACT Hideki Sano sano@crystal.kobe-u.ac.jp, sano@cs.kobe-u.ac.jp Department of Applied Mathematics, Graduate School of System Informatics, Kobe University, 1-1 Rokkodai, Nada, Kobe 657-8501, Japan

$$v_k(x) := (\psi \circ \phi)(v_{k-1}(x)) + (\psi \circ f)(u(2k-1-x, \cdot)),$$

with ϕ being implicitly defined by (2). In the above, we assume that the initial condition $u_0, v_0 \in H^1(0,1)$ satisfies the compatible conditions $u_0(1) = \phi(v_0(1)) + f(u_0(\cdot))$, $v_0(0) = \psi(u_0(0))$. Although it is difficult to show the well-posedness of (1) within the framework of functional analysis, we can directly determine the solution.

For the wave equation with a van der Pol boundary condition not including an integral term, the observer design has been studied in [2]. In this paper, we first construct observers for (1) with $\gamma(x) \not\equiv 0$, and then apply them to image encryption as an example of secure communication. For lumped parameter systems, secure communication systems using chaotic synchronization have been investigated by many researchers since the mid-1990s. The common idea is the following: After communication information is embedded into a chaotic signal in the modulation component, it is sent to the receiving side, and, in the demodulation component, the communication information is restored by chaotic synchronization [3–7]. Here, chaotic synchronization is a phenomenon such that two systems whose states chaotically behave with the same dynamic characteristics are synchronized by adding a control input to one system. For example, it is accomplished by constructing observers. On the other hand, there are a few works concerning the design of secure communication systems using the chaos of PDEs [8–10]. In [9], it has been shown that two identical time-delayed Chua's circuits can be synchronized using a boundary control and that the synchronization can be applied to multichannel spread-spectrum communications. In [8], for two identical systems (1) with $\gamma(x) \equiv 0$, it has been shown that they can be synchronized by a simple control law, based on the method of characteristic line and that the synchronization is applicable to image encryption, where the constants α, β, κ of (1) and (2) play a role of encryption keys. In [10], an image encryption scheme has been proposed based on a hyperbolic system with nonlinear boundary conditions, which brings a chaotic phenomenon. In that paper, the solution of the hyperbolic system is used to shuffle the position of each pixel. However, the method of synchronize two identical hyperbolic systems is not considered. That is, in [10], the encryption and decryption are assumed to be done non-simultaneously.

In the case where an integral term is included in the boundary condition such as system (1), we need to construct observers for synchronization. Especially, we use backstepping design for first-order hyperbolic systems (see, e.g. [11–19]). The merit of using the integral term lies in the fact that the weighted function $\gamma(x)$ gives an additional 'distributed' encryption key.

2. Observer design for synchronization

To estimate the states $u(t,\cdot)$ and $v(t,\cdot)$ of (1) from the output $v(t,1)$, we consider the 2×2 nonlinear hyperbolic system

$$\begin{cases} \hat{u}_t(t,x) = \hat{u}_x(t,x) + g(x)(v(t,1) - \hat{v}(t,1)), \\ \qquad t > 0,\ x \in (0,1), \\ \hat{v}_t(t,x) = -\hat{v}_x(t,x) + h(x)(v(t,1) - \hat{v}(t,1)), \\ \qquad t > 0,\ x \in (0,1), \\ \hat{u}(t,1) = \phi(v(t,1)) + \displaystyle\int_0^1 \gamma(x)\hat{u}(t,x)\,\mathrm{d}x, \quad t > 0, \\ \hat{v}(t,0) = \kappa \hat{u}(t,0), \quad t > 0, \\ \hat{u}(0,x) = \hat{u}_0(x), \quad \hat{v}(0,x) = \hat{v}_0(x), \quad x \in [0,1], \end{cases} \tag{3}$$

where it is assumed that $\hat{u}_0, \hat{v}_0 \in H^1(0,1)$, $\hat{u}_0(1) = \phi(v_0(1)) + f(\hat{u}_0(\cdot))$, $\hat{v}_0(0) = \psi(\hat{u}_0(0))$. System (3) is called a Luenberger-type observer. Introducing the error variables $\tilde{u} := u - \hat{u}$ and $\tilde{v} := v - \hat{v}$, the following system is obtained:

$$\begin{cases} \tilde{u}_t(t,x) = \tilde{u}_x(t,x) - g(x)\tilde{v}(t,1), \\ \qquad t > 0,\ x \in (0,1), \\ \tilde{v}_t(t,x) = -\tilde{v}_x(t,x) - h(x)\tilde{v}(t,1), \\ \qquad t > 0,\ x \in (0,1), \\ \tilde{u}(t,1) = \displaystyle\int_0^1 \gamma(x)\tilde{u}(t,x)\,\mathrm{d}x, \quad t > 0, \\ \tilde{v}(t,0) = \kappa \tilde{u}(t,0), \quad t > 0, \\ \tilde{u}(0,x) = \tilde{u}_0(x), \quad \tilde{v}(0,x) = \tilde{v}_0(x), \quad x \in [0,1]. \end{cases} \tag{4}$$

The main difference from [17, 18] is that system (1) has the nonlinear function ϕ in the boundary condition at $x = 1$. However, a suitable choice of observers leads to a linear error system. Hence, one can apply the backstepping method to the error system (4) as in [17, 18]. In particular, we use the Volterra–Fredholm integral transformation

$$w(t,x) = \tilde{u}(t,x) - \int_0^x p(x,y)\tilde{u}(t,y)\,\mathrm{d}y - \int_0^1 q(x,y)\tilde{v}(t,y)\,\mathrm{d}y. \tag{5}$$

The problem is to determine the kernels p and q in (5) and the gains g and h in (4) so as to achieve $\tilde{u}(t,\cdot) \to 0$ and $\tilde{v}(t,\cdot) \to 0$ as t goes to ∞.

