Hindawi
Mathematical Problems in Engineering
Volume 2018, Article ID 6382532, 15 pages
https://doi.org/10.1155/2018/6382532

Research Article

The Secure Transmission of Videos Using the Karhunen-Loéve (K-L) Decomposition and the Synchronization of the Unified Chaotic System with the Hyperchaotic Chen System

N. Smaoui[1], **M. Zribi**[2] **and T. Elmokadem**[2]

[1]*Department of Mathematics, Kuwait University, P.O. Box 5969, Safat 13060, Kuwait*
[2]*Department of Electrical Engineering, Kuwait University, P.O. Box 5969, Safat 13060, Kuwait*

Correspondence should be addressed to N. Smaoui; nsmaoui64@yahoo.com

Received 25 August 2018; Accepted 18 October 2018; Published 31 October 2018

Academic Editor: Cornelio Posadas-Castillo

A unique secure communication scheme that can be used for the transmission of gray-scale and color videos is presented in this paper. The proposed scheme is developed by using the Karhunen-Loéve (K-L) decomposition and the synchronization of the unified chaotic system with the hyperchaotic Chen system. First, the gray-scale or color video is represented by a set of N frames. In order to reduce the data, the K-L decomposition is used to come up with data coefficients and eigenfunctions that optimally obtain the crux of the N frames. Using only the most energetic eigenfunctions to approximate the original frames results in computational savings. The data coefficients corresponding to the most energetic eigenfunctions are encrypted and transmitted using a master system composed of a combination of the unified chaotic system and the hyperchaotic Chen system. At the receiver end, these coefficients are recovered and a controller of the sliding mode type is utilized forcing the master and slave systems to synchronize. Simulation results illustrate how the proposed control law is able to synchronize the master and the slave systems. In addition, a demonstration of the recovery of the original frames using the decrypted data coefficients along with the eigenfunctions of the frame is provided. The presented simulations indicate that the proposed scheme results in an excellent performance.

1. Introduction

Historically, the field of chaos synchronization has attracted many researchers from an array of disciplines [1–31] due to a number of applications which utilize chaos. Secure communication systems are among the potential applications of chaos synchronization. The concept relies on the idea of hiding the transmitted signal in the states of the transmitter's chaotic system. Retrieving the transmitted signal requires control or synchronization of the chaotic system at the transmitter end with the chaotic system at the receiver end.

Chaotic systems are extremely sensitive to initial conditions; this fact makes their dynamical behaviors unpredictable. Ott et al. [1] were the first to introduce the idea of control of chaos by forcing the behavior of chaotic dynamical system to follow a desired behavior. Pecora and Carroll [2] demonstrated that chaotic systems can be synchronized using a drive-response approach. Since then, chaotic synchronization methods have become very attractive in many fields.

In 1993, the chaotic modulation method was applied by Wu and Chua [3] in secure communication, and in 1996, chaotic parameter modulation method was introduced by Yang and Chua [4]. In 2005, Lu and Cao [7] designed adaptive controllers to synchronize the states of the chaotic Lorenz system with the states of the hyperchaotic Chen system. Moreover, adaptive control laws were then designed by Park [8] to synchronize two hyperchaotic Chen systems using Lyapunov stability theory. Recently, different control designs have been investigated to synchronize hyperchaotic and chaotic systems have been examined; for example, see [9–33].

In the past few years, many researchers have proposed various images/videos encryption techniques to encrypt and securely transmit images/videos [34–48]. In 2015, Lin Z. et al. [41] proposed a systematic methodology for real-time

video encryption and decryption system using a chaotic map-based; the system was implemented using an advanced RISC Machine (ARM) with embedded hardware. Ganesan K. et al. [42] proposed multicore CPUs and GPUs to facilitate a secure video transmission. In 2017, Chen S. et al. [40] proposed a systematic methodology based on chaos for video encryption and decryption in real-time.

This paper proposes an unprecedented secure communication scheme developed by using the K-L decomposition and the synchronization of hyperchaotic Chen with the unified chaotic systems for transmitting gray-scale and color videos. A promising advantage of using the unified chaotic system is its ability to have different behaviors and dynamical properties for different values of system parameter [10]. First, we represent each of the gray-scale and color videos by a set of N frames. Then, the K-L decomposition is utilized to generate data coefficients and eigenfunctions that optimally capture the original N frames. The data coefficients corresponding to the most energetic eigenfunctions are encrypted and transmitted using a master system composed of a combination of the unified chaotic system and the hyperchaotic Chen system. Even though the idea of using synchronization of hyperchaotic systems for secure communication is available in the literature, the novelty of this work is in the proposed scheme of decomposing the transmitted data before rather than masking the data directly as will be shown later. A sliding mode controller is then used at the receiver end to synchronize the two systems consisting of hyperchaotic Chen and unified chaotic systems to recover these data coefficients and thus reconstruct the transmitted videos. The sliding mode technique is chosen due to its popularity, robustness, finite-time convergence, and simplicity in implementation.

The rest of the paper is structured as follows: The Karhunen-Loéve decomposition is described in Section 2. Section 3 presents the unified chaotic system and the hyperchaotic Chen system. The design of the proposed controller is detailed in Section 4. Section 5 illustrates the proposed secure communication scheme. Simulation results validating the developed scheme are presented and discussed in Section 6. Finally, some concluding remarks are provided in Section 7.

2. The Karhunen-Loéve Decomposition

The K-L decomposition known as principal component analysis [49], factor analysis [50], proper orthogonal decomposition [51], singular value decomposition [52], quasiharmonic modes [53], and Hoteling transform [54] has wide applications in problems related to feature identification and data compression [51, 52, 55–63]. Since K-L decomposition was extensively discussed in many research work, we will only describe its main idea.

First, the data is considered to be a sequence of N real-valued vectors $\{X_i\}_{i=1}^{N}$, where the dimension of X_i is M such that $X_i = [X_1^i, X_2^i, \cdots, X_M^i]^T$. These vectors can represent a set of images.

Using the snapshot method [64], one can compute the symmetric and positive definite covariance matrix B as follows:

$$B = \left[B_{ij}\right] = \frac{1}{M}\left[\left\langle X_i, X_j\right\rangle\right], \quad i, j = 1, \ldots, N. \tag{1}$$

In (1), $\langle \cdot, \cdot \rangle$ denotes the usual Euclidian inner product.

The eigenfunctions of the data are orthogonal and defined such that

$$\Psi_k = \sum_{i=1}^{N} V_i^{[k]} X_i, \quad k = 1, \ldots, N, \tag{2}$$

where $V_i^{[k]}$ is the i^{th} component of the k^{th} eigenvector. Let X be such that

$$X = \sum_{i=1}^{N} C_i \Psi_i. \tag{3}$$

In (3), Ψ_i is the i^{th} eigenfunction and C_i $(i = 1, \ldots, N)$ are the data coefficients computed by projecting the data vector onto an eigenfunction such that

$$C_i = \left(\frac{X \cdot \Psi_i}{\Psi_i \cdot \Psi_i}\right), \quad i = 1, \ldots, N. \tag{4}$$

The energy of the data, E, is defined as follows:

$$E = \sum_{i=1}^{N} \lambda_i, \tag{5}$$

where λ_i is the eigenvalue of the ith eigenfunction. Because the energy percentage of each eigenfunction depends on the eigenfunction's associated eigenvalue, λ_k, it can be calculated as follows:

$$E_k = \frac{\lambda_k}{E}. \tag{6}$$

In case that all the eigenfunctions are used, then the original data can be fully restored. Moreover, using the most energetic eigenfunctions, an approximation of the original data can be reconstructed as follows:

$$\widetilde{X} = \sum_{i=1}^{K} C_i \Psi_i, \quad \text{where } K < N. \tag{7}$$

3. System Description

This section presents the hyperchaotic Chen system and the unified chaotic system needed for the development of the secure communication scheme; the hyperchaotic Chen system as well as the unified chaotic system is used to generate the master and slave systems.

The master system is obtained by combining the hyperchaotic Chen system with the unified chaotic system. The hyperchaotic Chen system is a fourth-order system of ODEs defined such as

$$\begin{aligned} \dot{x} &= a(y - x) + w \\ \dot{y} &= dx - xz + cy \\ \dot{z} &= xy - bz \\ \dot{w} &= yz + rw \end{aligned} \tag{8}$$

