2024 European Control Conference (ECC)
June 25-28, 2024. Stockholm, Sweden

Synchronization of chaotic hyperbolic PDE systems for image encryption using backstepping observer design

Jeanne Redaud[1,2] and Hideki Sano[2]

Abstract— **This paper proposes a secure image encryption process using chaotic hyperbolic partial differential equations (PDE) systems synchronization. Using an innovative invertible transform, we design a sensitive observer for an original chaotic system with an increased number of encryption keys. It achieves finite-time stabilization of the error system. Therefore, using the observation data sent by the transmitter, the receiver can synchronize the chaotic observer PDE system. From the encrypted data and observer state, we can then reconstruct the original data. An analytical key sensitivity analysis is illustrated in simulations. Unlike classical approaches, the observer system must be the less robust: the more sensitive it is to a variation of the system's parameters, the more secure the cryptosystem will be. Different modulation strategies based on the synchronized chaotic states are proposed. Their robustness to basic crypto-attacks is assessed on a simple test case.**

I. INTRODUCTION

With the development of new services in the last decades, global IP traffic has skyrocketed, mainly due to increased video traffic. With a parallel increase in cyberattacks, there is an urge for secure communication methods, particularly for image data. Transmitting image flows securely poses several problems. Due to the inherent properties of their structure (high redundancy, correlation between pixels), classical encryption procedures such as the Advanced Encryption Standard (AES) are not suitable [31]. Moreover, the cryptosystem must be computationally efficient to allow secure real-time image flow transmission (video encryption). Methods based on chaotic systems offer an alternative approach. Such systems can generate random-like time series, though these are fully deterministic. The readable data is then converted into an unrecognizable form, using the chaotic time-series to shuffle or modify the pixels [7], [28], [4]. The encrypted data is transmitted while preventing an unauthorized party from getting valuable information. The receiver uses his own chaotic system, synchronized using observation data sent by the transmitter, to recover the chaotic trajectories [13], [15]. He can then apply a decryption algorithm to recover the original image. The encryption keys of finite-dimensional chaotic systems are usually the initial conditions, to which the generated time-series are very sensitive. Since their number is limited, the complexity and security level of resulting cryptosystems was questioned [16].

A natural extension to generate more complex chaotic trajectories is to use infinite dimensional systems [25], [30]. Spatiotemporal chaotic systems can be modeled by coupled-map lattices obtained from local nonlinear dynamics and spatial diffusion [12], [25] or Partial Differential Equations (PDE) [30]. In particular, secure communication methods can be based on first-order hyperbolic PDE systems derived from wave-like equations [14]. Chaos can be obtained by adding nonlinear boundary reflection terms [24], such as van der Pol type boundary conditions [6], [5]. Secure communication systems based on synchronizing different chaotic vibrations of wave-like equations were proposed in [22], [23]. Interestingly, synchronization of chaotic hyperbolic PDE systems can also be obtained using observer designs [10]. In more recent works [21], [20], backstepping based Luenberger-type observers were proposed for such systems. They were designed to finite-time stabilize the error system, resulting into the synchronization of the original hyperbolic PDE system (transmitter) and the observer system (receiver). In this work, we extend previous results by considering additional couplings in the original chaotic PDE system. This additional complexity allows for better chaotic properties (such as higher Lyapunov exponents), and therefore higher speed of the encryption process [18]. Moreover, this also enlarges the key space and therefore considerably augments the security level of the resulting cryptosystem.

Secure communication of images using chaotic systems is still an active area of research [8], [31]. However, there still lacks a performance comparison of existing encryption strategies and the observer sensitivity with parameter uncertainties has not been studied. In this paper, we also aim to provide methodological hints for security assessment of chaotic PDE based cryptosystems. The interest of several chaos-based cryptosystems is questioned using a key analysis and classical indicators. In particular, the sensitivity of the proposed observer to encryption keys and its impact on image decryption is investigated.

Notations: We define $\mathscr{S} = [0,1]^2$ the unit square and the two subparts $\mathscr{T}^+ = \{(x,y) \in \mathscr{S} \mid 0 \leq 1-x \leq y \leq 1\}$ and $\mathscr{T}^- = \{(x,y) \in \mathscr{S} \mid 0 \leq y \leq 1-x \leq 1\}$.

II. SYSTEM UNDER CONSIDERATION

In this section, we present the two chaotic hyperbolic PDE systems further used for secured image encryption. The first system (transmitter) generates chaotic time series used to encrypt the information contained in the image. The

*This research was conducted during the Postdoctoral short-term fellowship (PE23006) and supported by JSPS KAKENHI Grant Number JP21K03370.

[1]Jeanne Redaud is with Université Paris-Saclay, CNRS, CentraleSupélec, Laboratoire des Signaux et Systèmes, 91190, Gif-sur-Yvette, France jeanne.redaud@centralesupelec.fr.

[2] Both authors are with Kobe University, Graduate School of System Informatics, Department of Applied Mathematics, Kobe 657-8501, Japan sano@crystal.kobe-u.ac.jp.

second one (receiver) is a Luenberger-type observer. It is synchronized with the first one using observation data.

A. Chaotic hyperbolic PDE system (transmitter)

1) New chaotic system with additional distributed keys: In this paper, we consider the 2×2 hyperbolic PDE system of states $(u,v)\in C^0([0,T],L^2(0,1)^2)$, satisfying

$$\begin{cases} \frac{\partial u}{\partial t}=\frac{\partial u}{\partial x}+\sigma_u(x)u(t,x),\\ \frac{\partial v}{\partial t}=-\frac{\partial v}{\partial x}+\sigma_v(x)v(t,x),\\ u(t,1)=F_{a,b}(v(t,1))+\int_0^1\alpha(x)v(t,x)\mathrm{d}x,\\ v(t,0)=\kappa u(t,0)+\int_0^1\beta(x)u(t,x)\mathrm{d}x, \end{cases} \tag{1}$$

with $\sigma_u,\sigma_v\in C^0([0,1],\mathbb{R})$, and $\alpha,\beta\in C^1([0,1],\mathbb{R})$. We have the following assumption

Assumption 1: The encryption keys satisfy

1) $0<a<1,\ b>0$,
2) $\beta(1)=\alpha(0)=0$.