Differentiating (5) and performing integration by parts, $w_t(t,x) - w_x(t,x)$ is calculated as

$$w_t(t,x) - w_x(t,x) = \left\{ q(x,1) - g(x) + \int_0^x p(x,y)g(y)\,\mathrm{d}y + \int_0^1 q(x,y)h(y)\,\mathrm{d}y \right\} \tilde{v}(t,1)$$

$$+\{p(x,0)-\kappa q(x,0)\}\tilde{u}(t,0)+\int_0^x\{p_x(x,y)+p_y(x,y)\}\tilde{u}(t,y)\,\mathrm{d}y+\int_0^1\{q_x(x,y)-q_y(x,y)\}\tilde{v}(t,y)\,\mathrm{d}y. \tag{6}$$

We here note the following facts:

(i) If all the terms enclosed in $\{\cdot\}$ of the right-hand side of (6) are zero, $w_t(t,x)-w_x(t,x)=0$ holds for all $\tilde{u}$ and $\tilde{w}$.
(ii) By (5), if $p(1,y)=\gamma(y)$ and $q(1,y)=0$ are satisfied, $w(t,1)=0$ holds for all $\tilde{u}$.
(iii) Putting $x=0$ in (5), one has

$$w(t,0)=\tilde{u}(t,0)-\int_0^1 q(0,y)\tilde{v}(t,y)\,\mathrm{d}y.$$

Under the condition $\gamma(0)=0$, we sequentially determine the kernels p and q and the gains g and h as follows:

Step 1 – Design of $\boldsymbol{p}$. 'Attention to (6) and (i), (ii)'. Let $D_p:=\{(x,y);\,0\le y\le x,\,0\le x\le 1\}$. Find the solution $p(x,y)$ to the hyperbolic equation

$$\begin{cases} p_x(x,y)+p_y(x,y)=0,\\ p(1,y)=\gamma(y)\end{cases} \tag{7}$$

on D_p. From (7), the solution is given by $p(x,y)=\gamma(1-x+y)$.

Step 2 – Design of $\boldsymbol{q}$. 'Using p, find q'. 'Attention to (6) and (i), (ii)'. Let $D_q:=\{(x,y);\,0\le x\le 1,\,0\le y\le 1\}$. Find the solution $q(x,y)$ to the hyperbolic equation

$$\begin{cases} q_x(x,y)-q_y(x,y)=0,\\ q(x,0)=\dfrac{1}{\kappa}p(x,0),\\ q(1,y)=0\end{cases} \tag{8}$$

on D_q. From (8), the solution is given by

$$q(x,y)=\begin{cases}\dfrac{1}{\kappa}\gamma(1-x-y), & \text{for } x+y\le 1,\\ 0, & \text{for } x+y>1.\end{cases}$$

Note that $q\in H^1(D_q)$ under the condition $\gamma(0)=0$.

Step 3 – Design of $\boldsymbol{h}$. 'Using q, find h'. 'Attention to (4) and (iii)'. Determine the gain $h(x), x\in[0,1]$ such that the solution $\tilde{v}(t,\cdot)$ of the hyperbolic Equation (9) vanishes for all $t\ge 1$.

$$\begin{cases}\tilde{v}_t(t,x)=-\tilde{v}_x(t,x)-h(x)\tilde{v}(t,1),\\ \tilde{v}(t,0)=\kappa\displaystyle\int_0^1 q(0,y)\tilde{v}(t,y)\,\mathrm{d}y,\\ \tilde{v}(0,x)=\tilde{v}_0(x).\end{cases} \tag{9}$$

Concretely, one can construct the gain h by solving Equations (10) and (11).

$$\begin{cases} r_x(x,y)+r_y(x,y)=0, & x\le y\le 1,\ 0\le x\le 1,\\ r(0,y)=\kappa q(0,y),\end{cases} \tag{10}$$

$$h(x)=r(x,1)+\int_x^1 r(x,y)h(y)\,\mathrm{d}y. \tag{11}$$

The derivation is shown in Appendix 2. Since it follows from (10) that $r(x,y)=\kappa q(0,y-x)$, the gain h is given by solving the integral Equation (11).

Step 4 – Design of $\boldsymbol{g}$. 'Using p, q, h, find g'. 'Attention to (6) and (i)'. Find the solution $g(x)$, $x\in[0,1]$ to the integral equation

$$g(x)=q(x,1)+\int_0^1 q(x,y)h(y)\,\mathrm{d}y+\int_0^x p(x,y)g(y)\,\mathrm{d}y. \tag{12}$$

As a result, for the error system (4), the following system can be considered as a target system:

$$\begin{cases} w_t(t,x)=w_x(t,x),\\ w(t,1)=0,\\ w(0,x)=w_0(x),\\ \hline \tilde{v}_t(t,x)=-\tilde{v}_x(t,x)-h(x)\tilde{v}(t,1),\\ \tilde{v}(t,0)=\kappa w(t,0)+\kappa\displaystyle\int_0^1 q(0,y)\tilde{v}(t,y)\,\mathrm{d}y,\\ \tilde{v}(0,x)=\tilde{v}_0(x).\end{cases} \tag{13}$$

For the upper part of system (13), we see that $w(t,\cdot)$ becomes zero at $t=1$, since

$$w(t,x)=\begin{cases} w_0(x+t), & \text{for } x+t\le 1,\\ 0, & \text{for } x+t>1.\end{cases}$$

Therefore, at $t=1$, the lower part of system (13) equals the hyperbolic Equation (9). From the way of construction of the gain h in the Step 3, $\tilde{v}(t,\cdot)$ becomes zero at $t=2$. On the other hand, it follows from (5) that

$$0=\tilde{u}(t,x)-\int_0^x p(x,y)\tilde{u}(t,y)\,\mathrm{d}y\quad\text{for } t\ge 2.$$

From the invertibility [20] of the transformation $\mathcal{T}: H^1(0,1)\to H^1(0,1)$ defined by

$$\mathcal{T}\tilde{u}(t,x)=\tilde{u}(t,x)-\int_0^x p(x,y)\tilde{u}(t,y)\,\mathrm{d}y,$$

we see that $\tilde{u}(t,\cdot)$ and $\tilde{v}(t,\cdot)$ vanish for $t\ge 2$. Now, we introduce a Hilbert space $X:=L^2(0,1)\times L^2(0,1)$ and its subspace

$$W:=\left\{(\mu,\nu)\in H^1(0,1)\times H^1(0,1);\ \mu(1)=\int_0^1\gamma(y)\mu(y)\,\mathrm{d}y,\ \nu(0)=\kappa\mu(0)\right\}.$$

Then, we have the following theorem:

Theorem 2.1: *Let* $\gamma\in C^1[0,1]$ *satisfy* $\gamma(0)=0$. *Let* g *and* h *be designed according to Steps* 1–4. *Then, for any initial condition* $(\tilde{u}_0,\tilde{v}_0)\in W$, *the error system* (4) *has a*

unique solution $(\tilde{u}, \tilde{v}) \in C([0,\infty); W) \cap C^1([0,\infty); X)$ *which vanishes for* $t \geq 2$.