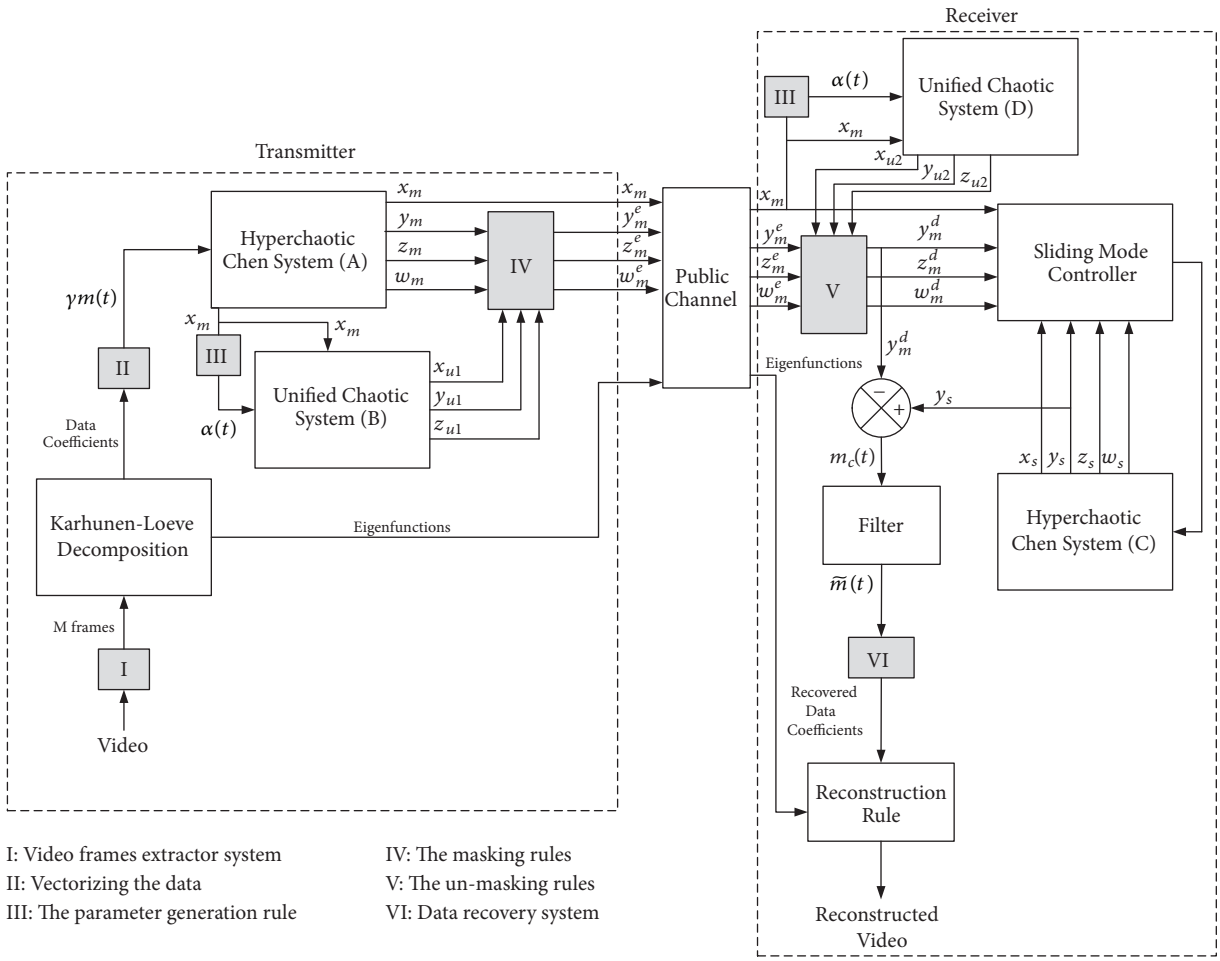

Figure 1: A depiction of the proposed communication scheme.

where x, y, z, and w represent the system states and the scalars a, b, c, d, and r are the parameters of the system. This system exhibits a hyperchaotic behavior when $a = 35$, $b = 3$, $c = 12$, $d = 7$, and $0 \leq r \leq 0.085$ [10].

The unified chaotic system is defined such that

$$\begin{aligned} \dot{x}_u &= (25\alpha + 10)\left(y_u - x_u\right) \\ \dot{y}_u &= (28 - 35\alpha)\, x_u - x_u z_u + (29\alpha - 1)\, y_u \\ \dot{z}_u &= x_u y_u - \frac{\alpha + 8}{3} z_u, \end{aligned} \tag{9}$$

where x_u, y_u, and z_u are the system states and α is a real parameter satisfying $\alpha \in [0, 1]$. Depending on the value of α, system (9) can display different behaviors and dynamical properties. For instance, system (9) exhibits the behavior of the Lorenz chaotic system when $\alpha = 0$ [55]. When $0 < \alpha < 0.8$, system (9) becomes the generalized Lorenz chaotic system. System (9) will be the *Lü* chaotic system if $\alpha = 0.8$ [6]. The unified chaotic system becomes the Chen chaotic system when $\alpha = 1$ [5]; and it becomes the generalized chaotic system when $0.8 < \alpha < 1$.

Therefore, the master system is defined as follows:

$$\begin{aligned} \dot{x}_m &= a\left(y_m - x_m\right) + w_m \\ \dot{y}_m &= d x_m - x_m z_m + c y_m - D \\ \dot{z}_m &= x_m y_m - b z_m \\ \dot{w}_m &= y_m z_m + r w_m \\ \dot{x}_{u1} &= (25\alpha + 10)\left(y_{u1} - x_{u1}\right) \\ \dot{y}_{u1} &= (28 - 35\alpha)\, x_m - x_m z_{u1} + (29\alpha - 1)\, y_{u1} \\ \dot{z}_{u1} &= x_m y_{u1} - \frac{\alpha + 8}{3} z_{u1} \end{aligned} \tag{10}$$

where x_m, y_m, z_m, and w_m represent the states of the Chen hyperchaotic system (A) with a, b, c, d, and r being its parameters. The states of the unified chaotic system (B) are x_{u1}, y_{u1}, and z_{u1}, and α is the system parameter. Also, $D = \gamma m(t)$ represents the message $m(t)$ to be transmitted (data coefficients) with a scaling factor γ. The overall system is depicted in Figure 1.

At the receiver side, the slave system is taken to be a combination of the hyperchaotic Chen system (C) and the unified chaotic system (D) (see Figure 1). It should be noted that the parameters of the master and slave systems should be the same.

Hence, the description of the slave system can be written as follows:

$$\begin{aligned}
\dot{x}_s &= a\left(y_s - x_s\right) + w_s + u_1 \\
\dot{y}_s &= dx_s - x_s z_s + cy_s + u_2 \\
\dot{z}_s &= x_s y_s - bz_s + u_3 \\
\dot{w}_s &= y_s z_s + rw_s + u_4 \\
\dot{x}_{u2} &= (25\alpha + 10)\left(y_{u2} - x_{u2}\right) \\
\dot{y}_{u2} &= (28 - 35\alpha)\, x_m - x_m z_{u2} + (29\alpha - 1)\, y_{u2} \\
\dot{z}_{u2} &= x_m y_{u2} - \frac{\alpha + 8}{3} z_{u2}
\end{aligned} \tag{11}$$

where x_s, y_s, z_s, and w_s are the states of the Chen hyperchaotic system (C), x_{u2}, y_{u2}, and z_{u2} are the states of the unified chaotic system (D), and the parameters a, b, c, d, and r are the same as for system (10). Also, the controllers of the slave system are u_1, u_2, u_3, and u_4. These controllers will be designed to synchronize the master and slave systems at the transmitter and receiver sides, respectively.

It can be seen from (10) and (11) that the signal $x_m(t)$ is used to drive the two unified chaotic systems at both sides. Also, the parameter α used in both systems is generated from $x_m(t)$ using a generation rule that must be the same at the transmitter and receiver sides.

4. Controller Design

A sliding mode control law is proposed in this section to synchronize the master and slave systems described in (10) and (11), respectively. This design is validated and proven to synchronize the two systems. The proof is divided into two parts. The first part of the proof shows that the signal $x_m(t)$ will synchronize the unified chaotic system (D) at the receiver end with the one at the transmitter side. The second part of the proof demonstrates that the proposed control law is able to synchronize the system at the receiver side with the one at the transmitter side.

The unified chaotic systems at both the transmitter and the receiver sides are described, respectively, as follows:

$$\begin{aligned}
\dot{x}_{u1} &= (25\alpha + 10)\left(y_{u1} - x_{u1}\right) \\
\dot{y}_{u1} &= (28 - 35\alpha)\, x_m - x_m z_{u1} + (29\alpha - 1)\, y_{u1} \\
\dot{z}_{u1} &= x_m y_{u1} - \frac{\alpha + 8}{3} z_{u1}
\end{aligned} \tag{12}$$

and

$$\begin{aligned}
\dot{x}_{u2} &= (25\alpha + 10)\left(y_{u2} - x_{u2}\right) \\
\dot{y}_{u2} &= (28 - 35\alpha)\, x_m - x_m z_{u2} + (29\alpha - 1)\, y_{u2} \\
\dot{z}_{u2} &= x_m y_{u2} - \frac{\alpha + 8}{3} z_{u2}.
\end{aligned} \tag{13}$$

Notice that the signal $x_m(t)$ is driving the two systems. The errors between the two unified chaotic systems are defined such that

$$\begin{aligned}
e_{xu} &= x_{u2} - x_{u1} \\
e_{yu} &= y_{u2} - y_{u1} \\
e_{zu} &= z_{u2} - z_{u1}
\end{aligned} \tag{14}$$

By differentiating these errors and using (12) and (13), we obtain the following:

$$\begin{aligned}
\dot{e}_{xu} &= (25\alpha + 10)\left(e_{yu} - e_{xu}\right) \\
\dot{e}_{yu} &= -x_m e_{zu} + (29\alpha - 1)\, e_{yu} \\
\dot{e}_{zu} &= x_m e_{yu} - \frac{\alpha + 8}{3} e_{zu}.
\end{aligned} \tag{15}$$

Theorem 1. *If the parameter α is designed to be in the interval $[0,\ 1/29)$, the signal $x_m(t)$ will synchronize the unified chaotic system (13) at the receiver with the unified chaotic system (12) at the transmitter (i.e., $\lim_{t\to\infty} e_{xu} = \lim_{t\to\infty} e_{yu} = \lim_{t\to\infty} e_{zu} = 0$) [10].*

Proof. Let the Lyapanov function candidate V_1 be such that [10]

$$\begin{aligned}
V_1 &= \frac{1}{2}\left(\frac{1}{25\alpha + 10} e_{xu}^2 + \frac{1}{2\,(1 - 29\alpha)}\left(e_{yu}^2 + e_{zu}^2\right)\right) \\
&= \frac{1}{2} e^T P e
\end{aligned} \tag{16}$$

where $e = [e_{xu}, e_{yu}, e_{zu}]^T$ and P is such that

$$P = \begin{bmatrix} \dfrac{1}{25\alpha + 10} & 0 & 0 \\ 0 & \dfrac{1}{2\,(1 - 29\alpha)} & 0 \\ 0 & 0 & \dfrac{1}{2\,(1 - 29\alpha)} \end{bmatrix} \tag{17}$$

Clearly, the matrix P is positive definite when α is in the interval $[0,\ 1/29)$. This implies that $V_1 > 0$ when $\alpha \in [0,\ 1/29)$.

