University of Dundee

Instability of impulsive stochastic systems with application to image encryption

Wei, Tengda; Lin, Ping; Zhu, Quanxin; Yao, Qi

[Link to publication in Discovery Research Portal](#)

Instability of impulsive stochastic systems with application to image encryption

Tengda Wei[a,b], Ping Lin[b], Quanxin Zhu[c,*], Qi Yao[b]

[a]*School of Mathematics and Statistics, Shandong Normal University, Jinan, 250014, PR China*
[b]*Department of Mathematics, University of Dundee, Dundee DD1 4HN, UK*
[c]*MOE-LCSM, School of Mathematics and Statistics, Hunan Normal University, Changsha 410081, PR China*

Abstract

This paper concerns the stochastic instability of impulsive stochastic systems with application to image encryption. Based on comparison principle, the sufficient conditions for instability in probability of impulsive stochastic systems are obtained by the instability of continuous comparison system established by Lyapunov function. It also shows how to determine stochastic instability of impulsive stochastic systems when stability conditions fail. The effectiveness of theoretical results is verified by two numerical examples, whose chaotic signals are successfully used for image encryption.

Keywords: Instability, impulsive stochastic system, comparison principle, image encryption

1. Introduction

Due to wide applications of stochastic systems in financial systems, networks, biological systems and air traffic systems [1–6], the last few decades have witnessed an avalanche of works on stochastic systems [7–12]. Among the recent reported literatures, impulsive stochastic systems (ISSs) have been the common interest of many researchers [13–19] whose intensive efforts are oriented towards

---

[*]Corresponding author.
Email addresses: `tdwei123@sdnu.edu.cn` (Tengda Wei), `plin@maths.dundee.ac.uk` (Ping Lin), `zqx22@126.com` (Quanxin Zhu), `qiyao8@126.com` (Qi Yao)

stability conditions [11]. If the stability conditions are not satisfied, the dynamical behavior of ISSs may be stable or unstable. Therefore, the consequent concern is how to determine instability properties, when stability cannot be ascertained. In [20], Li et al. have studied instability properties of a deterministic impulsive differential system, but there is less relative work about instability properties of ISSs. Therefore, the primary concern of this work is to generalize the method developed in [20] for instability analysis of ISSs.

In stability analysis of ISSs, comparison principle has been an effective method (see [21–24] and references therein). For instance, stochastic stability of ISSs was studied by comparison principle combined with Lyapunov function and Itô formula in [21]. Then, comparison principles with delays were proposed for impulsive stochastic delay systems [22–24]. Most of the existing studies focus on the upper comparison systems for ISSs with stable continuous dynamics and destabilizing impulse or unstable continuous dynamics and stabilizing impulse, and the few care about the lower comparison systems. However, the lower comparison systems are crucial for instability analysis of ISSs because their instability implies the instability of ISSs once the corresponding comparison principle is established. Hence, an additional inspiration of this work is to construct the lower comparison system of unstable ISSs by comparison principle.

As one of the major applications of nonlinear systems, chaos-based image encryption has sparked many valuable works [25–28]. For instance, Fridrich fistly proposed two main procedures of chaos-based image encryption schemes, permutation and diffusion, in [25]. Then, a symmetric image encryption scheme with bit-level permutation was developed in [27], which was extended in [28]. Recently, image encryption schemes based on neural networks were proposed in the literatures [29–31]. In most of the existing works on image encryption, the parameters of nonlinear systems are usually set by experimental tests. The question, under what conditions a nonlinear system is unpredictable by probabilistic polynomial-time machines, is crucial in image ecryption [26]. If ISSs have unstable dynamical behavior, the numerical signals generated by ISSs may be unpredictable, indicating promising application of unstable ISSs to image en-

2

cryption. Moreover, the random factor in stochastic dynamical systems usually causes more fluctuation than deterministic systems, so one may courageously think that stochastic systems, especially ISSs, are likely to generate chaotic signals suitable for image encryption. However, there are less relative studies on the application of ISSs to image encryption.