Proof: The theorem can be proved by using a way similar to [17, Theorem 3]. So, we here omit it. ■

Remark 2.1: The gains g and h constructed in this section satisfy $(g, h) \in W$, where W is the subspace of X defined before Theorem 2.1. See Appendix 3 for the derivation.

3. Application to image encryption

In this section, we study the modulation/demodulation of image data with $(M+1) \times (L+1)$ pixel. We first need to discretize system (1) and synchronization system (3) to spatial direction and time direction. Divide the interval $[0,1]$ into L equal subintervals and define $x_i := i\Delta x$ $(i = 0, 1, 2, \ldots, L)$, where $\Delta x := 1/L$. Let Δt be a time mesh width and define $t_k := k\Delta t$ $(k = 0, 1, 2, \ldots)$. For the states $u(t,x)$, $v(t,x)$ of system (1), let $u_i[k]$, $v_i[k]$ be numerical solutions that approximate $u(t_k, x_i)$ and $v(t_k, x_i)$, and define the $(L+1)$-dimensional vectors

$$u[k] := \begin{bmatrix} u_0[k] \\ u_1[k] \\ \vdots \\ u_L[k] \end{bmatrix}, \quad v[k] := \begin{bmatrix} v_0[k] \\ v_1[k] \\ \vdots \\ v_L[k] \end{bmatrix}.$$

For synchronization system (3), in the same fashion, using numerical solutions $\hat{u}_i[k]$, $\hat{v}_i[k]$ that approximate $\hat{u}(t_k, x_i)$, $\hat{v}(t_k, x_i)$, we define the $(L+1)$-dimensional vectors

$$\hat{u}[k] := \begin{bmatrix} \hat{u}_0[k] \\ \hat{u}_1[k] \\ \vdots \\ \hat{u}_L[k] \end{bmatrix}, \quad \hat{v}[k] := \begin{bmatrix} \hat{v}_0[k] \\ \hat{v}_1[k] \\ \vdots \\ \hat{v}_L[k] \end{bmatrix}.$$

To discretize these systems to spatial direction, we use the upwind difference scheme, that is,

$$\begin{aligned} u_x(t_k, x_i) &\cong \frac{u(t_k, x_{i+1}) - u(t_k, x_i)}{\Delta x}, \\ -v_x(t_k, x_i) &\cong -\frac{v(t_k, x_i) - v(t_k, x_{i-1})}{\Delta x}, \\ \hat{u}_x(t_k, x_i) &\cong \frac{\hat{u}(t_k, x_{i+1}) - \hat{u}(t_k, x_i)}{\Delta x}, \\ -\hat{v}_x(t_k, x_i) &\cong -\frac{\hat{v}(t_k, x_i) - \hat{v}(t_k, x_{i-1})}{\Delta x}. \end{aligned}$$

Further, for its time integration of u, v, $\hat{u}$, and $\hat{v}$, we use the Euler method with time mesh width $\Delta t = \Delta x$. Hereafter, we denote Equation (1) discretized system by $\Sigma_{(1)}$, and Equation (3) discretized system by $\Sigma_{(3)}$.

Remark 3.1: The above discretization is the upwind difference scheme based on the characteristic line. Since $\Delta t = \Delta x$, the waves u and $\hat{u}$ travel along the characteristic line $t + x = \text{const}$, and the waves v and $\hat{v}$ travel along the characteristic line $t - x = \text{const}$.

In what follows, we state the concrete construction of system in the case where one transmits an image data from subsystem S_1 to subsystem S_2.

Modulation

$$\mathrm{M}: \begin{cases} \omega[k+1] = G(\hat{u}[k], \hat{v}[k], \omega[k], s_1[k+1]), \\ \qquad\qquad k \geq 0, \quad \omega[0] = 0, \\ c_{12}[k] = \omega[k], \end{cases} \tag{14}$$

where $\omega[k]$ is the modulated state. G is a nonlinear mapping from $\mathbf{R}^{L+1} \times \mathbf{R}^{L+1} \times \mathbf{R}^{L+1} \times \mathbf{R}^{L+1}$ to $\mathbf{R}^{L+1}$. It is assumed that, for arbitrarily fixed $a, b, c \in \mathbf{R}^{L+1}$, $G(a, b, c, \cdot)$ has the inverse $G^{-1}(a, b, c, \cdot)$ and satisfies the following condition:

Condition 3.1: *For any real number* $\varepsilon > 0$, *there exists a real number* $\delta > 0$ *such that*

$$|\xi_1 - \xi_2|_{\mathbf{R}^{L+1}} < \delta \quad (\xi_1, \xi_2 \in \mathbf{R}^{L+1}) \implies$$
$$\sup_{a,b,c \in \mathbf{R}^{L+1}} |G^{-1}(a, b, c, \xi_1) - G^{-1}(a, b, c, \xi_2)|_{\mathbf{R}^{L+1}} < \varepsilon,$$

where $|\cdot|_{\mathbf{R}^{L+1}}$ *denotes the usual Euclidean norm.*

Especially, we choose G such that $\omega[k]$ of (14) behaves randomly and differently from $\hat{u}[k]$ and $\hat{v}[k]$ so that the original image cannot be found at all in the modulated image $\{c_{12}[k]\}$.

Demodulation

$$\begin{aligned} \mathrm{D}: \ & t_2[k+1] \\ & = G^{-1}(u[k-1], v[k-1], c_{12}[k-1], c_{12}[k]), \\ & \quad k \geq 1. \end{aligned} \tag{15}$$

Then, noting that $\Delta t = \Delta x$, we see that, after $k = 2L$ steps, $\hat{u}[k]$, $\hat{v}[k]$ are completely equal to $u[k]$, $v[k]$, respectively. As a result, after the same steps, $t_2[k+1]$ is completely equal to $s_1[k]$ under Condition 3.1. Figure 1 is the diagram when the synchronization system (3) is used. In the case where an image data of $(M+1) \times (L+1)$ pixel is transmitted from S_1 to S_2 , after a lapse of runup time, we have to set the original image data to $s_1[k] \in \mathbf{R}^{L+1}$ row by row and perform the sending operation $(M+1)$ times. On the other hand, on the receiving side, the image data of $(M+1) \times (L+1)$ pixel is restored by stocking up with $t_2[k] \in \mathbf{R}^{L+1}$ in sequence.