The coupling function $F_{a,b}$ is defined implicitly as

$$\forall v\in\mathbb{R},\ u=F_{a,b}(v)\Leftrightarrow b(u-v)^3+(1-a)(u-v)+2v=0.$$

Under the first condition of Assumption 1, this function is well-defined [11]. It is obtained from a van der Pol self-regulating boundary condition for the corresponding wave-like equation [5]. The chaotic properties of this system were studied in [18]. The initial conditions $u_0(x)=u(0,x),\ v_0(x)=v(0,x)\in H^1([0,1],\mathbb{R})$ satisfy

$$\begin{cases} u_0(1)=F_{a,b}(v_0(1))+\int_0^1\alpha(x)v_0(x)\mathrm{d}x,\\ v_0(0)=\kappa u_0(0)+\int_0^1\beta(x)u_0(x)\mathrm{d}x. \end{cases} \tag{2}$$

2) Well-posedness of the proposed system: We have the following theorem

Theorem 1: For all $(u_0,v_0)\in H^1([0,1],\mathbb{R}^2)$ satisfying the compatibility conditions (2), the system (1) admits a weak solution $(u(t,\cdot),v(t,\cdot))\in L^2([0,1],\mathbb{R}^2)$, for all $t\geq 0$.

Proof: Exponential change of variables: To simplify the well-posedness analysis of (1), we can first apply an exponential change of variables to get rid of in-domain coupling terms σ_u,σ_v. We define $\bar{u}(t,x)=e^{-\int_x^1\sigma_u(s)\mathrm{d}s}u(t,x),\ \bar{v}(t,x)=e^{\int_x^1\sigma_v(s)\mathrm{d}s}v(t,x)$, which satisfy

$$\begin{cases} \frac{\partial}{\partial t}\bar{u}(t,x)-\frac{\partial}{\partial x}\bar{u}(t,x)=0,\\ \frac{\partial}{\partial t}\bar{v}(t,x)+\frac{\partial}{\partial x}\bar{v}(t,x)=0,\\ \bar{u}(t,1)=F_{a,b}(\bar{v}(t,1))+\int_0^1\bar{\alpha}(x)\bar{v}(t,x)\mathrm{d}x,\\ \bar{v}(t,0)=\bar{\kappa}\bar{u}(t,0)+\int_0^1\bar{\beta}(x)\bar{u}(t,x)\mathrm{d}x, \end{cases} \tag{3}$$

with $\bar{\alpha}(x)=\alpha(x)e^{-\int_x^1\sigma_v(s)\mathrm{d}s}$, $\bar{\beta}(x)=e^{\int_0^1\sigma_v(s)\mathrm{d}s}\beta(x)e^{\int_x^1\sigma_u(s)\mathrm{d}s}$ and $\bar{\kappa}=e^{\int_0^1\sigma_v(s)+\sigma_u(s)\mathrm{d}s}\kappa$.

Method of characteristics: Using the method of characteristics, we now express $(\bar{u}(t,x),\bar{v}(t,x))$ the solution of (3) as a function of the initial conditions and $\bar{u}(\cdot,1)$, in particular for $t\in[0,2]$. We then show that $\bar{u}(\cdot,1)$ satisfies a Volterra equation of the second kind, which admits a unique square integrable solution [29]. Following the characteristic lines $X(s)=x\pm s,\ T(s)=t-s$, we have the following solutions for $x\in[0,1]$ and $t\in[0,2]$:

$$\bar{u}(t,x)=\begin{cases} \bar{u}_0(t+x), \text{ if } 0\leq t<1-x,\\ \bar{u}(t-(1-x),1), \text{ else} \end{cases} \tag{4}$$

$$\bar{v}(t,x)=\begin{cases} \bar{v}_0(x-t), \text{ if } 0\leq t<x,\\ \int_0^1\bar{\beta}(s)\left(\mathbb{1}_{[x,1+x-s]}(t)\bar{u}_0(t-x+s)\right.\\ \left.+\mathbb{1}_{[1+x-s,2]}(t)\bar{u}(t-x+s-1,1)\right)\mathrm{d}s\\ +\bar{\kappa}\left(\mathbb{1}_{[x,1+x]}(t)\bar{u}_0(t-x)\right.\\ \left.+\mathbb{1}_{[1+x,2]}(t)\bar{u}(t-x-1,1)\right), \text{ else.} \end{cases} \tag{5}$$

Using the above equations and the boundary conditions in $x=1$, we show that $\bar{u}(t,1)$ satisfies

$$\begin{aligned} \bar{u}(t,1)&=F_{a,b}(\bar{v}(t,1))+\int_0^1\bar{\alpha}(x)\bar{v}(x)\mathrm{d}x,\\ &=F_{a,b}\left(\mathbb{1}_{[0,1]}(t)\bar{v}_0(1-t)+\int_0^1\bar{\beta}(s)(\mathbb{1}_{[1,2-s]}(t)\bar{u}_0(t-1+s)\right.\\ &\qquad\left.+\mathbb{1}_{[2-s,2]}(t)\bar{u}(t+s-2,1)\mathrm{d}s+\bar{\kappa}\mathbb{1}_{[1,2]}(t)\bar{u}_0(t-1)\right)\\ &+\int_0^1\bar{\alpha}(s)\left(\mathbb{1}_{[0,s]}(t)\bar{v}_0(s-t)+\int_0^1\bar{\beta}(\nu)(\mathbb{1}_{[s,1+s-\nu]}(t)\times\right.\\ &\qquad\left.\bar{u}_0(t-s+\nu)+\mathbb{1}_{[1+s-\nu,2]}(t)\bar{u}(t-1-s+\nu,1)\mathrm{d}\nu\right)\mathrm{d}s\\ &+\int_0^1\bar{\alpha}(s)\bar{\kappa}\left(\mathbb{1}_{[s,1+s]}(t)\bar{u}_0(t-s)+\mathbb{1}_{[1+s,2]}(t)\bar{u}(t-s-1,1)\right)\mathrm{d}s. \end{aligned}$$