Motivated by the above discussions, this work investigates the instability of ISSs by comparison principle and proposes an unstable impulsive stochastic system for image encryption. The contribution lies as follows: (1) A novel comparison principle of an impulsive system and a continuous system is given where the instability of the impulsive system can be determined by the continuous comparison system, which extends Ref. [20] to a general case; (2) Based on the comparison results, sufficient conditions for instability in probability of ISSs are obtained to determine instability properties of ISSs when stability conditions fail; (3) The signals generated by ISSs are successfully applied to image encryption.

Notations: $\mathbb{N} = \{1, 2, 3, \cdots\}$. $\mathbb{R}^n$ is the n-dimensional Euclidean space equipped with norm $|\cdot|$. For any interval $T \subseteq \mathbb{R}$ and $I \subseteq \mathbb{R}^n$, $C(T, I) = \{\phi : T \to I$ is continuous$\}$ and $PC(T, I) = \{\phi : T \to I$ is piecewise continuous and $\phi(t^-) = \phi(t)\}$. For a function $\phi : \mathbb{R}^+ \to \mathbb{R}^+$, $D_-\phi(t) \triangleq \liminf\limits_{\Delta t \to 0^-} \frac{\phi(t + \Delta t) - \phi(t)}{\Delta t}$ is the lower-left Dini derivative of $\phi(t)$. The impulsive sequence satisfies $0 \leq t_0 < t_1 < \cdots < t_k < \cdots$ and $\lim\limits_{k \to \infty} t_k = \infty$. $N(t, s)$ represents the number of impulses in interval $[s, t)$. $PC^* = \{\phi \in PC(\mathbb{R}^+, \mathbb{R}^+) | \phi$ is discontinuous only at points $\{t_k\}_{k=1}^\infty\}$. $w(t) = (w_1(t), w_2(t), \cdots, w_l(t))^T$ is an l-dimensional Brownian motion defined on complete probability space $(\Omega, \mathcal{F}, P)$ with a filtration $\{\mathcal{F}_t\}_{t \geq 0}$. For any random variable ξ, $E(\xi)$ denotes the expectation value of ξ. tr is the trace operator. A function $\phi : \mathbb{R}^+ \to \mathbb{R}^+$ is of class $\mathcal{K}_\infty$ if it is continuous, strictly increasing and $\phi(0) = 0$, $\lim\limits_{t \to \infty} \phi(t) = +\infty$. $\mathcal{K}_1 = \{\phi \in \mathcal{K}_\infty : \phi(E(\xi)) \leq E(\phi(\xi))\}$ and $\mathcal{K}_2 = \{\phi \in \mathcal{K}_\infty : \phi(E(\xi)) \geq E(\phi(\xi))\}$ where $\xi \geq 0$ and $E(\xi) < +\infty$.

2. Preliminaries

Consider the following n-dimensional impulsive stochastic systems

$$\begin{cases} dx(t) = f(t, x(t))dt + g(t, x(t))dw(t), & t \geq t_0, \ t \neq t_k, \\ x(t_k^+) = I_k(t_k, x(t_k)), & k \in \mathbb{N}, \end{cases} \quad (1)$$

with initial value $x(t_0) = x_0 \in \mathbb{R}^n$, where $x(t) \in \mathbb{R}^n$, $f : \mathbb{R}^+ \times \mathbb{R}^n \to \mathbb{R}^n$, $g : \mathbb{R}^+ \times \mathbb{R}^n \to \mathbb{R}^{n \times l}$, and $I_k : \mathbb{R}^+ \times \mathbb{R}^n \to \mathbb{R}^n$, $k \in \mathbb{N}$. Assume that f, g and I_k are left continuous with right limit and satisfy local Lipschitz condition and linear growth condition to ensure the existence and uniqueness of the solutions to system (1) [32]. If $f(t, 0) = 0$, $g(t, 0) = 0$, and $I_k(t_k, 0) = 0$ for $k \in \mathbb{N}$, it admits a trivial solution $x(t) \equiv 0$.