4. Numerical simulation

In this numerical simulation, a monochrome image of 145×305 pixel (i.e. $M = 144$, $L = 304$) is used. In the system (1), we set $\alpha = 0.5$, $\beta = 1$, $\gamma(x) = 2\sin(7\pi x)$,

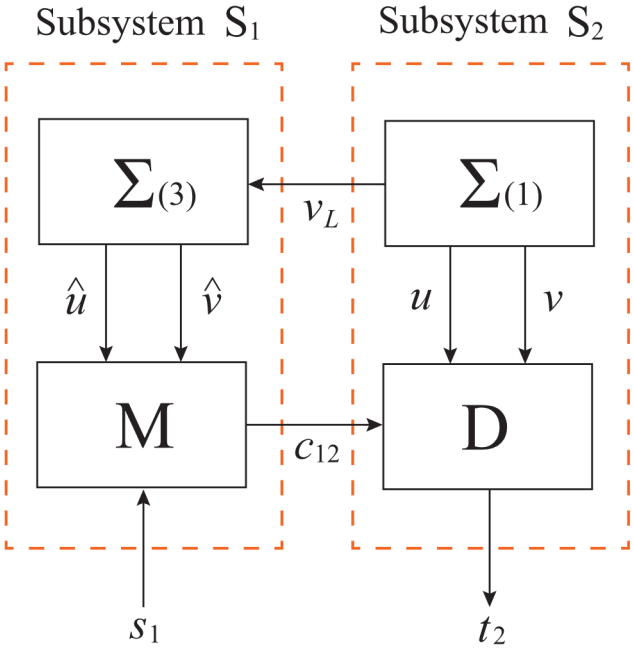

Figure 1. Secure communication system. $\Sigma_{(1)}$: Equation (1) discretized system. $\Sigma_{(3)}$: Equation (3) discretized system. M: modulation (14). D: demodulation (15). $\{s_1[k]\}$: original image. $\{c_{12}[k]\}$: modulated image. $\{t_2[k]\}$: restored image.

and $\kappa = \frac{1+\eta}{1-\eta}$, where $\eta = 0.525$. According to Steps 1–4, we can design the observer gains g and h. First of all, by Steps 1 and 2, we get the kernels p and q. As for the function $h(x), x \in [0,1]$, which should be solved in Step 3, we already know $r(x,y) = \kappa q(0, y-x)$. By a method of successive approximation, the integral equation w.r.t. $h(x)$ can be solved by the scheme

$$h_m(x) = r(x,1) + \int_x^1 r(x,y)h_{m-1}(y)\,\mathrm{d}y, \quad h_0(x) \equiv C.$$

Furthermore, in Step 4, the integral equation w.r.t. $g(x)$, $x \in [0,1]$ can be solved by the scheme

$$g_n^m(x) = q(x,1) + \int_0^1 q(x,y)h_m(y)\,\mathrm{d}y + \int_0^x p(x,y)g_{n-1}^m(y)\,\mathrm{d}y, \quad g_0^m(x) \equiv C.$$

In this numerical simulation, we set the initial constant as $C = 1$ and the spatial mesh width as $\Delta x = \Delta y = 1/304$. Also, we set each iteration of successive approximation as 9 times, that is, $(m,n) = (9,9)$. In Figure 2, the graphs of gains $h_9(x)$, $g_9^9(x)$ were plotted. Throughout this computation, we could verify the following facts:

(i) $g_9^9(1) = 0.3618$, $\int_0^1 \gamma(x)g_9^9(x)\,\mathrm{d}x = 0.3618$, that is, $g_9^9(1) = \int_0^1 \gamma(x)g_9^9(x)\,\mathrm{d}x$.
(ii) $h_9(0) = 1.7914$, $\kappa g_9^9(0) = 1.7914$, that is, $h_9(0) = \kappa g_9^9(0)$.

This shows that $g(x) = g_9^9(x)$ and $h(x) = h_9(x)$ satisfy $(g,h) \in W$ numerically (see Remark 2.1).

To perform numerical simulations, we set the modulation and demodulation components. Indeed, since the mapping G of (14) is nonlinear, it is difficult to construct G in a systematic way. In this paper, we extend the modulation and demodulation components of [5] so that each argument of G can take a vector value (see Remark 4.1). In (14), let us set

$$\begin{aligned} &G(a,b,c,\xi) \\ &\quad = H(c)(0.03|a|_V + 0.03|b|_V) \\ &\qquad + (0.5H(c) + 0.1I)(0.08|a|_V + 0.08|b|_V + \xi), \end{aligned}$$

where $a,b,c,\xi \in \mathbf{R}^{L+1}$ and I is the $(L+1)\times(L+1)$ identity matrix. For vector $z = (z_0, z_1, \ldots, z_L)^{\mathrm{T}}$, we introduce the notation

$$\begin{aligned} &H(z) := \mathrm{diag}(|z_0(1-z_0)|, \ldots, |z_L(1-z_L)|), \\ &|z|_V := (|z_0|, |z_1|, \ldots, |z_L|)^{\mathrm{T}}. \end{aligned}$$

Then, G^{-1} of (15) is calculated as

$$\begin{aligned} &G^{-1}(a,b,c,\xi) \\ &\quad = (0.5H(c) + 0.1I)^{-1}[\xi - H(c)(0.03|a|_V \\ &\qquad + 0.03|b|_V)] - 0.08|a|_V - 0.08|b|_V. \end{aligned}$$

For any $c \in \mathbf{R}^{L+1}$, the norm (i.e. the maximal singular value) of matrix $(0.5H(c) + 0.1I)^{-1}$ is estimated as $\|(0.5H(c) + 0.1I)^{-1}\| \le 10$. Hence, G^{-1} satisfies Condition 3.1. Figure 3 shows the numerical simulation result in the case of runup time $k = 6080$ steps $(t = 20)$. Here, we set $u_0(x) = \phi(v_0(1))e^{\frac{2}{7\pi}(1-\cos 7\pi x)}$ and $v_0(x) = (v_0(1) - \kappa\phi(v_0(1)))x + \kappa\phi(v_0(1))$ with $v_0(1) = 0.1$, and $\hat{u}_0(x) = u_0(x) + g_9^9(x)$, $\hat{v}_0(x) = v_0(x) + h_9(x)$, where these satisfy the compatible conditions with respect to the initial conditions of (1) and (3), since $(g_9^9, h_9) \in W$. Let the value of black be 0 and that of white be 0.01. The maximum of error between the original image $\{s_1[k]\}$ and the restored one $\{t_2[k]\}$ was 1.0408×10^{-16}.