The derivative of V_1 with respect to time along the trajectories of the error system (15) is

$$\begin{aligned}
\dot{V}_1 &= \frac{1}{25\alpha + 10} e_{xu}\dot{e}_{xu} + \frac{1}{2\,(1 - 29\alpha)}\left(e_{yu}\dot{e}_{yu} + e_{zu}\dot{e}_{zu}\right) \\
&= e_{xu}\left(e_{yu} - e_{xu}\right) \\
&\quad + \frac{1}{2\,(1 - 29\alpha)}\left(e_{yu}\left(-x_m e_{zu} + (29\alpha - 1)\, e_{yu}\right)\right. \\
&\quad \left. + e_{zu}\left(x_m e_{yu} - \frac{\alpha + 8}{3} e_{zu}\right)\right) = e_{xu}e_{yu} - e_{xu}^2 - \frac{1}{2} e_{yu}^2 \\
&\quad - \frac{\alpha + 8}{6\,(1 - 29\alpha)} e_{zu}^2 = -e^T Q e
\end{aligned} \tag{18}$$

where Q is defined as

$$Q = \begin{bmatrix} 1 & -\frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & \frac{\alpha + 8}{6(1 - 29\alpha)} \end{bmatrix}. \quad (19)$$

When $\alpha \in [0,\ 1/29)$, the matrix Q is positive definite which implies that $\dot{V}_1$ is negative definite. Therefore, it is guaranteed that the errors e_{xu}, e_{yu}, and e_{zu} asymptotically converge to zero when $\alpha \in [0,\ 1/29)$. In conclusion, the signal $x_m(t)$ will force the slave system (13) to be synchronized with the master system (12). □

Hence, after a time T_s, the unified chaotic systems will be synchronized, and the states x_{u1}, y_{u1}, and z_{u1} can be retrieved at the receiver side. These states are then used to unmask the states y_m^e, z_m^e, and w_m^e at the receiver side to obtain the states of the Chen system at the transmitter side as follows:

$$\begin{aligned} y_m^d(t) &= y_m(t) \\ z_m^d(t) &= z_m(t) \\ w_m^d(t) &= w_m(t), \quad for\ t > T_s. \end{aligned} \quad (20)$$

Let the synchronization errors between the two Chen systems be such that

$$\begin{aligned} e_x &= x_s - x_m \\ e_y &= y_s - y_m \\ e_z &= z_s - z_m \\ e_w &= w_s - w_m. \end{aligned} \quad (21)$$

By differentiating these errors with respect to time and using (10) and (11), we obtain the following error system:

$$\begin{aligned} \dot{e}_x &= a(e_y - e_x) + e_w + u_1 \\ \dot{e}_y &= de_x - z_s e_x - x_s e_z + e_x e_z + ce_y + D + u_2 \\ \dot{e}_z &= x_s e_y + y_s e_x - e_y e_x - be_z + u_3 \\ \dot{e}_w &= z_s e_y + y_s e_z - e_y e_z + re_w + u_4 \\ \dot{e}_{xu} &= (25\alpha + 10)(e_{yu} - e_{xu}) \\ \dot{e}_{yu} &= -x_m e_{zu} + (29\alpha - 1) e_{yu} \\ \dot{e}_{zu} &= x_m e_{yu} - \frac{\alpha + 8}{3} e_{zu}. \end{aligned} \quad (22)$$

Theorem 2. *Let the controllers be designed such that*

$$\begin{aligned} u_1 &= -a(e_y - e_x) - e_w - K_1 \operatorname{sign}(e_x) \\ u_2 &= -de_x + z_s e_x + x_s e_z - e_x e_z - ce_y - K_2 \operatorname{sign}(e_y) \\ u_3 &= -x_s e_y - y_s e_x + e_y e_x + be_z - K_3 \operatorname{sign}(e_z) \\ u_4 &= -z_s e_y - y_s e_z + e_y e_z - re_w - K_4 \operatorname{sign}(e_w). \end{aligned} \quad (23)$$

If the above controllers are applied to the slave system (11) at the receiver, the asymptotic convergence of the synchronization errors to zero is guaranteed.

Proof. Consider the following Lyapunov function candidate,

$$V_2 = \frac{1}{2}e_x^2 + \frac{1}{2}e_y^2 + \frac{1}{2}e_z^2 + \frac{1}{2}e_w^2 \quad (24)$$

Using the proposed controllers in (23), the derivative of V_2 with respect to time along the trajectories in (22) can be written as follows:

$$\begin{aligned} \dot{V}_2 &= e_x\dot{e}_x + e_y\dot{e}_y + e_z\dot{e}_z + e_w\dot{e}_w \\ &= e_x\left(a(e_y - e_x) + e_w + u_1\right) \\ &\quad + e_y\left(de_x - z_s e_x - x_s e_z + e_x e_z + ce_y + D + u_2\right) \\ &\quad + e_z\left(x_s e_y + y_s e_x - e_y e_x - be_z + u_3\right) \\ &\quad + e_w\left(z_s e_y + y_s e_z - e_y e_z + re_w + u_4\right) \\ &= -K_1 e_x \operatorname{sign}(e_x) - K_2 e_y \operatorname{sign}(e_y) + De_y \\ &\quad - K_3 e_z \operatorname{sign}(e_z) - K_4 e_w \operatorname{sign}(e_w) \\ &\le -K_1|e_x| - (K_2 - |D_2|)|e_y| - K_3|e_z| - K_4|e_w| \end{aligned} \quad (25)$$

It is evident from (25) that $\dot{V}_2 < 0$ for $K_2 > |D_2|$. Therefore, the asymptotic convergence of e_x, e_y, e_z, and e_w is guaranteed. Furthermore, if $\alpha \in [0,\ 1/29)$, it is ensured that e_{xu}, e_{yu}, and e_{zu} will asymptotically converge to zero as well according to (1). Thus, the proposed controllers force the synchronization errors to converge to zero asymptotically. □

As a result, the proposed controllers in (23) guarantee that the slave system is synchronized with the master system; a noisy version of the transmitted message can be recuperated according to the equation $\widetilde{m}(t) = y_s - y_m$.

Remark 3. The signal $x_m(t)$ is used to generate the parameter $\alpha(t)$ to make sure that $\alpha(t) \in [0, 1/29]$. One of the possible generation rules that can be used is $\alpha(t) = |x_m|/29(|x_m| + 1)$. Note that the α generation rule must be the same at both the transmitter and receiver sides.

5. The Proposed Secure Communication Scheme

A unique secure communication scheme developed by using the K-L decomposition and the synchronization of a combined hyperchaotic Chen system and the unified chaotic system is examined in this section. The developed scheme is utilized to transmit gray-scale and color videos through the encryption of the transmitted data. Figure 1 depicts a block diagram of the proposed secure communication scheme. The description of the scheme is as follows.

Consider a video (we will call it data) that requires secure transmission. We apply a separation rule to the data such that

(i) If the data is a gray-scale video, then the data is decomposed into N frames. The gray-scale frames are represented by an $m \times n$ data matrix containing the gray levels of the pixels.

(ii) If the data is a color video, then it is decomposed into N frames. The color frames (RGB frame) are represented using an $m \times n \times 3$ data matrix which specifies the levels of red, green, and blue color components for each pixel.

Using the Karhunen-Loéve decomposition on the N frames, one can generate the data coefficients and the eigenfunctions of the data. The eigenfunctions are transmitted without encryption through a public channel; this is the case because it is impossible to recreate the original data using only the eigenfunctions. To encrypt the data coefficients, we add them to one of the states in the master system. This is done by transforming the data coefficients into binary format to form a sequence of pulses $\gamma m(t)$ where the scalar γ represents the amplitude of the pulses. The sequence of pulses is appended to the state y_m of the master system to be encrypted. The states of the new system are then transmitted to the receiver through a noise-free public channel.

It is well known that hyperchaotic systems are extremely sensitive to initial conditions; hence it will not be possible to recover the original data using the transmitted states even if these states are intercepted. The reason for that is that the eigenfunctions of the original data are not known to the intruder who successfully intercepts the master system even in the case when the data coefficients are successfully retrieved. Hence, the proposed scheme for data transmission is very secure.