Let $\mathcal{C}^{1,2}(\mathbb{R}^+ \times \mathbb{R}^n, \mathbb{R}^+)$ denote the family of all nonnegative functions $V(t, x)$ on $\mathbb{R}^+ \times \mathbb{R}^n$, which are continuous, once differentiable in t and twice differentiable in x. For each $V \in \mathcal{C}^{1,2}(\mathbb{R}^+ \times \mathbb{R}^n, \mathbb{R}^+)$, the Itô operator $\mathcal{L}V(t, x)$ of function $V(t, x)$, associated with system (1), is defined by

$$\mathcal{L}V(t, x) = V_t(t, x) + V_x(t, x)f(t, x) + \frac{1}{2}\text{tr}(g^T(t, x)V_{xx}(t, x)g(t, x)), \quad (2)$$

where $V_t = \frac{\partial V}{\partial t}$, $V_x = (\frac{\partial V}{\partial x_1}, \frac{\partial V}{\partial x_2}, \cdots, \frac{\partial V}{\partial x_n})$, and $V_{xx} = (\frac{\partial^2 V}{\partial x_i \partial x_j})_{n \times n}$ [7].

Definition 1 ([33])**.** The trivial solution to system (1) is stable in probability, if for each $\epsilon > 0$, $\eta > 0$, there exists $\delta = \delta(t_0, \epsilon, \eta) > 0$ such that $E(|x_0|) < \delta$ implies $P\{|x(t, t_0, x_0)| \geq \epsilon\} < \eta$ for $t \geq t_0$. Furthermore, the trivial solution is asymptotically stable in probability, if it is stable in probability and for each $\epsilon > 0$, $\eta > 0$, there exist $\delta_0 > 0$ and $T = T(t_0, \epsilon, \eta) > 0$ such that $E(|x_0|) < \delta_0$ implies $P\{|x(t, t_0, x_0)| \geq \epsilon\} < \eta$ for $t \geq t_0 + T$.

Definition 2. The trivial solution to system (1) is unstable in probability, if it is not stable in probability.

Definition 3. The trivial solution to system (1) is asymptotically unstable in probability, if for arbitrary $\delta > 0$ and $T > 0$, there exist $\epsilon > 0$ and $\eta > 0$ and some $\hat{t} \geq t_0 + T$ such that $E(|x_0|) < \delta$ implies $P\{|x(\hat{t}, t_0, x_0)| \geq \epsilon\} > \eta$.

4

Before investigating instability of ISSs, we propose a novel comparison principle of an impulsive system and a continuous system and give a lemma to determine the existence of the continuous comparison system. Define a destabilizing impulsive filter by $\rho_d(s) = \ln(\max\{s, 1\})$ and a stabilizing impulsive filter by $\rho_s(s) = \ln(\min\{s, 1\})$ for $s > 0$. First, let us consider the following impulsive system and continuous system

$$
\mathcal{S}_1: \begin{cases} D_- m(t) \geq \mu(t)m(t), \ t \in (t_{k-1}, t_k], \\ m(t_k^+) \geq q_k m(t_k), \ k \in \mathbb{N}, \\ m(t_0) = m_0 \in \mathbb{R}^+, \end{cases} \tag{3}
$$

$$
\mathcal{S}_2: \begin{cases} \dot{r}(t) = \lambda(t)r(t), \ t \geq t_0, \\ r(t_0) = r_0 \in (0, m_0], \end{cases} \tag{4}
$$

where $m \in PC^*$, $r, \mu, \lambda \in C(\mathbb{R}^+, \mathbb{R})$ and $\{q_k\}_{k \in \mathbb{N}}$ are some positive constants.