Next, we consider the case where the weighted function contained in the nonlocal boundary condition of system (1) fluctuates from $\gamma(x) = 2\sin(7\pi x)$ to $\overline{\gamma}(x) = 1.95\sin(6.75\pi x)$ (see Figure 4). The function $\gamma(x)$ contained in system (3) remains the same. Then, using the same observer gains g and h as in Figure 2, we had a numerical simulation result shown in Figure 5, where the same initial condition and the same runup time as in Figure 3 were used. We cannot find the original image at all from the restored image. In this case, the maximum of error between the original image $\{s_1[k]\}$ and the restored one $\{t_2[k]\}$ was 0.5689. From the right column of Figure 5, we see that the error system with states $\tilde{u}$ and $\tilde{v}$ is destabilizing due to a small discrepancy in the function $\gamma(x)$.

Remark 4.1: In [5], two chaotic systems using the 2-dimensional Hénon mapping are considered. In that

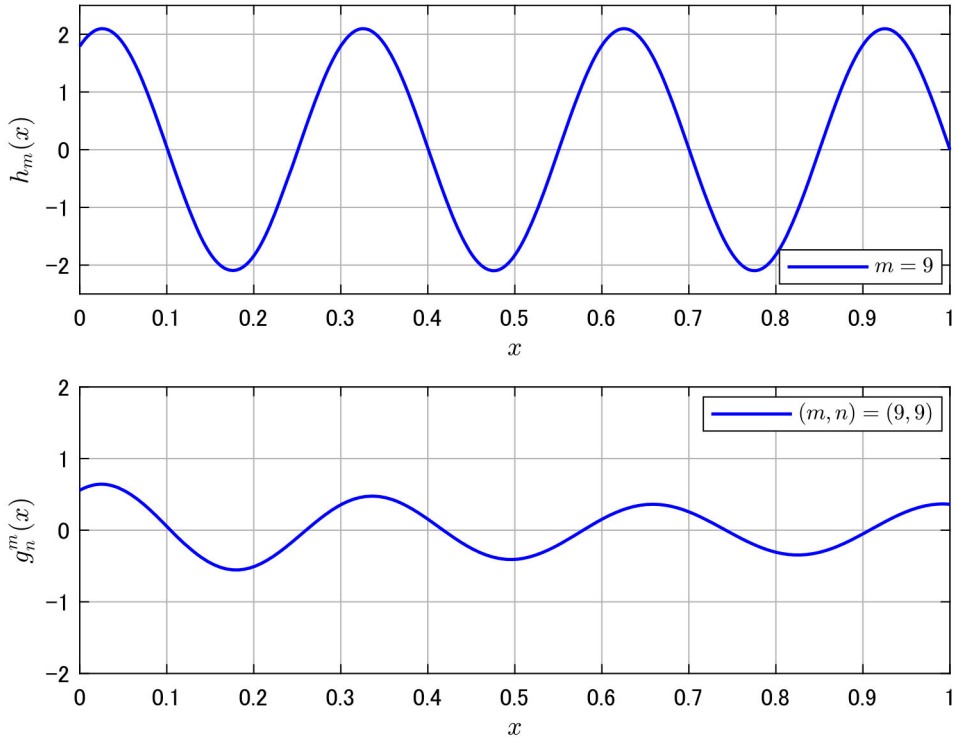

Figure 2. Observer gains.

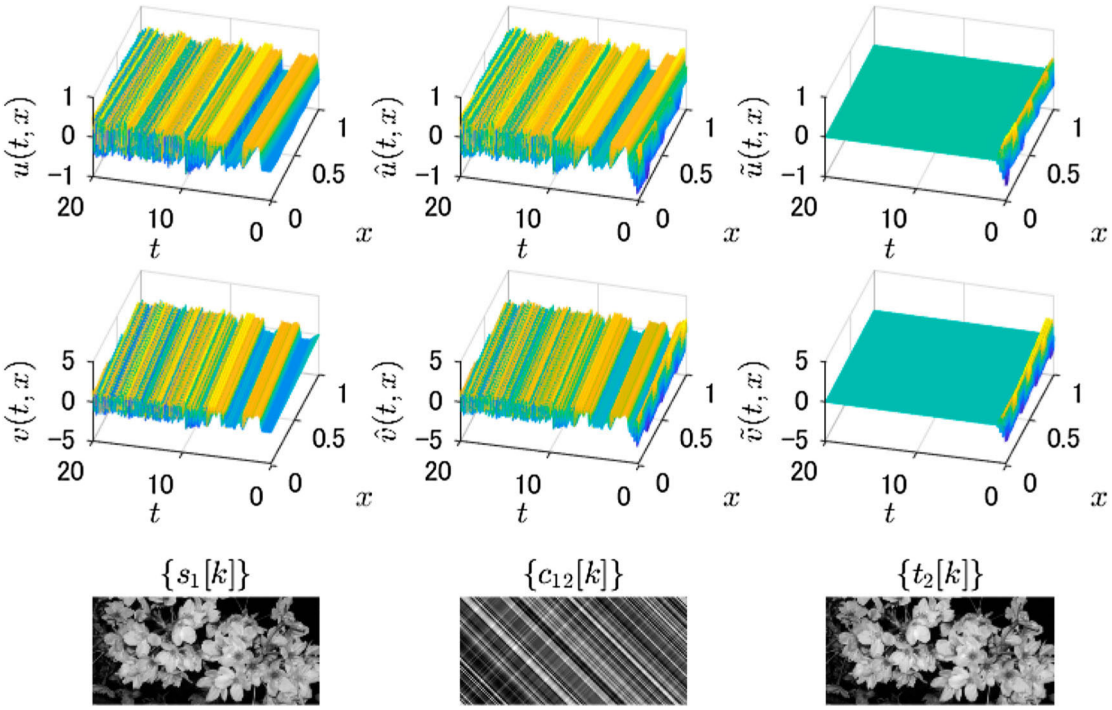

Figure 3. Image encryption. $\{s_1[k]\}$: original image. $\{c_{12}[k]\}$: modulated image. $\{t_2[k]\}$: restored image.