From there, using several changes of variables in the integral terms, we can define the boundary term for all $t\in[0,2]$ by

$$\begin{aligned} \bar{u}(t,1)&=F_{a,b}(\bar{v}_0(1-t))+\int_0^{1-t}\bar{\alpha}(\theta+t)\bar{v}_0(\theta)\mathrm{d}\theta\\ &\quad+\int_t^{t+1}\left(\int_0^{t-\theta+1}\bar{\alpha}(s)\bar{\beta}(\theta+s-t)\mathrm{d}s\right)\bar{u}_0(\theta)\mathrm{d}\theta\\ &\quad+\bar{\kappa}\int_{t-1}^t\bar{\alpha}(t-\theta)\bar{u}_0(\theta)\mathrm{d}\theta,\ \forall\ t\in[0,1], \end{aligned} \tag{6}$$

$$\begin{aligned} \bar{u}(t,1)&=F_{a,b}\left(\int_{t-1}^1\bar{\beta}(\theta+1-t)\bar{u}_0(\theta)\mathrm{d}\theta\right.\\ &\quad\left.+\int_0^{t-1}\bar{\beta}(\theta-t+2)\bar{u}(\theta,1)\mathrm{d}\theta+\bar{\kappa}\bar{u}_0(t-1)\right)\\ &\quad+\int_{t-1}^t\left(\int_0^{t-\theta}\bar{\alpha}(s)\bar{\beta}(\theta+s-t+1)\mathrm{d}s\right)\bar{u}(\theta,1)\mathrm{d}\theta\\ &\quad+\int_0^{t-1}\left(\int_{t-1-\theta}^1\bar{\alpha}(s)\bar{\beta}(\theta+s-t+1)\mathrm{d}s\right)\bar{u}(\theta,1)\mathrm{d}\theta\\ &\quad+\bar{\kappa}\int_0^{t-1}\bar{\alpha}(t-\theta-1)\bar{u}(\theta,1)\mathrm{d}\theta,\ \forall\ t\in(1,2]. \end{aligned} \tag{7}$$

Using (6), we can rewrite the second integral term in $F_{a,b}$ as a function of the initial conditions $(\bar{u}_0,\bar{v}_0)$, and define

$$\begin{aligned} f_0[\bar{u}_0,\bar{v}_0](\theta)&=F_{a,b}(\bar{v}_0(1-\theta))+\int_0^{1-\theta}\bar{\alpha}(\theta+s)\bar{v}_0(s)\mathrm{d}s\\ &\quad+\int_\theta^{\theta+1}\left(\int_0^{\theta-s+1}\bar{\alpha}(\nu)\bar{\beta}(\nu+s-\theta)\mathrm{d}\nu\right)\bar{u}_0(s)\mathrm{d}s\\ &\quad+\bar{\kappa}\int_{\theta-1}^t\bar{\alpha}(\theta-s)\bar{u}_0(s)\mathrm{d}s. \end{aligned}$$

Therefore, $\bar{u}(\cdot,1)$ is defined for $t\in(1,2]$ as the solution of the Volterra equation of the second kind

$$\bar{u}(\cdot,1)-\int_0^t N(\theta,t)\bar{u}(\theta,1)\mathrm{d}\theta=\mathscr{F}(\bar{u}_0,\bar{v}_0), \tag{8}$$

with $N(\cdot,\cdot)$ defined on $[0,1]\times[1,2]$ by

$$N(\theta,t)=\mathbb{1}_{[t-1,1]}(\theta)\left(\int_0^{t-\theta}\bar{\alpha}(s)\bar{\beta}(\theta+s-t+1)\mathrm{d}s\right)$$

$$+\mathbb{1}_{[0,t-1]}(\theta)\left(\bar{\kappa}\bar{\alpha}(t-\theta-1)+\int_{t-1-\theta}^{1}\bar{\alpha}(s)\bar{\beta}(\theta+s-t+1)\mathrm{d}s\right),$$

and the nonlinear function $\mathscr{F}:\ L^2([0,1],\mathbb{R}^2)\to L^2([1,2],\mathbb{R})$ defined by

$$\mathscr{F}(\bar{u}_0,\bar{v}_0)=F_{a,b}\left(\int_{t-1}^{1}\bar{\beta}(\theta+1-t)\bar{u}_0(\theta)\mathrm{d}\theta\right.$$
$$\left.+\int_0^{t-1}\bar{\beta}(\theta-t+2)f_0[\bar{u}_0,\bar{v}_0](\theta)\mathrm{d}\theta+\bar{\kappa}\bar{u}_0(t-1)\right).$$

The well-posedness of the Volterra equation of the second type (8) [1] guarantees the existence of a unique solution verifying $\bar{u}(\cdot,1)\in L^2((-2,0];\mathbb{R})$ for a source term and initial conditions in the proper functional space. From the expression (4)-(5), it follows that there exists a unique weak solution $(\bar{u}(t,x),\bar{v}(t,x))$ to system (3). Using the inverse change of variables, it directly follows that there exists a unique weak solution $(u(t,x),v(t,x))$ to the original system (1). ∎

System (1) is an extension to [21], [20] which only considered boundary couplings of the form $v(t,0)=\kappa u(t,0)$. Adding in-domain couplings σ_u,σ_v and integral couplings allow to enlarge the key space.