In Figure 1, the master system at the transmitter is considered to be a combination of the hyperchaotic Chen system (System A) and transmitted directly through the public channel. The states of the unified chaotic system (System B) at the transmitter (x_{u1}, y_{u1}, and z_{u1}) are used to mask the y_m, z_m, and w_m states of the hyperchaotic Chen system (System A) producing the masked states y_m^e, z_m^e, and w_m^e, respectively. This stage is considered to increase the complexity of the proposed encryption to ensure that intruders are unable to retrieve any information from the transmitted data. The masked states are then transmitted to the receiver through the public channel. It should be noted that the masking rules should be the same at the transmitter and receiver sides.

The received x_m state is utilized to drive the unified chaotic system (System D) and is used to generate the parameter $\alpha(t)$ with the same generation rule that is used at the transmitter side. After the synchronization between the two unified chaotic systems, the states x_{u1}, y_{u1}, and z_{u1} are retrieved at the receiver side. These states are then utilized to unmask the received masked states y_m^e, z_m^e, and w_m^e to obtain the states y_m, z_m, and w_m. Using these generated states, a controller which is based on the sliding mode technique is used to synchronize the hyperchaotic Chen system (System C) at the receiver with the one at the transmitter. After the synchronization, a noisy version of the transmitted message $m_c(t)$ (data coefficients) can be retrieved and filtered in order to reconstruct the original message $\widetilde{m}(t)$.

Once we obtain the retrieved message $\widetilde{m}(t)$, we can recover the transmitted binary data coefficients and convert them back to real values. The obtained real-valued data coefficients along with the received eigenfunctions are used to recreate the original transmitted video by using (7).

6. Simulation Studies

Two simulation cases of the proposed communication scheme are presented in this section. The first case deals with the transmission of gray-scale videos while the second case deals with the transmission of color videos. In each of the two cases, the original video is decomposed into $N = 49$ frames; each frame is represented by a 120×160 data matrix for each of the gray-scale frames and for the color frames. These two cases are presented in the following two subsections.

6.1. Transmission of a Gray-Scale Video. In this subsection, we present the case of transmitting a gray-scale video using the proposed secure communication scheme. We consider a video from the Matlab toolbox of a traffic camera that observes vehicular behavior on a road for about 3.25 seconds. This video has 49 frames with a dimension of 120×160 pixels, and these frames are shown in Figure 2.

First, the K-L decomposition is applied on these 49 frames to obtain 49 eigenfunctions. Figure 3 depicts the most 16 energetic eigenfunctions. The generated 16 most energetic eigenfunctions are transmitted using a public channel. The energy associated with each eigenfunctions is shown in Figure 4. Figure 4(a) depicts the energy of all eigenfunctions while Figure 4(b) illustrates the energy associated with the remaining eigenfunctions not including the first one. It is noted from this figure that the first eigenfunction captures most of the energy (about 97.13 %).

The data coefficients are converted into binary numbers, and a sequence of pulses with a period $T_p = 1$ is formed to represent the data coefficients. That is, the formed message is such that

$$m(t) = \begin{cases} 1 & \text{if the bit is 1 } \forall t \in \left[t_0, t_0 + T_p\right] \\ 0 & \text{if the bit is 0 } \forall t \in \left[t_0, t_0 + T_p\right] \end{cases} \tag{26}$$

The message $m(t)$ is added to the master system at the transmitter in the y_m state. Additionally, we define the generation rule of the α parameter to be such that

$$\alpha(t) = \frac{|x_m|}{29\left(|x_m| + 1\right)}. \tag{27}$$

This choice of the α generation rule ensures that $\alpha \in [0, 1/29)$. Then the produced states of the unified chaotic system x_{u1}, y_{u1}, and z_{u1} are used to mask the states y_m, z_m, and w_m. The masking rules are chosen in the following recursive manner:

$$\begin{aligned} y_m^e &= \frac{y_m + x_{u1}}{|x_{u1}| + 1} \\ z_m^e &= y_m^e + \frac{z_m - y_{u1}}{|y_{u1}| + 1} \\ w_m^e &= z_m^e + \frac{w_m + z_{u1}}{|z_{u1}| + 1}. \end{aligned} \tag{28}$$

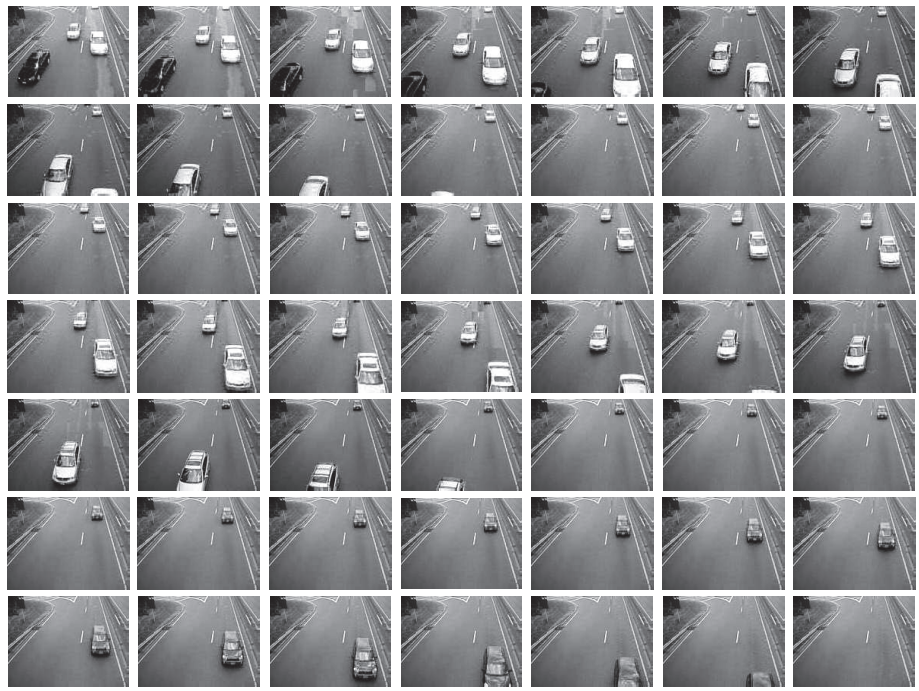

Figure 2: The frames of the original gray-scale video to be transmitted using the proposed scheme.

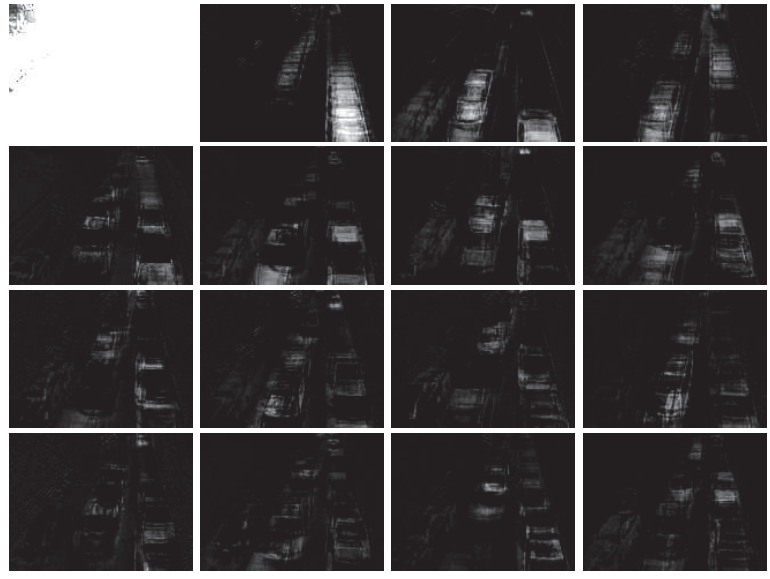

Figure 3: The most 16 energetic eigenfunctions.

After adding the message to the master system, masking the states, and transmitting them, the proposed controller forces the slave system to synchronize with the master system. This fact can be clearly seen from Figures 5 and 6; Figure 5 depicts the synchronization errors of the Chen systems while Figure 6 depicts the synchronization errors of the unified chaotic systems. It is evident that all errors converge to zero except e_y which contains a noisy version of the transmitted data. Therefore, the original data is recovered from e_y after filtering it. Part of the recovered message is shown in Figure 7.

Using the recovered message, the data coefficients are then recovered and utilized alongside the received eigenfunctions in order to reconstruct the original vectors according to (7) which are reshaped to 120×160 arrays to reconstruct the original frames. The reconstructed frames using all eigenfunctions are presented in Figure 8. This clearly verifies the efficiency of the proposed scheme.

To demonstrate that the developed communication scheme has another attribute besides being secure, the transmitted video can be reconstructed using some of the

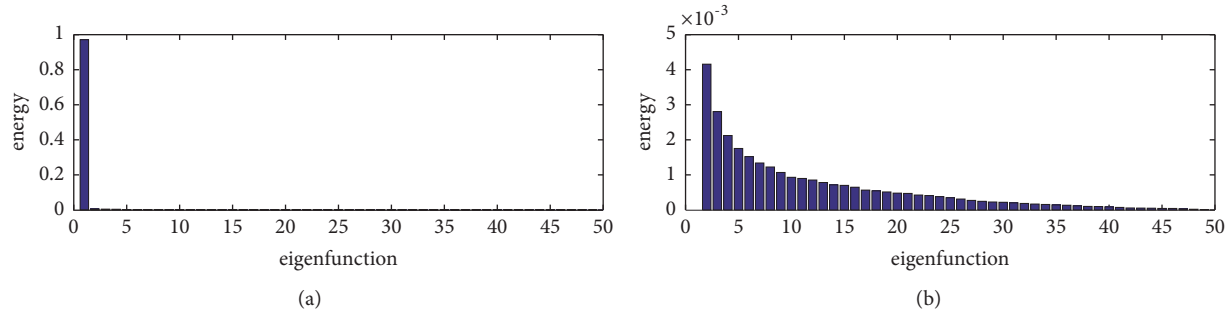

Figure 4: (a) Energy associated with all eigenfunctions. (b) Energy associated with all the eigenfunctions except the first one (gray-scale video).