paper, the signals s_1 and t_2 of Figure 1 are scalar. In particular, G of (14) is set as

$$G(a, c, \xi) = r_1|a|H(c) + (r_2 H(c) + r_3)(r_4|a| + \xi), \quad a, c, \xi \in \mathbf{R},$$

where $H(z) := |z(1 - z)|$, $z \in \mathbf{R}$, and r_1, r_2, r_3, r_4 are some positive constants. Also, for arbitrarily fixed $a, c \in \mathbf{R}$, the inverse of G is given by

$$G^{-1}(a, c, \xi) = \frac{\xi - r_1|a|H(c)}{r_2 H(c) + r_3} - r_4|a|, \quad a, c, \xi \in \mathbf{R}.$$

In this paper, we have extended the G such that each argument of G can take a vector value.

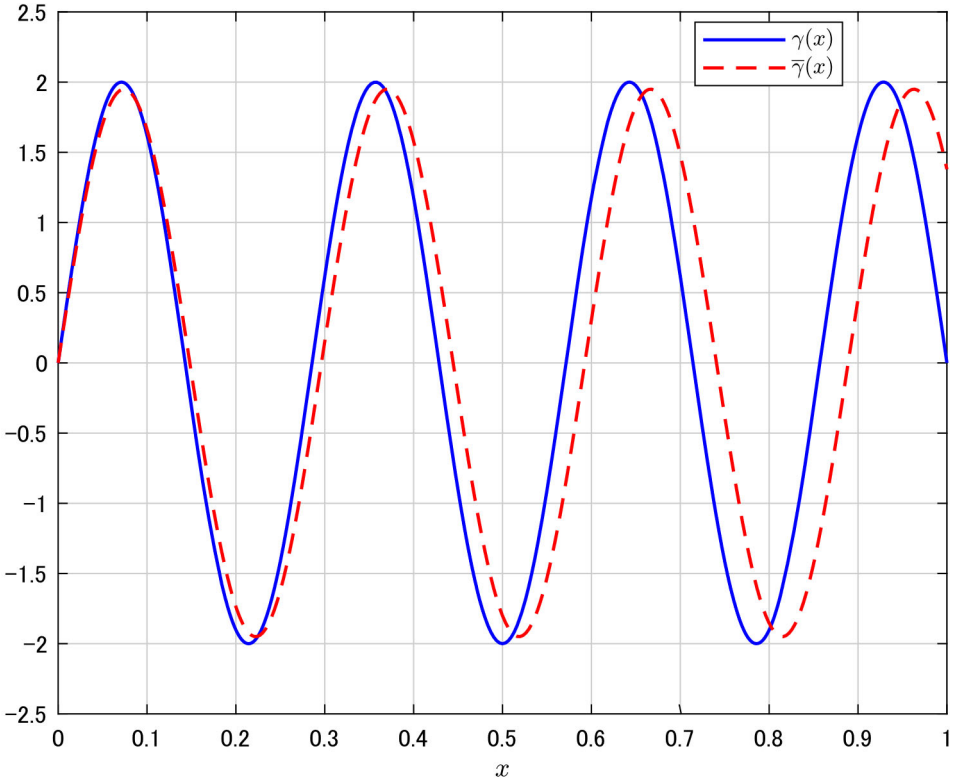

Figure 4. Distributed key function. Solid line: $\gamma(x) = 2\sin(7\pi x)$. Dash line: $\overline{\gamma}(x) = 1.95\sin(6.75\pi x)$.

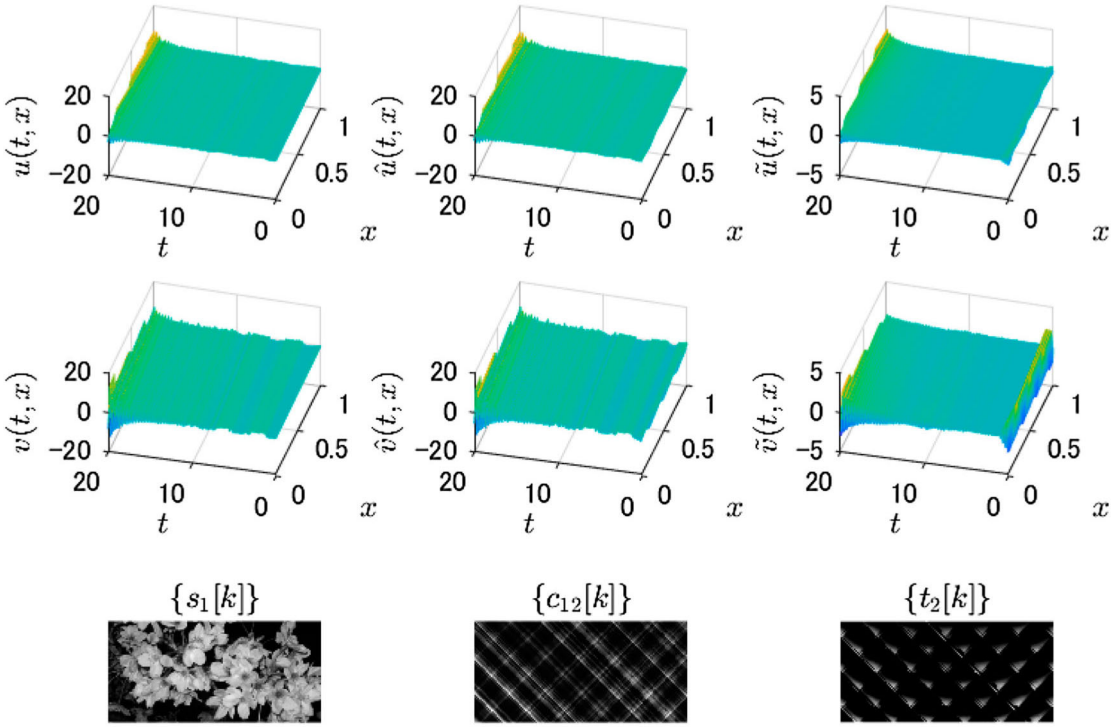

Figure 5. Case where the distributed key function $\gamma(x)$ is fluctuated. $\gamma(x) = 2\sin(7\pi x)$ and $\overline{\gamma}(x) = 1.95\sin(6.75\pi x)$ are used in $\Sigma_{(3)}$ and $\Sigma_{(1)}$, respectively. $\{s_1[k]\}$: original image. $\{c_{12}[k]\}$: modulated image. $\{t_2[k]\}$: restored image.