Lemma 1. *Suppose that the following conditions are satisfied*

$$
\rho_d(q_k) + \int_{t_k}^{t} \mu(s)ds \geq \int_{t_k}^{t} \lambda(s)ds, \tag{5}
$$

$$
\rho_d(q_k) + \rho_s(q_{k+1}) + \int_{t_k}^{t_{k+1}} \mu(s)ds \geq \int_{t_k}^{t_{k+1}} \lambda(s)ds, \tag{6}
$$

for $t \in (t_k, t_{k+1}]$ and $k + 1 \in \mathbb{N}$ where $q_0 = 1$. Then, $m(t) \geq r(t)$ for $t \geq t_0$.

Proof. First, we will show that $m(t) \geq r(t)$ for $t \in [t_0, t_1]$. If it is not true, there exists $t^* \in (t_0, t_1]$ such that $m(t^*) < r(t^*)$. However, it follows from $m(t) > 0$ and $D_- m(t) \geq \mu(t)m(t)$ for $t \in (t_0, t_1]$ that $m(t^*) \geq m_0 \exp\left(\int_{t_0}^{t^*} \mu(s)ds\right)$. For $r(t)$, the positivity of initial condition ensures that $r(t) \geq 0$ for $t \geq t_0$ under the continuity of λ. Similarly, we have $r(t^*) \leq r_0 \exp\left(\int_{t_0}^{t^*} \lambda(s)ds\right)$. Therefore, $\int_{t_0}^{t^*} \mu(s)ds < \int_{t_0}^{t^*} \lambda(s)ds$. which contradicts (5) under the fact that $\rho_d(q_0) = 0$. Thus, $m(t) \geq r(t)$ for $t \in [t_0, t_1]$. Noticing that $m(t_1^+) < m(t_1)$ for $0 < q_1 < 1$, we shall prove that $m(t_1^+) \geq r(t_1)$ when $0 < q_1 < 1$. Along the same line as the proof for the case of $(t_0, t_1]$, the contrary of $m(t_1^+) \geq r(t_1)$ results in that

$$
\ln q_1 + \int_{t_0}^{t_1} \mu(s)ds < \int_{t_0}^{t_1} \lambda(s)ds, \tag{7}
$$

which also contradicts (6) under the fact that $\rho_s(q_1) = \ln q_1$ for $0 < q_1 < 1$.

Then, we can derive that $m(t) \geq r(t)$ for $t \in (t_k, t_{k+1}]$ and $m(t_{k+1}^+) \geq r(t_{k+1})$ for $0 < q_{k+1} < 1$, provided that $m(t) \geq r(t)$ for $t \in (t_{k-1}, t_k]$ and $m(t_k^+) \geq r(t_k)$ for $0 < q_k < 1$, $k \in \mathbb{N}$. Suppose that there exists $t^* \in (t_k, t_{k+1}]$ such that $m(t^*) < r(t^*)$, one can derive that

$$m(t^*) \geq \begin{cases} m(t_k^+) \exp(\int_{t_k}^{t^*} \mu(s)ds), & \text{if } 0 < q_k < 1, \\ q_k m(t_k) \exp(\int_{t_k}^{t^*} \mu(s)ds), & \text{if } q_k \geq 1, \end{cases} \tag{8}$$

and

$$r(t^*) \leq r(t_k) \exp \left(\int_{t_k}^{t^*} \lambda(s)ds \right), \tag{9}$$

which lead to

$$\rho_d(q_k) + \int_{t_k}^{t^*} \mu(s)ds < \int_{t_k}^{t^*} \lambda(s)ds. \tag{10}$$

This contradicts (5) as well. The deduction process of $m(t_{k+1}^+) \leq r(t_{k+1})$ for $0 < q_{k+1} < 1$ is the same fashion and consequently omitted. By mathematical induction, the proof of this lemma is completed. $\square$

Lemma 2. *There exists a function $\lambda \in C(\mathbb{R}^+, \mathbb{R})$ such that conditions (5)-(6) are satisfied and the solution to impulsive system $\mathcal{S}_1$ satisfies that $m(t) \geq r_0 \exp \left(\int_{t_0}^{t} \lambda(s)ds \right)$ for $t \geq t_0$, where r_0 is a positive constant related to m_0.*