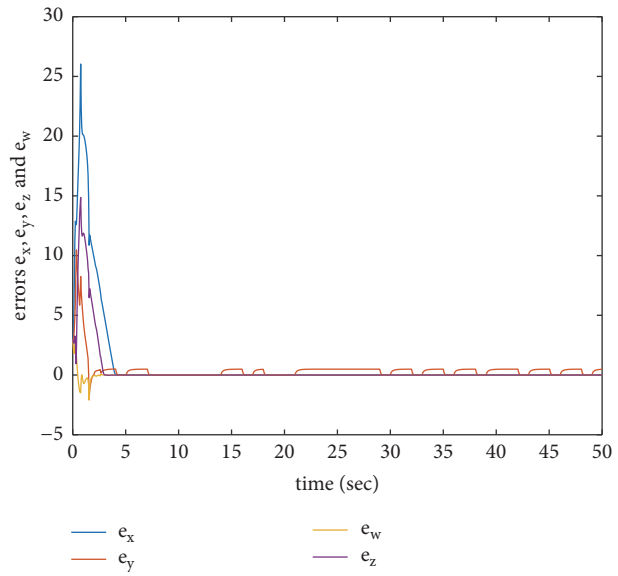

Figure 5: The errors of the Chen systems versus time for 50 seconds (gray-scale video).

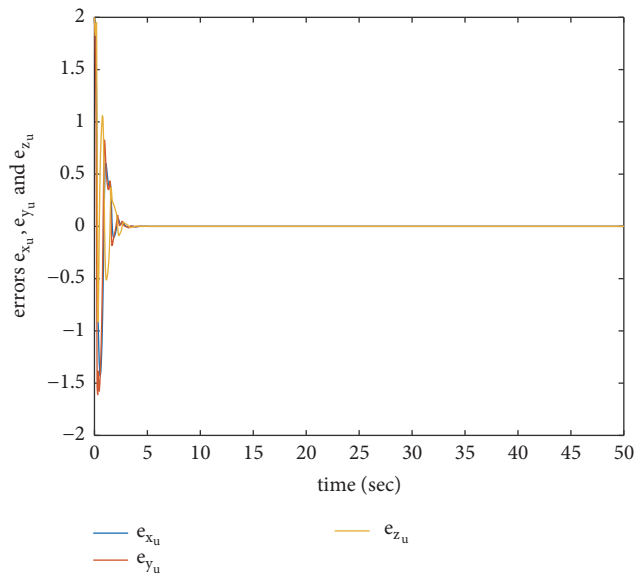

Figure 6: The errors of the unified chaotic systems versus time for 50 seconds (gray-scale video).

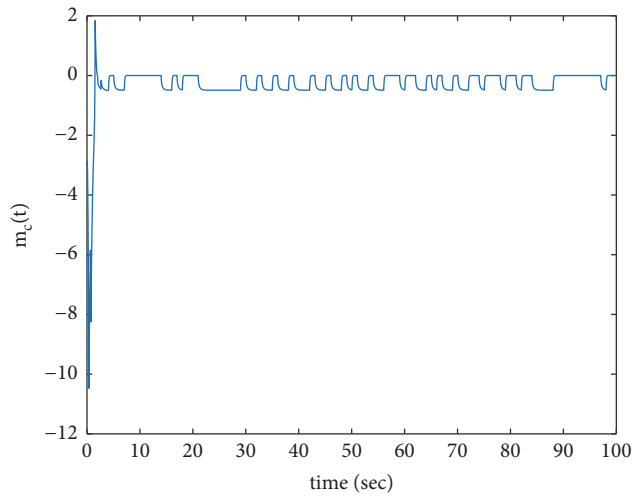

FIGURE 7: The recovered signal $m_c(t)$ versus time for 100 seconds (gray-scale video).

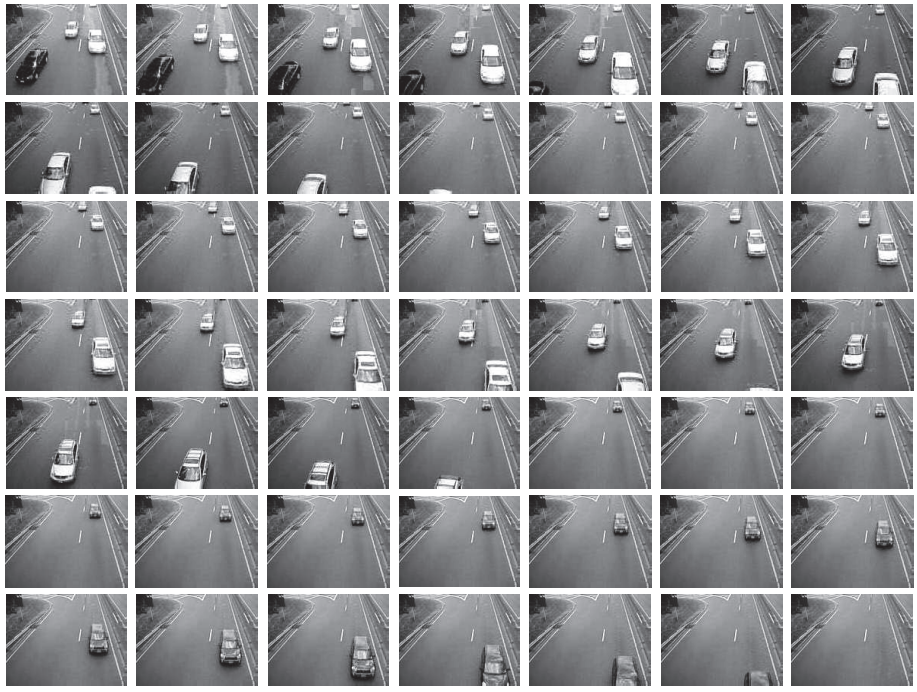

FIGURE 8: The recovered gray-scale video using all eigenfunctions.

eigenfunctions (see Figure 9). Figure 9 depicts the reconstructed video using the most 35 energetic eigenfunctions along with their corresponding data coefficients. Furthermore, the Peak Signal-to-Noise Ratio (PSNR) [65], which is a known video quality metric, was used to compare the quality of the reconstructed videos for different cases. The calculated PSNR values are 51.6 dB, 40.3 dB, 36.8 dB, and 27.5 dB when using 49, 35, 30, and 15 most energetic eigenfunctions, respectively. It should be noted that PSNR was calculated by comparing each frame with its reference and then taking the average for the whole video. It can be seen from these results that a better quality can be obtained by using more eigenfunctions, and the best case is by using all eigenfunctions.

6.2. Transmission of a Color Video. In this subsection, we consider the transmission of a color video using the developed communication scheme. The color version of the traffic video used in Section 6.1 is utilized here. Figure 10 presents the frames of the color video which are represented by a $120 \times 160 \times 3$ data matrices.

First, K-L decomposition is applied on these 49 frames to obtain 49 eigenfunctions. Figure 11 depicts the most 16 energetic eigenfunctions. The generated 16 most energetic eigenfunctions are transmitted using a public channel. Figure 12 depicts the energy associated with each eigenfunctions. Figure 12(a) shows the energy of all eigenfunctions while Figure 12(b) depicts the energy associated

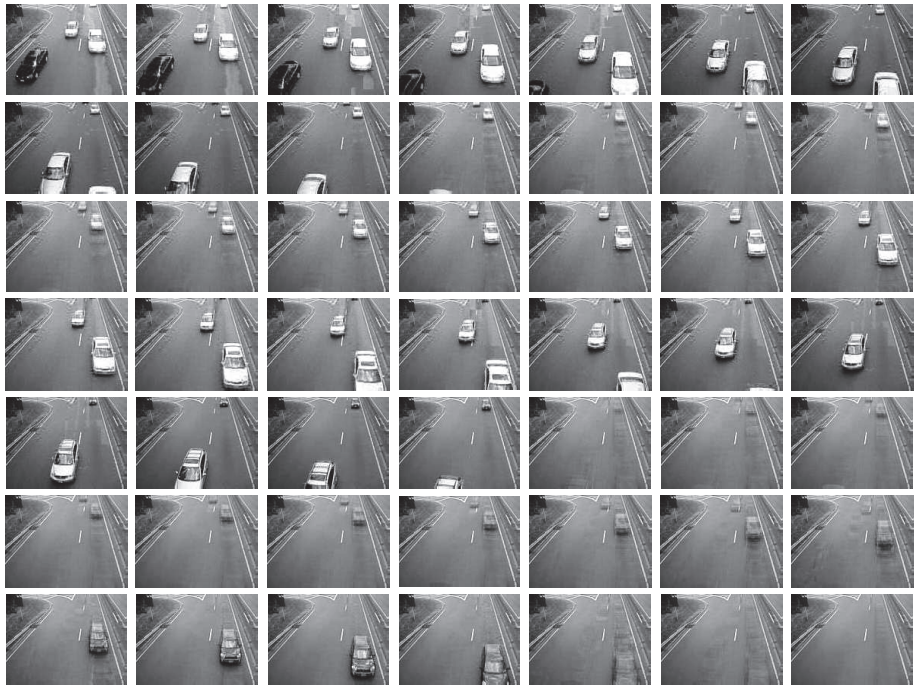

Figure 9: The recovered gray-scale video using the most 35 energetic eigenfunctions.