5. Conclusion

In this paper, we proposed the observer design method for a nonlinear hyperbolic system with a modified van der Pol boundary condition including an integral term, and then, as an application example, we treated image encryption which was regarded as a kind of secure communication. The proposed method of image encryption includes three constant keys α, β, κ and one distributed key function $\gamma(x)$, $x \in [0,1]$. Indeed, since the $\gamma(x)$ is approximated as $\gamma(x_i)$, $i = 0, 1, \ldots, L$, the proposed

method will include very large number of constant keys compared to that of [8]. In this sense, the method proposed here can be said to be safer.

Acknowledgements

The authors would like to thank the reviewers for their helpful comments and suggestions.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research is supported by KAKENHI (Grant-in-Aid for Scientific Research (C), No. 21K03370), Japan Society for the Promotion of Science.

Notes on contributors

Hideki Sano received a B.S. degree in Mathematics and the M.S. degree in Mathematics from Keio University, Japan, in 1989 and 1992, respectively. In 1995, he received the Ph.D. degree in Electrical Engineering from Keio University, Japan. He is currently a Professor in the Department of Applied Mathematics, Graduate School of System Informatics, Kobe University, Japan. His current research interests include the systems and control theory of partial differential equations.

Masashi Wakaiki received the B.S. degree in Engineering and the M.S. and Ph.D. degrees in Informatics from Kyoto University, Kyoto, Japan, in 2010, 2012, and 2014, respectively. He is currently an Associate Professor in the Department of Applied Mathematics, Graduate School of System Informatics, Kobe University. His research interests include networked control systems and security for control.

References

[1] Chen G, Hsu SB, Zhou J. Chaotic vibration of the wave equation with nonlinear feedback boundary control: progress and open questions. In: Chen GR, Yu X, editors. Chaos control: theory and applications. Berlin: Springer-Verlag; 2003. p. 25–50. (Lecture notes in control and information sciences; 292).

[2] Li L, Huang Y, Xiao M. Observer design for wave equations with van der Pol type boundary conditions. SIAM J Control Optim. 2012;50:1200–1219.

[3] Cuomo KM, Oppenheim AV. Circuit implementation of synchronized chaos with applications to communications. Phys Rev Lett. 1993;71:65–68.

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

[5] Ushio T. Chaotically synchronizing control and its application to secure communication. Trans Inf Process Soc Jpn. 1995;36:525–530 (in Japanese).

[6] Ushio T. Control of chaotic synchronization in composite systems with applications to secure communication systems. IEEE Trans Circuits Syst I: Fundam Theory Appl. 1996;43:500–503.

[7] Yoshimura K. Multichannel digital communications by the synchronization of globally coupled chaotic systems. Phys Rev E. 1999;60:1648–1657.

[8] Sano H, Wakaiki M, Yaguchi T. Secure communication systems using distributed parameter chaotic synchronization. SICE Trans. 2021;57(2):78–85 (in Japanese).

[9] Suzuki M, Sakamoto N. Controlling ideal turbulence in time-delayed Chua's circuits and an application to communications. Proceedings of the Joint 48th IEEE Conference on Decision and Control and 28th Chinese Control Conference. IEEE; 2009. p. 2040–2045.

[10] Zhang Y, Xiao D, Shu YL, et al. A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations. Signal Process: Image Commun. 2013;28:292–300.

[11] Auriol J, Di Meglio F. Minimum time control of heterodirectional linear coupled hyperbolic PDEs. Automatica. 2016;71:300–307.

[12] Bastin G, Coron JM. Stability and boundary stabilization of 1-d hyperbolic systems. Switzerland: Birkhäuser-Springer; 2016.

[13] Bribiesca-Argomedo F, Krstic M. Backstepping-forwarding control and observation for hyperbolic PDEs with Fredholm integrals. IEEE Trans Autom Control. 2015;60(8):2145–2160.

[14] Di Meglio F, Vazquez R, Krstic M. Stabilization of a system of $n+1$ coupled first-order hyperbolic linear PDEs with a single boundary input. IEEE Trans Autom Control. 2013;58(12):3097–3111.

[15] Hu L, Di Meglio F, Vazquez R, et al. Control of homodirectional and general heterodirectional linear coupled hyperbolic PDEs. IEEE Trans Autom Control. 2016;61(11):3301–3314.

[16] Krstic M, Smyshlyaev A. Boundary control of PDEs: a course on backstepping designs. Philadelphia: SIAM; 2008.

[17] Sano H, Wakaiki M, Maruyama H. Backstepping observers for two linearized Kermack–McKendrick models. IFAC-PapersOnLine. 2018;51(32):456–461.

[18] Sano H, Wakaiki M. State estimation of Kermack–McKendrick PDE model with latent period and observation delay. IEEE Trans Autom Control. 2021;66(10):4982–4989.

[19] Strecker T, Aamo OM. Output feedback boundary control of 2×2 semilinear hyperbolic systems. Automatica. 2017;83:290–302.

[20] Miller RK. Nonlinear Volterra integral equations. Menlo Park (CA): W.A. Benjamin, Inc.; 1971.

Appendices

Appendix 1. Characterization of the solution of (1)