Proof. Define the additional functions $\{\sigma_k(t)\}_{k=0}^{\infty}$ by

$$\sigma_k(t) = \begin{cases} \beta_k \sin(\frac{t - t_k}{h_k}\pi), & t \in (t_k, t_k + h_k], \\ 0, & t \in [t_0, t_k] \cup (t_k + h_k, +\infty), \end{cases} \tag{11}$$

where $\beta_k = \frac{\pi(\rho_d(q_k) + \rho_s(q_{k+1}))}{2h_k}$, $q_0 = 1$, and $0 < h_k \leq t_{k+1} - t_k$. Then, we can deduce that conditions (5)-(6) are satisfied with $\lambda(t) = \mu(t) + \sum_{k=0}^{\infty} \sigma_k(t)$. When $t \in (t_k, t_k + h_k)$, $k + 1 \in \mathbb{N}$,

$$\begin{aligned} \int_{t_k}^{t} \lambda(s)ds &= \int_{t_k}^{t} \sigma_k(s)ds + \int_{t_k}^{t} \mu(s)ds \\ &\leq \frac{\pi\rho_d(q_k)}{2h_k} \int_{t_k}^{t_k + h_k} \sin(\frac{s - t_k}{h_k}\pi)ds + \int_{t_k}^{t} \mu(s)ds \\ &= \rho_d(q_k) + \int_{t_k}^{t} \mu(s)ds. \end{aligned} \tag{12}$$

6

When $t \in [t_k + h_k, t_{k+1}]$, $k + 1 \in \mathbb{N}$,

$$
\begin{aligned}
\int_{t_k}^{t} \lambda(s)ds &= \int_{t_k}^{t_k+h_k} \sigma_k(s)ds + \int_{t_k}^{t} \mu(s)ds \\
&= \beta_k \int_{t_k}^{t_k+h_k} \sin(\frac{s-t_k}{h_k}\pi)ds + \int_{t_k}^{t} \mu(s)ds \qquad (13) \\
&= \rho_d(q_k) + \rho_s(q_{k+1}) + \int_{t_k}^{t} \mu(s)ds.
\end{aligned}
$$

Therefore, conditions (5)-(6) are satisfied with $\lambda(t) = \mu(t) + \sum_{k=0}^{\infty} \sigma_k(t)$ and the continuous comparison system $\mathcal{S}_2$ are also determined. Since the solution to $\mathcal{S}_2$ is $r(t) = r_0 \exp\left(\int_{t_0}^{t} \lambda(s)ds\right)$, the conclusion is proved by Lemma 1. $\qquad \square$

Remark 1. Lemma 2 determines the existence of $\lambda(t)$ satisfying conditions (5)-(6), which also guarantees the existence of continuous comparison system $\mathcal{S}_2$. When considering impulsive system $\mathcal{S}_1$, we can build up the continuous comparison system $\mathcal{S}_2$ by setting $\lambda(t) = \mu(t) + \sum_{k=0}^{\infty} \sigma_k(t)$ where the functions $\{\sigma_k(t)\}_{k=0}^{\infty}$ are defined by (11). Then, the comparison principle of system $\mathcal{S}_1$ and system $\mathcal{S}_2$ are established with functions $\mu(t)$ and $\lambda(t)$ satisfying conditions (5)-(6) and the instability of system $\mathcal{S}_1$ can be determined if system $\mathcal{S}_2$ is unstable.

Remark 2. Noted that, when $\mu(t) > 0$, the condition $D_- m(t) \geq \mu(t)m(t)$ implies the exponential divergence of system $\mathcal{S}_1$ without impulses. When the impulses are imported into system $\mathcal{S}_1$, that is $m(t_k^+) \geq q_k m(t_k)$, the system may be divergent or convergent. The conditions (5)-(6) of Lemma 1 retain the divergence of $m(t)$, which will lead to instability of ISSs in later section.