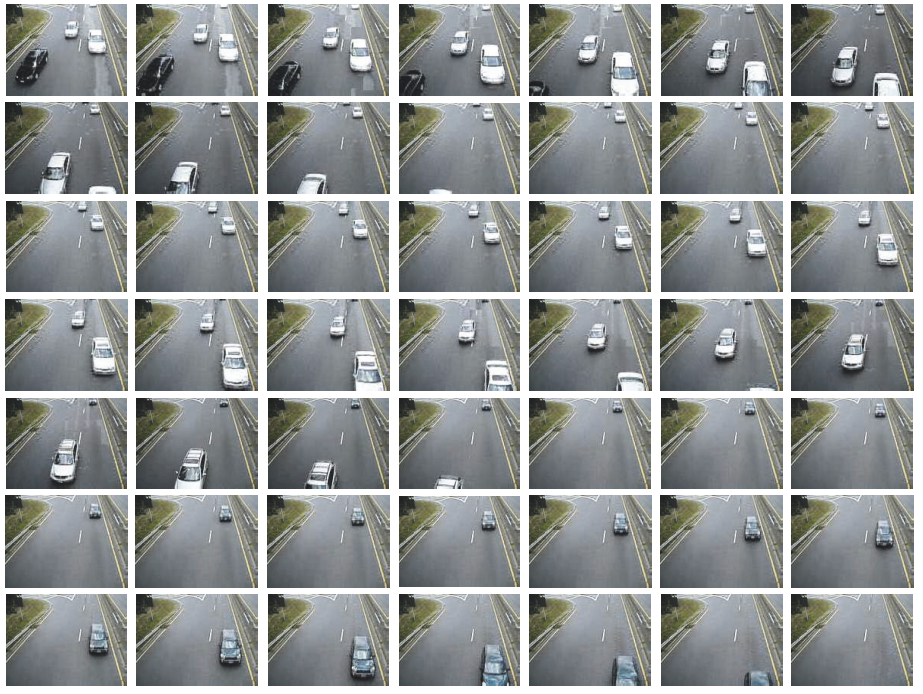

Figure 10: The frames of the original color video to be transmitted using the proposed scheme.

with the rest of the eigenfunctions not including the first one.

Next, we transform the obtained data coefficients into binary to form a sequence of pulses as described in Section 6.1. This sequence of pulses is added to the y_m state of the master system and all the states of the system are masked and transmitted. The sliding mode control law at the receiver end is used to synchronize the master and slave systems; see Figures 13 and 14. A noisy version of the transmitted data is then recovered by using e_y where a part of that message is shown in Figure 15.

Once the sent message is recovered, it is transformed back from binary to obtain the real-valued data coefficients. The recovered data coefficients are used in conjunction with

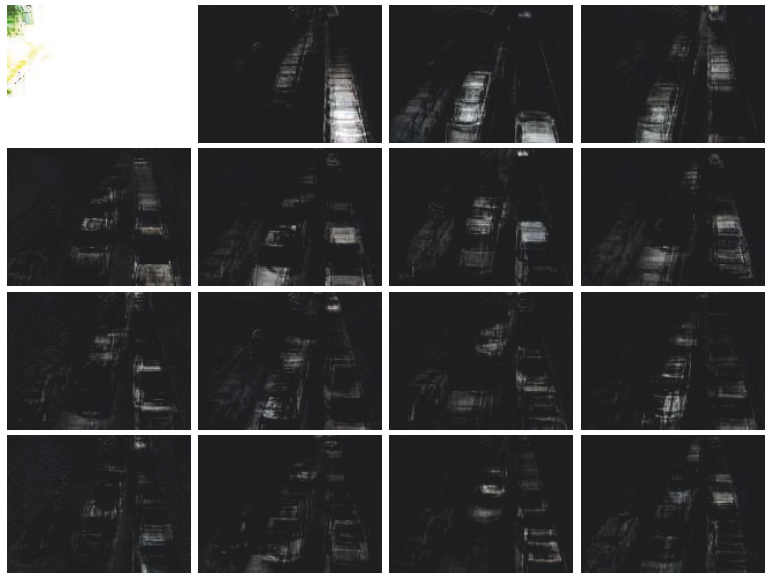

Figure 11: The most 16 energetic eigenfunctions.

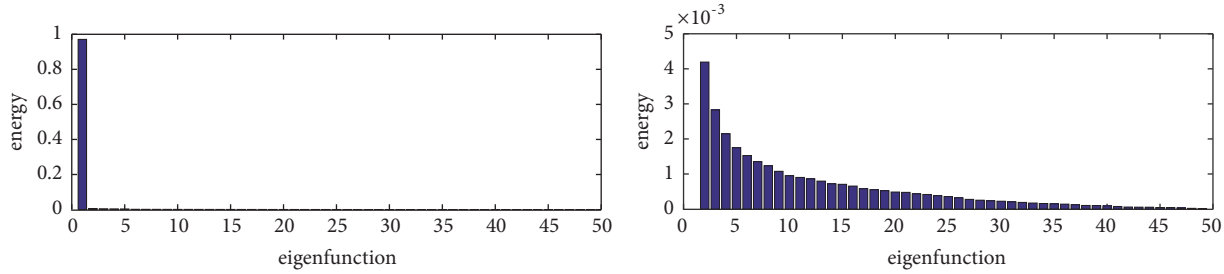

Figure 12: Energy associated with the eigenfunctions (color video).

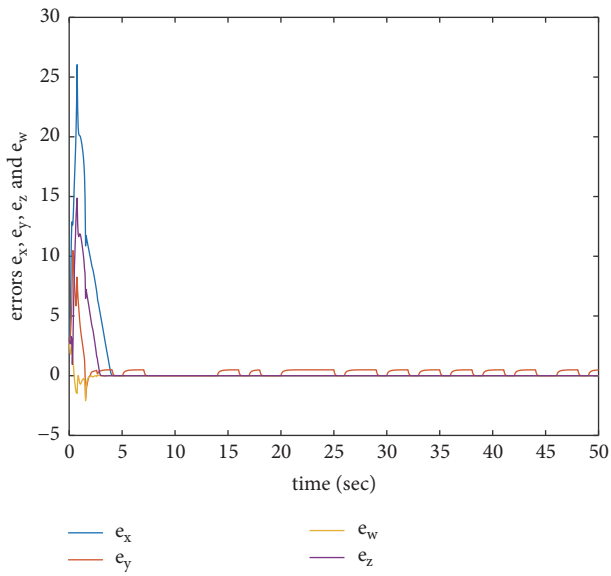

Figure 13: The errors of the Chen systems versus time for 50 seconds (color video).

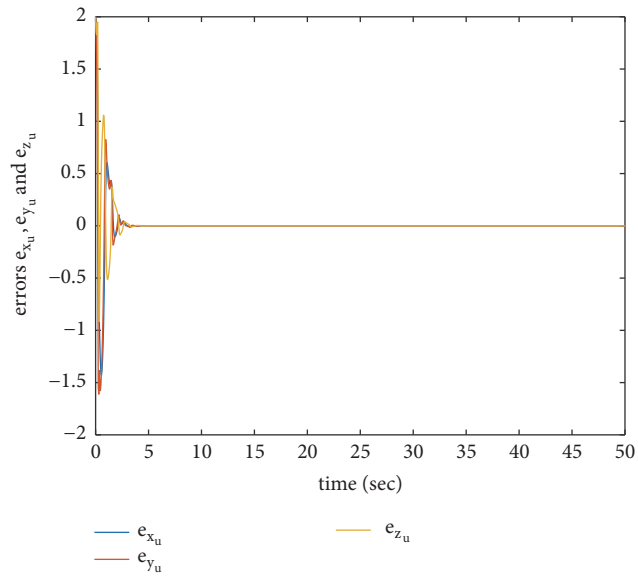

Figure 14: The errors of the unified chaotic systems versus time for 50 seconds (color video).

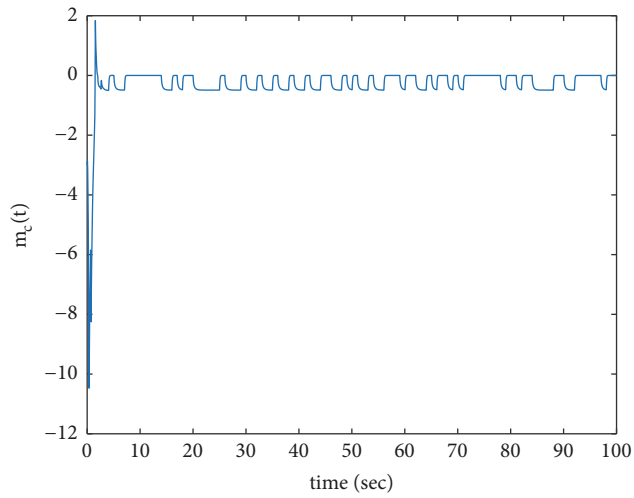

Figure 15: The recovered signal $m_c(t)$ versus time for 100 seconds (color video).