B. Chaotic Observer system (receiver)

1) Luenberger-type observer system: Our objective is to construct a sensitive observer system to estimate the states $(u(t,x),v(t,x))$, using the observation data $Y(t)=v(t,1)$. Following [19], we propose a classical Luenberger-type observer system, as a copy of the dynamics (1) with additional output injection terms of gains f,g. The observer states $(\hat{u}(t,x),\hat{v}(t,x))$ satisfy

$$\begin{cases}\frac{\partial\hat{u}}{\partial t}=\frac{\partial\hat{u}}{\partial x}+\sigma_u(x)\hat{u}(t,x)+f(x)(\hat{v}(t,1)-Y(t)),\\ \frac{\partial\hat{v}}{\partial t}=-\frac{\partial\hat{v}}{\partial x}+\sigma_v(x)\hat{v}(t,x)+g(x)(\hat{v}(t,1)-Y(t)),\\ \hat{u}(t,1)=F_{a,b}(Y(t))+\int_0^1\alpha(x)\hat{v}(t,x)\mathrm{d}x,\\ \hat{v}(t,0)=\kappa\hat{u}(t,0)+\int_0^1\beta(x)\hat{u}(t,x)\mathrm{d}x.\end{cases}\tag{9}$$

System (9) differs from the one considered in [20] due to the presence of the integral term at the boundary condition $x=0$. Defining the variables $\tilde{u}:=u-\hat{u}$, $\tilde{v}:=v-\hat{v}$, the error system reads as follows

$$\begin{cases}\frac{\partial\tilde{u}}{\partial t}(t,x)=\frac{\partial\tilde{u}}{\partial x}(t,x)+\sigma_u(x)\tilde{u}(t,x)+f(x)\tilde{v}(t,1),\\ \frac{\partial\tilde{v}}{\partial t}(t,x)=-\frac{\partial\tilde{v}}{\partial x}(t,x)+\sigma_v(x)\tilde{v}(t,x)+g(x)\tilde{v}(t,1),\\ \tilde{u}(t,1)=\int_0^1\alpha(x)\tilde{v}(t,x)dx,\\ \tilde{v}(t,0)=\kappa\tilde{u}(t,0)+\int_0^1\beta(x)\tilde{u}(t,x)dx.\end{cases}\tag{10}$$

Following the backstepping methodology, we can determine the observer gain functions (f,g) to achieve finite-time stabilization of error system (10).

2) Target error system: Using an invertible transform, we aim to map system (10) to the following target error system

$$\begin{cases}\frac{\partial\xi}{\partial t}(t,x)=\frac{\partial\xi}{\partial x}(t,x)+\sigma_u(x)\xi(t,x),\\ \frac{\partial\eta}{\partial t}(t,x)=-\frac{\partial\eta}{\partial x}(t,x)+\sigma_v(x)\eta(t,x)+q(x,0)\xi(t,0),\\ \xi(t,1)=0,\ \eta(t,0)=\kappa\xi(t,0).\end{cases}\tag{11}$$

We can immediately see that this system is a cascaded system from ξ to η. It is finite-time stable since $\xi(t,\cdot)=0$ for all $t>1$, and then $\eta(t,\cdot)=0$ for all $t>2$.

3) Invertible transform: Due to the presence of integral couplings in the error system (10), we cannot use a classical Volterra integral transform to map it to the target system (11). Indeed, such transform offers a limited number of degrees of freedom, and both recirculation terms inside the domain and integral terms at the boundary cannot be simultaneously suppressed. Consider two kernel functions $p(\cdot,\cdot)\in C^0(\mathscr{T}^+,\mathbb{R})$, and $q(\cdot,\cdot)\in C^0(\mathscr{T}^-,\mathbb{R})$, whose expression will be given later. Define the following integral transform

$$\mathfrak{T}:\ L^2(0,1)^2\longrightarrow L^2(0,1)^2$$
$$\begin{pmatrix}u(x)\\v(x)\end{pmatrix}\mapsto\begin{pmatrix}u(x)-\int_{1-x}^1p(x,y)v(y)dy\\ v(x)-\int_0^{1-x}q(x,y)u(y)dy\end{pmatrix}.\tag{12}$$

We have the following

Theorem 2: For any functions $p(\cdot,\cdot)\in C^0(\mathscr{T}^+,\mathbb{R})$, and $q(\cdot,\cdot)\in C^0(\mathscr{T}^-,\mathbb{R})$, transform $\mathfrak{T}$ defined in (12) is boundedly invertible on $L^2(0,1)^2$.

Proof: Denote $K^+(x,y)=\int_{1-y}^{1-x}q(x,s)p(s,y)\mathrm{d}s$ and $K^-(x,y)=\int_{1-x}^{1-y}p(x,s)q(s,y)\mathrm{d}s$. Define $\mathscr{F}^-:u(x)\mapsto u(x)-\int_0^xK^-(x,y)u(y)\mathrm{d}y$ and $\mathscr{F}^+:u(x)\mapsto u(x)-\int_x^1K^+(x,y)u(y)\mathrm{d}y$, two invertible Volterra integral transforms. Assume $\begin{pmatrix}u & v\end{pmatrix}^\top\in\ker(\mathfrak{T})$, then usual computations lead to $\mathscr{F}^-(u)=0$, $\mathscr{F}^+(v)=0$, so $\ker(\mathfrak{T})=0_{L^2(0,1)^2}$. By Fredholm's alternative [2], the operator $\mathfrak{T}$ is invertible. Its boundedness is straightforward. ∎

Using this invertible transform, we can define new states variables as, for all $t\geq0$, $\begin{pmatrix}\xi(t,x)\\\eta(t,x)\end{pmatrix}=\mathfrak{T}(\begin{pmatrix}\tilde{u}(t,x)\\\tilde{v}(t,x)\end{pmatrix})$. We now follow the backstepping methodology to derive the equations satisfied by kernels (p,q) to ensure that (ξ,η) are solutions of (11).