Remark 3. The functions ρ_d and ρ_s are the destabilizing and stabilizing impulsive filters, e.g. $\rho_d(q) = q$ for $q > 1$ and $\rho_d(q) = 0$ for $0 < q < 1$. With the help of these filters, the comparison results can handle both destabilizing and stabilizing impulses, so we extend Ref. [20] to a more general case.

3. Instability Analysis of ISSs

In this section, sufficient conditions for instability in probability of ISSs (1) are derived by stochastic analysis based on the new comparison principle.

Theorem 1. *Assume that there exist functions* $V \in \mathcal{C}^{1,2}(\mathbb{R}^+ \times \mathbb{R}^n, \mathbb{R}^+)$, $c_1 \in \mathcal{K}_1$, $c_2 \in \mathcal{K}_2$ *and* $\mu, \lambda \in C(\mathbb{R}^+, \mathbb{R})$ *such that conditions* (5)-(6) *are satisfied and*

(i) $c_1(|x|) \leq V(t,x) \leq c_2(|x|)$ *for* $(t,x) \in [t_0, \infty) \times \mathbb{R}^n$;

(ii) $\mathcal{L}V(t,x) \geq \mu(t)V(t,x)$, $t \geq t_0$, $t \neq t_k$;

(iii) $V(t_k, I_k(t_k, x(t_k))) \geq q_k V(t_k, x(t_k))$, $k \in \mathbb{N}$.

Then, the instability of system $\mathcal{S}_2$ *implies the instability in probability of the trivial solution to system* (1).

Proof. Given $x_0 \in \mathbb{R}^n \setminus \{0\}$, we denote $V(t) = V(t, x(t))$. By the generalizing Itô formula [7], it yeilds

$$dV(t) = \mathcal{L}V(t, x(t))dt + V_x(t, x(t))g(t, x(t))dw(t), \tag{14}$$

where $t \in (t_{k-1}, t_k]$, $k \in \mathbb{N}$. Then, integrating from t to $t + \Delta t$ with sufficiently absolutely small $\Delta t < 0$ such that $t + \Delta t \in (t_{k-1}, t_k]$ and taking the expectation, we have

$$EV(t + \Delta t) - EV(t) = \int_t^{t+\Delta t} E\mathcal{L}V(s, x(s))ds. \tag{15}$$

Based on the continuity of V, f and g with respect to t, we have $D_- EV(t) = E\mathcal{L}V(t, x(t))$. From Lemma 1, we obtain that $EV(t) \geq r(t)$ for $t \in [t_0, t_1] \cup (t_k, t_{k+1}]$, $k \in \mathbb{N}$. Suppose that the trivial solution to system (1) is stable in probability. Define $\Omega_n(t) = \{\omega \in \Omega : |x(t)| \geq n\}$ and $\Omega_n(t) \setminus \Omega_{n+1}(t) = \{\omega \in \Omega : n \leq |x(t)| < n+1\}$ where $n = 0, 1, 2, \cdots$. Since the trivial solution to system (1) is stable in probability, for $\epsilon_2 = n > 0$ and $\eta = \frac{a}{(n+1)^3}$ where $a > 0$ will be determined later, there exists $\delta_2 > 0$ such that $E(|x_0|) < \delta_2$ implies $P(|x(t, t_0, x_0)| \geq n) = P(\Omega_n(t)) < \frac{a}{(n+1)^3}$. Since system $\mathcal{S}_2$ is unstable, for $\delta_1 = c_1(\delta_2) > 0$, there exist $\epsilon_1 > 0$, $r_0 < \delta_1$ and some $\hat{t} > t_0$ such that $E|x_0| < \delta_2$ for those x_0 with $EV(t_0, x_0) \leq r_0 < \delta_1$ and $EV(\hat{t}, x(\hat{t}, t_0, x_0)) \geq r(\hat{t}, r_0) \geq \epsilon_1$. However,

$$EV(\hat{t}, x(\hat{t}, t_0, x_0)) \leq c_2(E|x(\hat{t}, t_0, x_0)|) \leq c_2\left(\sum_{n=0}^{\infty}(n+1)P(\Omega_n(\hat{t}) \setminus \Omega_{n+1}(\hat{t}))\right)$$

$$\leq c_2\left(\sum_{n=0}^{\infty}(n+1)P(\Omega_n(\hat{t}))\right) \leq c_2\left(a\sum_{n=0}^{\infty}\frac{1}{(n+1)^2}\right) < c_2(2a) = \epsilon_1, \tag{16}$$