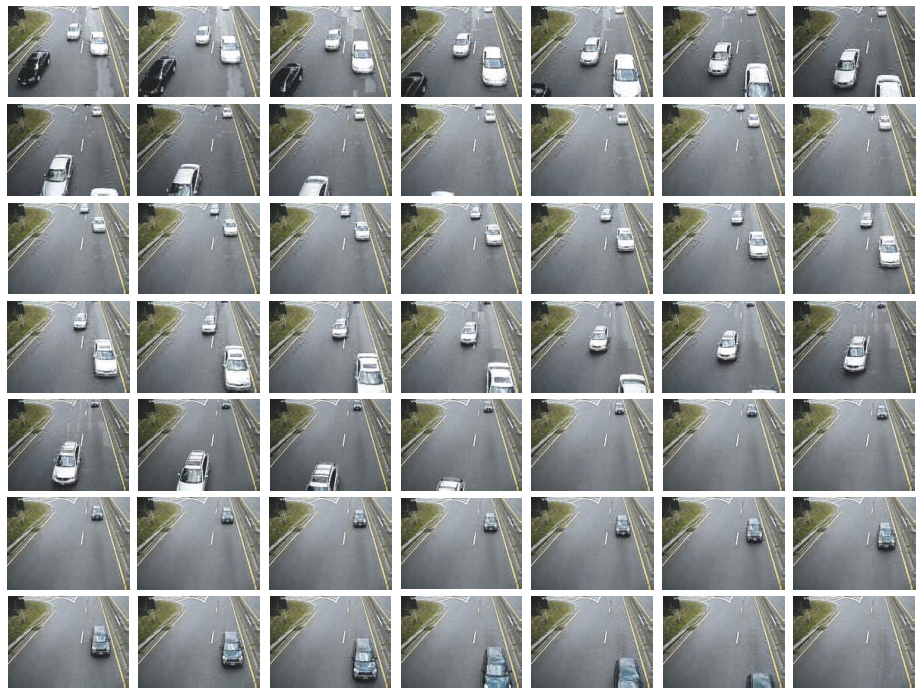

Figure 16: The recovered video using all eigenfunctions (color video).

the received eigenfunctions to reconstruct the data vectors using (7). Finally, the data vectors are reshaped to retrieve the transmitted color frames. The retrieved frames using all eigenfunctions which proves the efficiency of the developed communication scheme are presented in Figure 16.

The reconstructed frames when only the most 35 energetic eigenfunctions are used are shown in Figure 17. Moreover, the PSNR was calculated as a quality metric by considering different cases using 49, 35, 30, and 15 most energetic eigenfunctions for transmission and reconstruction. The corresponding PSNR values are 56.7 dB, 41.8 dB, 37.4 dB, and 27.5 dB, respectively. It is obvious that the reduction of transmitted eigenfunctions and coefficients comes at the expense of the reconstructed video quality which is a trade-off that can be made depending the desired requirements.

7. Conclusion

This article considers a unique secure communication scheme developed by using the Karhunen-Loéve decomposition and the synchronization of master with slave systems where each system consists of the Chen hyperchaotic system and the unified chaotic system is considered. The Karhunen-Loéve decomposition is employed as a data reduction method to successfully generate data coefficients and optimal eigenfunctions that capture the original set of video frames. Using

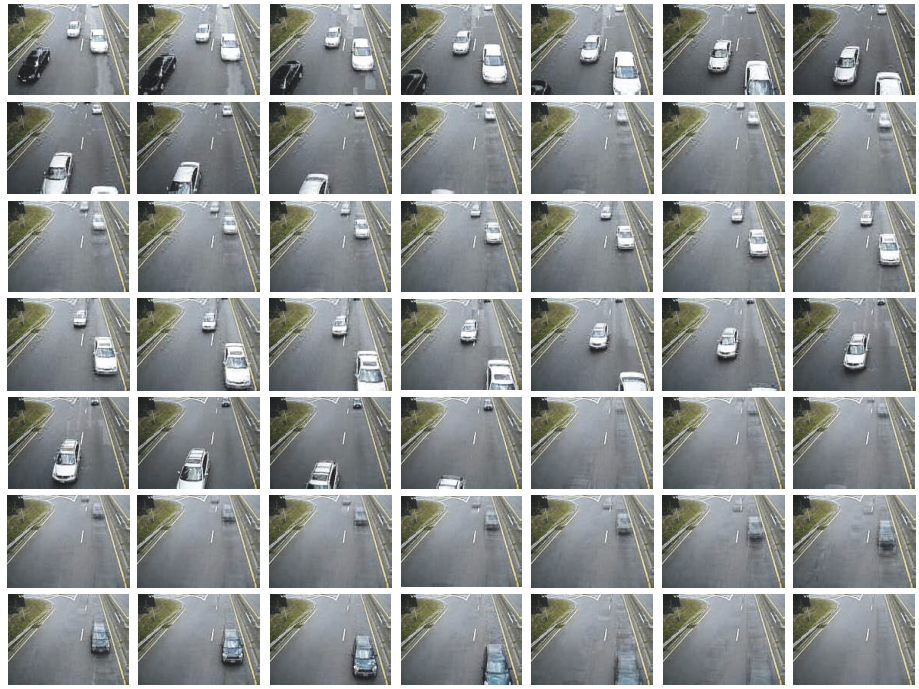

Figure 17: The recovered video using the most 35 energetic eigenfunctions (color video).

only the most energetic eigenfunctions to approximate the original frames leads to computational savings. The obtained data coefficients are encrypted before being transmitted using a master system and received using a slave system through the secure communication scheme. A sliding mode control design is presented to synchronize the master and slave systems. Furthermore, computer simulations are executed to verify the performance of the proposed scheme, and the results of these simulations are presented and discussed.

The real-time implementation of the proposed method is a challenging task and will be the subject of future research studies.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos," *Physical Review Letters*, vol. 64, no. 11, pp. 1196–1199, 1990.

[2] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, 1990.

[3] C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," *International Journal of Bifurcation and Chaos*, vol. 3, no. 6, pp. 1619–1627, 1993.

[4] T. Yang and L. O. Chua, "Secure communication via chaotic parameter modulation," *IEEE Transaction on Circuits and Systems*, vol. 43, no. 9, pp. 817–819, 1996.

[5] G. Chen and T. Ueta, "Yet another chaotic attractor," *International Journal of Bifurcation and Chaos*, vol. 9, no. 7, pp. 1465-1466, 1999.

[6] J. Lü and G. Chen, "A new chaotic attractor coined," *International Journal of Bifurcation and Chaos*, vol. 12, no. 3, pp. 659–661, 2002.

[7] J. Q. Lu and J. D. Cao, "Adaptive complete synchronization of two identical or different chaotic (hyperchaotic) systems with fully unknown parameters," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 15, no. 4, Article ID 043901, 10 pages, 2005.

[8] J. H. Park, "Adaptive synchronization of hyperchaotic Chen system with uncertain parameters," *Chaos, Solitons & Fractals*, vol. 26, no. 3, pp. 959–964, 2005.

[9] A. Chen, J. Lu, J. Lü, and S. Yu, "Generating hyperchaotic Lü attractor via state feedback control," *Physica A: Statistical Mechanics and its Applications*, vol. 364, pp. 103–110, 2006.

[10] N. Smaoui, A. Karouma, and M. Zribi, "Secure communications based on the synchronization of the hyperchaotic Chen and the unified chaotic systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 8, pp. 3279–3293, 2011.

[11] S.-J. Cho, M. Jin, T.-Y. Kuc, and J. S. Lee, "Control and synchronization of chaos systems using time-delay estimation and supervising switching control," *Nonlinear Dynamics*, vol. 75, no. 3, pp. 549–560, 2014.

[12] Z.-P. Wang and H.-N. Wu, "Synchronization of chaotic systems using fuzzy impulsive control," *Nonlinear Dynamics*, vol. 78, no. 1, pp. 729–742, 2014.

[13] Y. Liu and S. M. Lee, "Control and synchronization of chaos systems using time-delay estimation and supervising switching control," *Nonlinear Dynamics*, pp. 1–12, 2016.

[14] D. Liu, Z. Wu, and Q. Ye, "Adaptive impulsive synchronization of uncertain drive-response complex-variable chaotic systems," *Nonlinear Dynamics*, vol. 75, no. 1-2, pp. 209–216, 2014.

[15] X. Yang, Z. Yang, and X. Nie, "Exponential synchronization of discontinuous chaotic systems via delayed impulsive control and its application to secure communication," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 5, pp. 1529–1543, 2014.

[16] X.-T. Tran and H.-J. Kang, "Robust adaptive chatter-free finite-time control method for chaos control and (anti-)synchronization of uncertain (hyper)chaotic systems," *Nonlinear Dynamics*, vol. 80, no. 1-2, pp. 637–651, 2015.

[17] L. Liu, W. Ding, C. Liu, H. Ji, and C. Cao, "Hyperchaos synchronization of fractional-order arbitrary dimensional dynamical systems via modified sliding mode control," *Nonlinear Dynamics*, vol. 76, no. 4, pp. 2059–2071, 2014.

[18] X. Xiao, L. Zhou, and Z. Zhang, "Synchronization of chaotic Lur'e systems with quantized sampled-data controller," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 2039–2047, 2014.