4) Kernel equations: Differentiating (12) with respect to time and space, and injecting therein (10), we show that the kernels (p,q) must satisfy

$$\begin{cases}\frac{\partial p}{\partial x}(x,y)-\frac{\partial p}{\partial y}(x,y)=(\sigma_v(y)-\sigma_u(x))p(x,y),\\ \frac{\partial q}{\partial x}(x,y)-\frac{\partial q}{\partial y}(x,y)=(-\sigma_u(y)+\sigma_v(x))q(x,y),\end{cases}\tag{13}$$

with boundary conditions

$$p(1,y)=\alpha(y),\ q(0,y)=\beta(y).\tag{14}$$

The system (13)-(14) is well-posed and admits a unique solution. Using the method of characteristics, we show that the kernels are defined for all $(x,y)\in\mathscr{T}^+$, by

$$p(x,y)=\alpha(y+x-1)e^{\int_x^1\sigma_u(s)\mathrm{d}s}e^{-\int_{y+x-1}^y\sigma_v(s)\mathrm{d}s},\tag{15}$$

and for all $(x,y)\in\mathscr{T}^-$, by

$$q(x,y)=\beta(y+x)e^{\int_0^x\sigma_v(s)\mathrm{d}s}e^{-\int_y^{y+x}\sigma_v(s)\mathrm{d}s}.\tag{16}$$

5) Observer gains: Under the second condition of Assumption 1, transform (12) maps system (10) to the finite-time stable target system (11) if the observer gains satisfy the following well-posed system of coupled integral equations

$$\begin{cases}f(x)-\int_{1-x}^1p(x,y)g(y)dy=-\alpha(x)e^{\int_x^1\sigma_u(s)-\sigma_v(s)\mathrm{d}s},\\ g(x)-\int_0^{1-x}q(x,y)f(y)dy=0.\end{cases}\tag{17}$$

III. Key sensitivity analysis

In this section, we study the sensitivity of the observer system (9) with respect to the different encryption keys, regardless of the encryption/decryption technique used.

A. Theoretical analysis

1) Sensitivity with respect to encryption keys (σ_u, σ_v): First, assume the receiver side only knows an approximation of the in-domain couplings and define for all $x \in [0,1]$, $\hat{\sigma}_u(x) = \sigma_u(x) + \varepsilon_u(x)$, and $\hat{\sigma}_v(x) = \sigma_v(x) + \varepsilon_v(x)$. Following the backsteppping methodology, we show that defining adequate observer gains and kernels $(\hat{p}, \hat{q})$ for (12), we can map the resulting error system to

$$\begin{cases} \frac{\partial \xi}{\partial t} - \frac{\partial \xi}{\partial x} = \hat{\sigma}_u(x)\xi(t,x) + \mathscr{E}_\xi(u,v,x), \\ \frac{\partial \eta}{\partial t} + \frac{\partial \eta}{\partial x} = \hat{\sigma}_v(x)\eta(t,x) + q(x,0)\xi(t,0) + \mathscr{E}_\eta(u,v,x), \\ \xi(t,1) = 0, \ \eta(t,0) = \kappa\xi(t,0), \end{cases}$$

for some linear operators $\mathscr{E}_\xi, \mathscr{E}_\eta$. Using the method of characteristics, and the inverse of transform (12), we can express for $T \gg 0$ the error states $(\tilde{u}, \tilde{v})$ in function of $u, v, \varepsilon_u, \varepsilon_v$ using bounded linear operators. Their expression is not given here for sake of brevity. Since the chaotic state (u,v) is bounded, the error system evolves chaotically in steady state.

2) Sensitivity with respect to encryption keys (α, β): We now assume that the receiver side only knows an approximation of the integral boundary couplings and define for all $x \in [0,1]$, $\hat{\alpha}(x) = \alpha(x) + \varepsilon_\alpha(x)$, and $\hat{\beta}(x) = \beta(x) + \varepsilon_\beta(x)$. Similarly, the resulting error system can be mapped to

$$\begin{cases} \frac{\partial \xi}{\partial t} - \frac{\partial \xi}{\partial x} = \sigma_u(x)\xi(t,x), \\ \frac{\partial \eta}{\partial t} + \frac{\partial \eta}{\partial x} = \sigma_v(x)\eta(t,x) + q(x,0)\xi(t,0), \\ \xi(t,1) = -\int_0^1 \varepsilon_\alpha(x)v(t,x)\mathrm{d}x, \\ \eta(t,0) = \kappa\xi(t,0) - \int_0^1 \varepsilon_\beta(x)u(t,x)\mathrm{d}x. \end{cases} \tag{18}$$

Solving system (18), we can also express the error states $(\tilde{u}, \tilde{v})$ in function of $u, v, \varepsilon_u, \varepsilon_v$ using bounded linear operators for $T \gg 0$. Therefore, the observer system appears not very sensitive to the encryption keys in general. For small variations around the real value of the encryption key, the error remains bounded.

B. Numerical simulations

We now illustrate the observer sensitivity to changes in encryption keys with numerical simulations on Matlab. The space domain $[0,1]$ is discretized in $L = 250$ intervals. In this section, we use the encryption keys of form $\theta(x) = \overline{\theta}(10x) + 0.1\,\mathtt{randn}$, with $(\overline{\sigma_u}, \overline{\sigma_v}, \overline{\alpha}, \overline{\beta}) = (0.5, 0.1, 0.05, 1)$ and $(a, b, \kappa) = (0.5, 1, 3.2105)$. The initial conditions are randomly generated, and satisfy (2). Beforehand, the kernels $(p.q)$ and the observer gains (f,g) can be computed using the method of successive approximations. The hyperbolic PDE system are solved using an upwind difference scheme based on the characteristic line [23], [21], with $\Delta t = \Delta x$. As seen in [18], the PDE system (1) generates bounded chaotic trajectories. When the encryption keys are shared without error, the error states converge to zero in finite-time.