8

where $a = c_2^{-1}(\epsilon_1)/2$, which is contradiction. Therefore, the trivial solution to system (1) is unstable in probability if system $\mathcal{S}_2$ is unstable. $\square$

Remark 4. As we all know, the stability in mean of stochastic systems implies the stability in probability by Chebyshev's theorem. Conversely, the instability in probability of ISSs (1) implies the instability in mean.

Based on Theorem 1 and Lemma 2 which determines the continuous comparison system $\mathcal{S}_2$ with $\lambda(t) = \mu(t) + \sum\limits_{k=0}^{\infty} \sigma_k(t)$, the following moment estimate and corollaries are immediate consequences.

Theorem 2. *If there exist functions $V \in \mathcal{C}^{1,2}(\mathbb{R}^+ \times \mathbb{R}^n, \mathbb{R}^+)$, $c_1 \in \mathcal{K}_1$, $c_2 \in \mathcal{K}_2$ and $\mu \in C(\mathbb{R}^+, \mathbb{R})$ such that conditions (i)-(iii) in Theorem 1 hold, the solution $x(t)$ to system (1) satisfies the following moment estimate*

$$EV(t, x(t)) \geq K_0 \exp\Big(\int_{t_0}^{t} \mu(s)ds\Big) \prod_{i=1}^{k-1} q_i \min_{i=k,k+1}\{1, q_i\}, \qquad (17)$$

for $t \in (t_k, t_{k+1}]$, $k \in \mathbb{N}$, where K_0 is a constant related to the initial condition.

Proof. From Lemma 2 and Theorem 1, we have $EV(t, x(t)) \geq K_0 \exp\Big(\int_{t_0}^{t} \lambda(s)ds\Big)$ for $t \geq t_0$, where $K_0 = c_1(E|x_0|)/2$, $\lambda(t) = \mu(t) + \sum\limits_{k=0}^{\infty} \sigma_k(t)$ and the functions $\{\sigma_k(t)\}_{k=0}^{\infty}$ are defined by (11). When $t \in (t_k, t_{k+1})$, $k \in \mathbb{N}$, we get

$$EV(t, x(t)) \geq K_0 \exp\Big(\int_{t_0}^{t} \mu(s)ds + \sum_{i=1}^{k} \int_{t_{i-1}}^{t_i} \sigma_i(s)ds + \int_{t_k}^{t} \sigma_k(s)ds\Big)$$

$$\geq K_0 \exp\Big(\int_{t_0}^{t} \mu(s)ds + \frac{\pi \rho_s(q_{k+1})}{2h_k} \int_{t_k}^{t} \sin(\frac{s - t_k}{h_k}\pi)ds\Big) \prod_{i=1}^{k-1} q_i \min_{i=k}\{1, q_i\}$$

$$\geq K_0 \exp\Big(\int_{t_0}^{t} \mu(s)ds\Big) \prod_{i=1}^{k-1} q_i \min_{i=k,k+1}\{1, q_i\}. \qquad (18)$$

When $t = t_k$, $k \in \mathbb{N}$, the moment estimate (17) is obviously true. Then, the proof is completed. $\square$

Corollary 1. Assume that there exist functions $V \in \mathcal{C}^{1,2}(\mathbb{R}^+ \times \mathbb{R}^n, \mathbb{R}^+)$, $c_1 \in \mathcal{K}_1$, $c_2 \in \mathcal{K}_2$ and $\mu \in C(\mathbb{R}^+, \mathbb{R})$ such that conditions (i)-(iii) hold. Then, the