[19] X. Wu and H. Zhang, "Synchronization of two hyperchaotic systems via adaptive control," *Chaos, Solitons and Fractals*, vol. 39, no. 5, pp. 2268–2273, 2009.

[20] M. Zribi, N. Smaoui, and H. J. Salim, "Synchronization of the unified chaotic systems using a sliding mode controller," *Chaos, Solitons & Fractals*, vol. 42, no. 5, pp. 3197–3209, 2009.

[21] Y. Li, W. K. S. Tang, and G. Chen, "Generating hyperchaos via state feedback control," *International Journal of Bifurcation and Chaos*, vol. 15, no. 10, pp. 3367–3376, 2005.

[22] C. Tao and X. Liu, "Feedback and adaptive control and synchronization of a set of chaotic and hyperchaotic systems," *Chaos, Solitons & Fractals*, vol. 32, no. 4, pp. 1572–1581, 2007.

[23] P. V. Kokotovie, "The joy of feedback: nonlinear and adaptive," *IEEE Control Systems Magazine*, vol. 12, no. 3, pp. 7–17, 1992.

[24] J. Hu, S. Chen, and L. Chen, "Adaptive control for anti-synchronization of Chua's chaotic system," *Physics Letters A*, vol. 39, no. 6, pp. 455–460, 2005.

[25] W.-H. Chen, D. Wei, and X. Lu, "Global exponential synchronization of nonlinear time-delay Lur'e systems via delayed impulsive control," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 9, pp. 3298–3312, 2014.

[26] S. Shao, M. Chen, and X. Yan, "Adaptive sliding mode synchronization for a class of fractional-order chaotic systems with disturbance," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 1855–1866, 2016.

[27] Q. Jia, "Adaptive control and synchronization of a new hyperchaotic system with unknown parameters," *Physics Letters A*, vol. 362, pp. 424–429, 2007.

[28] T. L. Carroll and L. M. Pecora, "Synchronizing chaotic circuits," *IEEE Transaction on Circuits and Systems*, vol. 38, no. 4, pp. 453–456, 1991.

[29] X. Wu, C. Bai, and H. Kan, "A new color image crytosystem via hyperchaos synchronization," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 1884–1897, 2014.

[30] M. A. Rafique, M. Rehan, and M. Siddique, "Adaptive mechanism for synchronization of chaotic oscillators with interval time-delays," *Nonlinear Dynamics*, vol. 81, no. 1-2, pp. 495–509, 2015.

[31] J. A. Vargas, E. Grzeidak, and E. M. Hemerly, "Robust adaptive synchronization of a hyperchaotic finance system," *Nonlinear Dynamics*, vol. 80, no. 1-2, pp. 239–248, 2015.

[32] M. Xiao and J. Cao, "Synchronization of a chaotic electronic circuit system with cubic term via adaptive feedback control," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 8, pp. 3379–3388, 2009.

[33] L. P. Liu, J. Pu, X. Song, Z. Fu, and X. Wang, "Adaptive sliding mode control of uncertain chaotic systems with input nonlinearity," *Nonlinear Dynamics*, vol. 76, no. 4, pp. 1857–1865, 2014.

[34] N. Smaoui, M. Zribi, and T. Elmokadem, "A novel secure communication scheme based on the Karhunen-Loéve decomposition and the synchronization of hyperchaotic Lü systems," *Nonlinear Dynamics*, vol. 90, no. 1, pp. 271–285, 2017.

[35] Z. Lin, S. Yu, C. Li, J. Lü, and Q. Wang, "Design and smartphone-based implementation of a chaotic video communication scheme via WAN remote transmission," *International Journal of Bifurcation and Chaos*, vol. 26, no. 9, Article ID 1650158, 8 pages, 2016.

[36] P. Chen, S. Yu, X. Zhang et al., "ARM-embedded implementation of a video chaotic secure communication via WAN remote transmission with desirable security and frame rate," *Nonlinear Dynamics*, vol. 86, no. 2, pp. 725–740, 2016.

[37] P. Thapliyal and M. Sharma, "Image Encryption and Authentication Scheme using 3D Chaotic Map," *International Journal of Computer Applications*, vol. 117, no. 17, pp. 15–18, 2015.

[38] Y. Liu, X. Tong, and S. Hu, "A family of new complex number chaotic maps based image encryption algorithm," *Signal Processing: Image Communication*, vol. 28, no. 10, pp. 1548–1559, 2013.

[39] S. Mohammadi, "A semi-blind watermarking algorithm for color images using chaotic maps," *Journal of Knowledge-Based Engineering and Innovation, JKBEI*, 2015.

[40] S. Chen, S. Yu, J. Lu, G. Chen, and J. He, "Design and FPGA-Based Realization of a Chaotic Secure Video Communication System," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 9, pp. 2359–2371, 2018.

[41] Z. Lin, S. Yu, J. Lü, S. Cai, and G. Chen, "Design and ARM-Embedded Implementation of a Chaotic Map-Based Real-Time Secure Video Communication System," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 7, pp. 1203–1216, 2015.

[42] K. Ganesan, J. G. George, and P. V. Nithin, "Real Time Secure Video Transmission Using Multicore CPUs and GPUs," *Advances in Computing*, vol. 5, no. 1, pp. 1–8, 2015.

[43] A. Christian and R. Shelth, "Secured digital video authentication system," *International Journal of Scientific Research in Science and Technology*, vol. 3, no. 3, pp. 223–227, 2017.

[44] F. Liu and H. Koenig, "A survey of video encryption algorithms," *Computers & Security*, vol. 29, no. 1, pp. 3–15, 2010.

[45] Y. Negi, "A survey on video encryption techniques," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 4, pp. 234–237, 2008.

[46] W. Wang, H. Huang, C. Xie, and L. Han, "CBSNTS: A choatic based security network transmission system," *Journal of Networks*, vol. 9, no. 8, p. 1985, 2014.

[47] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Secure advanced video coding based on selective encryption algorithms," *IEEE Transactions on Consumer Electronics*, vol. 52, no. 2, pp. 621–629, 2006.

[48] T. A. Fadil, S. N. Yaakob, B. Ahmad, and A. Yahya, "A chaotic neural network-based encryption algorithm for MPEG-2 encoded video signal," *International Journal of Artificial Intelligence and Soft Computing*, vol. 3, no. 4, pp. 360–371, 2013.

[49] R. C. Gonzalez and P. Wintz, *Digital Image Processing*, pp. 122-130, Addison Wesley, Reading, MA, USA, 2nd edition, 1987.

[50] H. Harman, *Modern Factor Analysis*, The University of Chicago Press, Chicago, USA, 1960.

[51] J. L. Lumley, "The Structure of Inhomogeneous Turbulent Flows," in *Atmospheric Turbulence and Radio Wave Propagation*, A. M. Yaglom and V. I. Tatarski, Eds., pp. 166–178, Nauka, Moskow, 1967.

[52] G. H. Golub and C. F. Van Loan, *Matrix Computations*, North Oxford Academic, Oxford, UK, 1983.

[53] C. L. Brooks, M. Karplus, and B. M. Pettitt, *Proteins: A Theoretical Perspective of Dynamics, Structure and Thermodynamics*, Wiley Publishing Co., New York, USA, 1988.

[54] H. Hoteling, "Analysis of complex statistical variables in principal components," *Journal of Experimental Psychology*, vol. 24, p. 417, 1953.

[55] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the Atmospheric Sciences*, vol. 20, pp. 130–141, 1963.

[56] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, McGraw-Hill, New York, NY, USA, 1965.

[57] A. Rosendeld and A. C. Kak, *Digital Picture Processing*, Academic Press, New York, USA, 1982.

[58] V. R. Algazi and D. J. Sakrison, "On the Optimality of the Karhunen-Loéve expansion," *IEEE Transactions on Information Theory*, vol. 15, no. 2, pp. 319–421, 1969.

[59] C. A. Andrews, J. M. Davies, and G. R. Schwarz, "Adaptive Data Compression," *Proceedings of the IEEE*, vol. 55, no. 3, pp. 267–277, 1967.

[60] N. Smaoui and R. B. Gharbi, "Using Karhunen-Loéve decomposition and artificial neural network to model miscible fluid displacement in porous media," *Applied Mathematical Modelling*, vol. 24, no. 8-9, pp. 657–675, 2000.

[61] N. Smaoui, "Artificial neural network-based low-dimensional model for spatio-temporally varying cellular flames," *Applied Mathematical Modelling*, vol. 21, no. 12, pp. 739–748, 1997.

[62] N. Smaoui and S. Al-Yakoob, "Analyzing the dynamics of cellular flames using Karhunen-Loève decomposition and autoassociative neural networks," *SIAM Journal on Scientific Computing*, vol. 24, no. 5, pp. 1790–1808, 2003.

[63] N. Smaoui, "Linear versus nonlinear dimensionality reduction of high-dimensional dynamical systems," *SIAM Journal on Scientific Computing*, vol. 25, no. 6, pp. 2107–2125, 2004.

[64] L. Sirovich, "Turbulence and the dynamics of coherent structures, Part I: Coherent structures," *Quarterly of Applied Mathematics*, vol. 45, XLV, no. 3, pp. 561–571, 1987.

[65] Q. Huynh-Thu and M. Ghanbari, "The accuracy of PSNR in predicting video quality for different video scenes and frame rates," *Telecommunication Systems*, vol. 49, no. 1, pp. 35–48, 2012.