We now assume that one of the shared keys is altered. This could happen due to noise in the secure transmission or a malicious attack. Considering state $(u,v) \in C^0([0,T]; L^2(0,1)^2)$, we define $\|[\tilde{k}]\|_{L^2}$ as the L^2-norm of the error state $(\tilde{u}, \tilde{v})$ at numerical step $t_k = 1000 \times k\Delta t$, averaged on 3s. We modify a distributed key $\theta \in \mathbb{R}^L$, by adding a Gaussian noise of varying average $\delta\theta$ and standard deviation of 0.001. We quantify the resulting error using $\varepsilon_\theta = \|\hat{\theta} - \theta\|_1 / \|\theta\|_1$ where $\|\theta\|_1 = \sum_{i=1}^L |\theta_i|$. When the observer couplings are identical (reference), we have $(\|[\tilde{1}]\|_{L^2}, \|[\tilde{5}]\|_{L^2}, \|[\tilde{10}]\|_{L^2}) = (1.9 \cdot 10^{-3}, 2.04 \cdot 10^{-10}, 0)$.

First, we consider that the in-domain couplings (σ_u, σ_v) are altered on the receiver side. The kernel equations (13) are modified, and so are the observer gains (f,g). We see

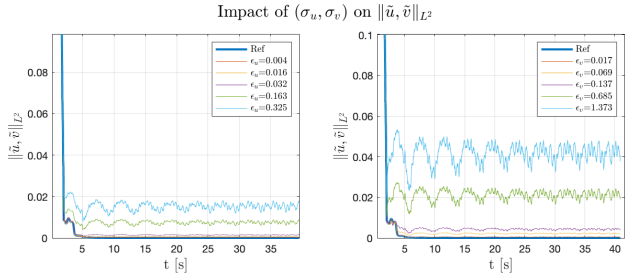

Fig. 1. Impact on altered σ_u (left) and σ_v (right) on the L^2-norm of the error state. Noise average is in $\{0.001, 0.005, 0.01, 0.05, 0.1\}$.

in Figure 1 that the error system is not stabilized but keeps oscillating in steady state. The evolution of the error $\|[\tilde{k}]\|_{L^2}$ at different time steps for varying $\delta\sigma_i$ (and consequently varying ε_{σ_i}) are represented in Figure 2. It evolves linearly with the relative average error on σ_u (left) and σ_v (right). Even after 5000 steps (orange curve), we could expect the error to be of order 10^{-4} to 10^{-2}, even when the error on the couplings is limited. We obtain similar results when

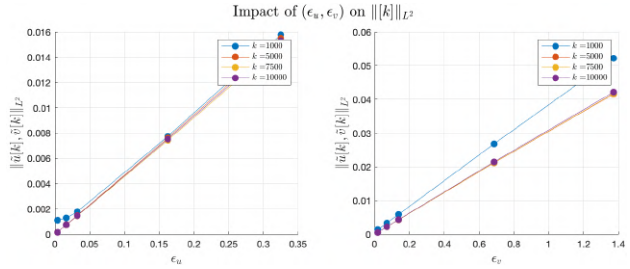

Fig. 2. Impact on altered σ_u (left) and σ_v (right) on the average error at different timesteps.

modifying parameters (α, β) (Figures 3-4). As illustrated in Figure 4, the indicators evolve linearly with ε_α, ε_β.

Following this sensitivity analysis, we quantified the limited impact that small discrepancies in the encryption keys may have on the chaotic states $(\hat{u}, \hat{v})$. To ensure secure communication, the cryptosystem is expected to be sensitive to variations of order 10^{-4} into the synchronized chaotic states.

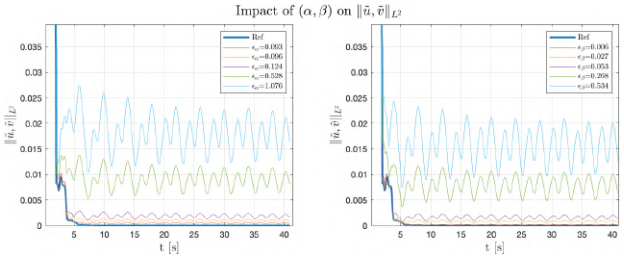

Fig. 3. Impact on altered α (left), and β (right) on the L^2-norm of the error state. Noise average is in $\{0.001, 0.005, 0.01, 0.05, 0.1\}$ ($\times 0.1$ for α).

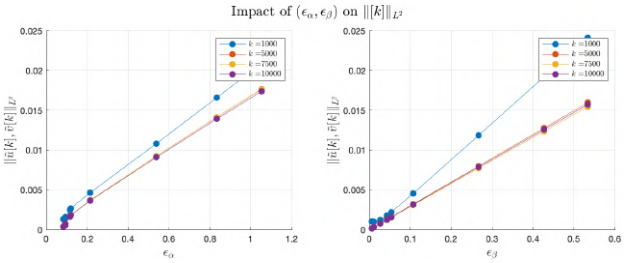

Fig. 4. Impact on altered $\bar{\alpha}$ (left), and $\bar{\beta}$ (right) on the average error at different timesteps.

IV. APPLICATION TO IMAGE ENCRYPTION

In this section, we present the secure communication process for transmitting images. It is of high interest to consider the *robustness* of the cryptosystem with respect to the encryption keys [27]. The cryptosystem should resist known-plaintexts attacks. To satisfy Kerchhoff principle [9], even when the structure of the observer system, it should not be possible to recover the real keys (and therefore the original image) by trial and error.

For the sake of simplicity, we only consider grayscale images represented by 2D matrices in space $\mathscr{D} = [\![0,255]\!]^{L\times M}$. The images are rescaled in $\bar{\mathscr{D}} = [0,0.01]^{L\times M}$. Each line corresponds to a discrete vector, such that for $1 \leq k \leq M$, we define $s_1[k] \in [0,0.01]^L$. After a run-up time $r_N \gg 1$ steps, at each timestep k, the vector $s_1[k]$ (containing the information of the original image) is encrypted on the transmitter side, using the chaotic trajectories generated by (1).