First, we consider the case of $t = \tau$ $(0 \le \tau < 2)$. The initial data $u(0,x)$ of u, i.e. $u_0(x)$ travels along the characteristic line $x + \tau = \text{const}$ while $\tau \le 1 - x$. That is, $u(\tau, x) = u_0(x + \tau)$ holds for $\tau \le 1 - x$. In due course, the wave u reaches $x = 0$. At that moment, the wave u reflects and becomes the wave v, where, by the boundary condition at $x = 0$, the wave v takes the value operated by ψ. After the reflection, the wave v travels along the characteristic line $\tau - x = \text{const}$ while $x < \tau \le 1 + x$. Accordingly, $v(\tau, x) = \psi(u_0(\tau - x))$ holds for $x < \tau \le 1 + x$. Further, the wave v reaches $x = 1$. At that moment, the wave v reflects and

becomes the wave u, where, by the boundary condition at $x = 1$, the wave u takes the form of the sum of the value operated by ϕ and the integral term $f(u)$. After the reflection, the wave u travels along the characteristic line $x + \tau =$ const while $2 - x < \tau < 2$. Then, $u(\tau, x) = (\phi \circ \psi)(u_0(x + \tau - 2)) + f(u(\tau + x - 1, \cdot))$ holds for $2 - x < \tau < 2$. The same goes for the initial data $v(0, x)$ of v, i.e. $v_0(x)$. Thus, for $x \in [0, 1]$ and $t = \tau$ $(0 \le \tau < 2)$, we have

$$u(\tau,x) = \begin{cases} u_0(x+\tau), & \text{for } \tau \le 1-x, \\ \phi(v_0(2-x-\tau)) & \\ \quad +f(u(-1+\tau+x,\cdot)), & \text{for } 1-x < \tau \\ & \quad \le 2-x, \\ (\phi\circ\psi)(u_0(x+\tau-2)) & \\ \quad +f(u(-1+\tau+x,\cdot)), & \text{for } 2-x \\ & \quad < \tau < 2, \end{cases} \tag{A1}$$

$$v(\tau,x) = \begin{cases} v_0(x-\tau), & \text{for } \tau \le x, \\ \psi(u_0(\tau-x)), & \text{for } x < \tau \\ & \quad \le 1+x, \\ (\psi\circ\phi) & \\ \quad (v_0(x-\tau+2)) & \\ \quad +(\psi\circ f)(u(-1+\tau-x,\cdot)), & \text{for } 1+x \\ & \quad < \tau < 2. \end{cases} \tag{A2}$$

Next, let us set

$$u_1(x) := u(2,x) = (\phi\circ\psi)(u_0(x)) + f(u(1+x,\cdot)),$$
$$v_1(x) := v(2,x) = (\psi\circ\phi)(v_0(x)) + (\psi\circ f)(u(1-x,\cdot)).$$

Here, we consider $u_1(x)$ and $v_1(x)$ as initial data and repeat the same discussion as in the above. Then, for $x \in [0, 1]$ and $t = 2 + \tau$ $(0 \le \tau < 2)$, we have

$$u(2+\tau,x) = \begin{cases} u_1(x+\tau), & \text{for } \tau \le 1-x, \\ \phi(v_1(2-x-\tau)) & \\ \quad +f(u(1+\tau+x,\cdot)), & \text{for } 1-x < \tau \\ & \quad \le 2-x, \\ (\phi\circ\psi)(u_1(x+\tau-2)) & \\ \quad +f(u(1+\tau+x,\cdot)), & \text{for } 2-x \\ & \quad < \tau < 2, \end{cases} \tag{A3}$$

$$v(2+\tau,x) = \begin{cases} v_1(x-\tau), & \text{for } \tau \le x, \\ \psi(u_1(\tau-x)), & \text{for } x < \tau \\ & \quad \le 1+x, \\ (\psi\circ\phi)(v_1(x-\tau+2)) & \\ \quad +(\psi\circ f) & \\ \quad (u(1+\tau-x,\cdot)), & \text{for } 1+x \\ & \quad < \tau < 2. \end{cases} \tag{A4}$$

Further, setting

$$u_2(x) := u(4,x) = (\phi\circ\psi)(u_1(x)) + f(u(3+x,\cdot)),$$
$$v_2(x) := v(4,x) = (\psi\circ\phi)(v_1(x)) + (\psi\circ f)(u(3-x,\cdot)),$$

and repeating the above discussion, we obtain the characterization of the solution of (1) as stated in the Introduction.

Appendix 2. Derivation of (10) and (11)

For system (9), we set the target system as (A5) and the integral transformation as (A6).

$$\begin{cases} \zeta_t(t,x) = -\zeta_x(t,x), \\ \zeta(t,0) = 0, \\ \zeta(0,x) = \zeta_0(x), \end{cases} \tag{A5}$$

$$\zeta(t,x) = \tilde{v}(t,x) - \int_x^1 r(x,y)\tilde{v}(t,y)\,dy. \tag{A6}$$

Clearly, the solution $\zeta(t,\cdot)$ of (A5) vanishes for all $t \ge 1$. Differentiating (A6) and performing integration by parts, $\zeta_t(t,x) + \zeta_x(t,x)$ is calculated as

$$\begin{aligned} &\zeta_t(t,x) + \zeta_x(t,x) \\ &\quad = \left\{ r(x,1) - h(x) + \int_x^1 r(x,y)h(y)\,dy \right\} \tilde{v}(t,1) \\ &\qquad - \int_x^1 \{r_y(x,y) + r_x(x,y)\}\tilde{v}(t,y)\,dy. \end{aligned} \tag{A7}$$

If the two terms enclosed in $\{\cdot\}$ of the right-hand side of (A7) are zero, $\zeta_t(t,x) + \zeta_x(t,x) = 0$ holds for all $\tilde{v}$. Also, putting $x = 0$ in (A6) and using the boundary condition of (9) yields

$$\zeta(t,0) = \int_0^1 (\kappa q(0,y) - r(0,y))\tilde{v}(t,y)\,dy.$$

If $\kappa q(0,y) = r(0,y)$, $\zeta(t,0) = 0$ holds for all $\tilde{v}$. Thus, we obtain (10) and (11).

Appendix 3. Derivation of $(g, h) \in W$

First, putting $x = 0$ in (11) and (12), we have

$$h(0) = r(0,1) + \int_0^1 r(0,y)h(y)\,dy, \tag{A8}$$

$$g(0) = q(0,1) + \int_0^1 q(0,y)h(y)\,dy. \tag{A9}$$

Here, noting that $r(0,y) = \kappa q(0,y)$ by (10), we have

$$h(0) = \kappa q(0,1) + \kappa \int_0^1 q(0,y)h(y)\,dy = \kappa g(0). \tag{A10}$$

Next, putting $x = 1$ in (12), and noting that $q(1,y) = 0$ by (8) and that $p(1,y) = \gamma(y)$ by (7), we have

$$g(1) = \int_0^1 p(1,y)g(y)\,dy = \int_0^1 \gamma(y)g(y)\,dy. \tag{A11}$$

Based on the discussion of Section 2, we know that $g \in H^1(0,1)$, $h \in H^1(0,1)$. Hence, it follows from (A10) and (A11) that $(g,h) \in W$.