The encrypted vector $w[k]$ is embedded with the observation signal $Y[k] = v(t_k,1)$ into a transmitted signal $c_{12}[k]$ and sent to the receiver. On the receiver side, the system (9) is solved simultaneously, using the observation signal. We assume that the static discrete and distributed encryption keys $\sigma_u, \sigma_v, \alpha, \beta \in \mathbb{R}^L$ have been shared beforehand in a secure manner, using an asymmetric public-private key cryptosystem such as RSA for instance. The encrypted line can then be decrypted by applying a demodulation process, using the synchronized chaotic states $\hat{u}[k], \hat{v}[k]$. More precisely, define G a mapping from $\mathbb{R}^L \times \mathbb{R}^L \times \mathbb{R}^L \times \mathbb{R}^L$ to $\mathbb{R}^L$. We assume that for fixed $(x_1,x_2,x_3) \in \mathbb{R}^{3L}$, $G(x_1,x_2,x_3,\cdot) : \mathbb{R}^L \to \mathbb{R}^L$, is invertible, and its inverse $G^{-1}(x_1,x_2,x_3,\cdot)$ is contractive. The modulated message $w[k]$ is constructed as follows

$$M : \begin{cases} w[k+1] = G(u[k],v[k],w[k],s_1[k+1]), \\ c_{12}[k] = (w[k],Y[k]) \in \mathbb{R}^{L+1}. \end{cases} \quad (19)$$

The decrypted information can be recovered as follows,

$$\mathrm{D}: \; t_2[k+1] = G^{-1}(\hat{u}[k-1],\hat{v}[k-1],w[k-1],w[k]), \quad (20)$$

if the value $t_2[k+1]$ converges to $s_1[k]$ when $k \to +\infty$. We finally compare on a sample image of 187×250 pixels the sensitivity of the cryptosystem with three different modulation processes: one based on a nonlinear mapping [20], [21], one based on chaos masking [13] and one based on chaos shuffling [17]. When the receiver knows all the keys, the three modulation processes allow to reconstruct the original image. Following [23], we use the Error Function Attack (EFA) [27], which corresponds to an average pixel error, to quantify the sensitivity of the cryptosystem to the different keys. With the three methods, when the encryption keys are ideally shared (reference), we obtained $(EFA_1, EFA_2, EFA_3) = (2.7 \cdot 10^{-15}, 2.3 \cdot 10^{-15}, 2.3 \cdot 10^{-15})$. Now, to test the robustness of the cryptosystem, we assume that a hacker tries to guess one of the encryption keys, by using a constant approximation. With the best constant approximation, we now obtain the following errors $(EFA_1, EFA_2, EFA_3) = (25.2, 69.8, 78.0)$.

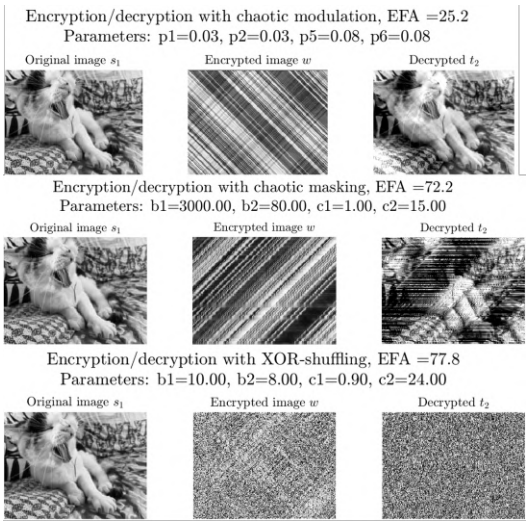

Fig. 5. Comparison of encrypted/decrypted image for the three chaos-based methods when $\hat{\alpha} = \|\alpha\|_1$.

In Figure 5, we represented the encrypted/decrypted images for the same original image. Unfortunately, the modulation protocol proposed in [20], [23] was shown to be not sensitive to encryption keys [17]. We obtain a higher sensitivity for chaos masking, using high ponderations on the state values to amplify the impact of the desynchronization in the modulation process. However, as shown in this example, modulation protocols combining chaos-based pixel position shuffling and diffusion are the most promising. It is illustrated by the comparison of the EFA key basin in Figure 6. Here, we consider α generated using a Gaussian distribution of standard deviation 0.01 and average 0.05. For method 1 (left), the EFA curve has a convex shape and presents small values, while for method 3, no key basin is observed. Even small ε_α prevents the reconstruction of the original image.

The cryptosystem is therefore very robust.

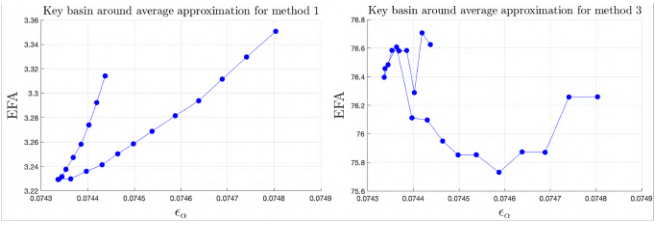

Fig. 6. Comparaison of key basin for constant $\hat{\alpha}$ approximation for method 1 [26], [20] (left) and method 3 [17] (right).

V. CONCLUSIONS

In this paper, we proposed a novel backstepping-based observer design for a chaotic hyperbolic PDE system with additional integral boundary couplings. It is based on an original integral transform. This observer system can be synchronized with the original system using observation data, in the case where all coupling functions are shared. However, if not, an error term remains, that prevents the observer state from converging toward the real state. When used in a chaos-based encryption protocol, such a chaotic hyperbolic PDE system has the advantage of generating highly chaotic trajectories in a short time, and having a large key space. Using sensitive modulation/demodulation protocols, combining chaos-based pixel position shuffling and diffusion, for instance, a robust secure communication system can be obtained. To add a security layer to the encryption process, the discrete and distributed encryption keys could be dynamically generated using the synchronization of a finite-dimensional chaotic system [3], or similarly to [20]. This will be subject to further investigation.

REFERENCES

[1] G. Bastin and J.-M. Coron. *Stability and boundary stabilization of 1-D hyperbolic systems*. Springer, 2016.

[2] H. Brezis. *Functional analysis, Sobolev spaces and partial differential equations*. Springer Science & Business Media, 2010.

[3] T.L. Carroll and L.M. Pecora. Synchronizing chaotic circuits. *IEEE Transactions on Circuits and Systems*, 38(4):453–456, 1991.

[4] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu. A novel image encryption scheme based on dna sequence operations and chaotic systems. *Neural computing & applications*, 31(1):219–237, 2019.

[5] G. Chen, S.-B. Hsu, and J. Zhou. *Chaotic Vibration of the Wave Equation with Nonlinear Feedback Boundary Control: Progress and Open Questions*, pages 25–50. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[6] G. Chen, S.-B. Hsu, J. Zhou, G. Chen, and G.B Crosta. Chaotic vibrations of the one-dimensional wave equation due to a self-excitation boundary condition. part i: Controlled hysteresis. *Transactions of the American Mathematical Society*, 350:4265–4311, 1998.

[7] W.-B. Chen and X. Zhang. Image encryption algorithm based on henon chaotic system. In *2009 International Conference on Image Analysis and Signal Processing*, pages 94–97, 2009.

[8] P. Fang, H. Liu, C. Wu, and M. Liu. A survey of image encryption algorithms based on chaotic system. *The Visual computer*, 39(5):1975–2003, 2023.

[9] A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:5–38, 161–191, 1883.

[10] M. Krstic. *Boundary control of PDEs. A course on backstepping designs.*, volume 16 of *Advances in design and control*. Siam, 2008.

[11] L. Li, Y. Huang, and M. Xiao. Observer design for wave equations with van der pol type boundary conditions. *SIAM Journal on Control and Optimization*, 50(3):1200–1219, 2012.

[12] Ping Li, Zhong Li, Wolfgang A. Halang, and Guanrong Chen. A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map. *Physics Letters A*, 349(6):467–473, 2006.

[13] J.L Mata-Machuca, R. Martínez-Guerra, R. Aguilar-López, and Aguilar-Ibañez. C. A chaotic system in synchronization and secure communications. *Communications in Nonlinear Science and Numerical Simulation*, 17(4):1706–1713, 2012.

[14] T. Matsumoto. A chaotic attractor from chua's circuit. *IEEE Transactions on Circuits and Systems*, 31(12):1055–1058, 1984.

[15] L. M. Pecora and T. L. Carroll. Synchronization of chaotic systems. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 25(9):097611, 2015.

[16] M. Preishuber, T. Hütter, S. Katzenbeisser, and A. Uhl. Depreciating motivation and empirical security analysis of chaos-based image and video encryption. *IEEE Transactions on Information Forensics and Security*, 13(9):2137–2150, 2018.

[17] J. Redaud and H. Sano. Enhanced image encryption algorithm based on chaotic hyperbolic pde systems synchronization. *Transactions on Image Processing*, page (submitted), 06 2024.

[18] J. Redaud and H. Sano. Numerical analysis of a chaotic coupled hyperbolic pde system for secure image encryption. In *7 th IFAC Conference on Analysis and Control of Nonlinear Dynamics and Chaos (ACNDC24)*, page (submitted), 06 2024.

[19] H. Sano. Observers for 2×2 hyperbolic systems with coupled nonlocal boundary condition. pages 1250–1255, 05 2022.

[20] H. Sano. Common encryption key generation and secure communication using pde chaotic synchronization. In *IFAC world Congress*, 07 2023.

[21] H. Sano and M. Wakaiki. Synchronizing chaotic pde system using backstepping and its application to image encryption. *SICE journal of control, measurement, and system integration*, 15(2):182–190, 2022.

[22] H. Sano, M. Wakaiki, and T. Yaguchi. Secure communication systems using distributed parameter chaotic synchronization. *Transactions of the Society of Instrument and Control Engineers*, 57(2):78–85, 2021.

[23] H. Sano, M. Wakaiki, and T. Yaguchi. Secure communication systems based on synchronization of chaotic vibration of wave equations. *Journal of Signal Processing*, 26(6):147–158, 2022.

[24] Y. Shu. Chaotifing a linear hyperbolic system of partial differential equations by means of nonlinear boundary reflection. *Nonlinear Analysis: Theory, Methods & Applications*, 69(5):1768–1774, 2008.

[25] C-Y. Song, Y.-L. Qiao, and X.-Z. Zhang. An image encryption scheme based on new spatiotemporal chaos. *Optik - International Journal for Light and Electron Optics*, 124(18):3329–3334, 2013.

[26] T. Ushio. Control of chaotic synchronization in composite systems with applications to secure communication systems. *IEEE transactions on circuits and systems. 1, Fundamental theory and applications*, 43(6):500–503, 1996.

[27] X. Wang, M. Zhan, C.-H. Lai, and H. Gang. Error function attack of chaos synchronization based encryption schemes. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 14(1):128–137, 2003.

[28] H. Wen, C. Zhang, P. Chen, R. Chen, J.n Xu, Y. Liao, Z. Liang, D. Shen, L. Zhou, and J. Ke. A quantum chaotic image cryptosystem and its application in iot secure communication. *IEEE access*, 9:20481–20492, 2021.

[29] K. Yosida. *Lectures on differential and integral equations*, volume 10. Interscience Publishers, 1960.

[30] Y. Zhang, D. Xiao, Y. Shu, and J. Li. A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations. *Signal processing. Image communication*, 28(3):292–300, 2013.

[31] U. Zia, M. Mccartney, B. Scotney, J. Martínez, M. AbuTair, J. Memon, and A. Sajjad. Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*, 21, 04 2022.