9

trivial solution to system (1) is unstable in probability if there exists a constant M such that

$$\int_{t_0}^{t} \mu(s)ds + \sum_{i=1}^{k} \ln q_i \geq M, \ t \in (t_k, t_{k+1}], \ k \in \mathbb{N}.$$

Proof. There exists $M > 0$ such that $\int_{t_0}^{t} \mu(s)ds + \sum_{i=1}^{k} \ln q_i \geq M$ for $t \in (t_k, t_{k+1}]$ and $k \in \mathbb{N}$, so there exists $\hat{t} \in (t_k, t_{k+1})$ such that $EV(\hat{t}, x(\hat{t})) \geq M'_k$ where $M'_k = K_0 \min_{i=k,k+1}\{1, q_i\}e^{M-\ln q_k}$. Then, it follows from Theorem 2 that $c_2(E|x(\hat{t})|) \geq M'_k$, indicating that $E|x(\hat{t})| \geq c_2^{-1}(M'_k)$. Suppose that system (1) is stable in probability, then for $\epsilon = n$ and $\eta = \frac{a}{(n+1)^3}$ where $a = c_2^{-1}(M'_k)/2$ and $n \in \mathbb{N}$, there exists $\delta_0 > 0$ such that $E|x_0| \leq \delta_0$ implies $P(|x(t)| \geq n) < \frac{a}{(n+1)^3}$. Analogous to (16), we have

$$E|x(t)| \leq \sum_{n=0}^{\infty}(n+1)P(\Omega_n(t)) \leq \sum_{n=0}^{\infty} \frac{a}{(n+1)^2} < c_2^{-1}(M'_k), \qquad (19)$$

for all $t \geq t_0$, which contradicts $E|x(\hat{t})| \geq c_2^{-1}(M'_k)$. Therefore, the trivial solution to system (1) is unstable in probability. $\qquad\square$

Corollary 2. Assume that there exist functions $V \in \mathcal{C}^{1,2}(\mathbb{R}^+ \times \mathbb{R}^n, \mathbb{R}^+)$, $c_1 \in \mathcal{K}_1$, $c_2 \in \mathcal{K}_2$ and $\mu \in C(\mathbb{R}^+, \mathbb{R})$ such that conditions (i)-(iii) hold. Then, the trivial solution to system (1) is asymptotically unstable in probability if there exists a function $\phi \in \mathcal{K}_\infty$ such that

$$\int_{t_0}^{t} \mu(s)ds + \sum_{i=1}^{k} \ln q_i \geq \ln \phi(t - t_0), \ t \in (t_k, t_{k+1}], \ k \in \mathbb{N}.$$

Proof. Suppose that the trivial solution to system (1) is not asymptotically unstable in probability. Then, for arbitrary $\epsilon = n$ and $\eta = \frac{1}{(n+1)^3}$, there exist $\delta_0 > 0$ and $T > 0$ such that $E|x_0| < \delta_0$ implies $P(|x(t)| \geq n) < \frac{1}{(n+1)^3}$ for $t \geq t_0 + T$, which indicates that $E|x(t)| < 2$ for $t \geq t_0 + T$ along the same line of (16). However, since $\phi \in \mathcal{K}_\infty$, there exists $\hat{t} \geq t_0 + T$ such that $|\phi(\hat{t})| > e^M$ for arbitrary $M \in \mathbb{R}$, furthermore, $\int_{t_0}^{t} \mu(s)ds + \sum_{i=1}^{k} \ln q_i > M$. Analogous to the proof of Corollary 1, we can choose M large enough so that $E|x(\hat{t})| \geq 2$ which leads to contradiction. Then, the proof is completed. $\qquad\square$

10

Corollary 3. Assume that there exist a constant ν, and a function $\mu \in C(\mathbb{R}^+, \mathbb{R}^+)$ such that

$$2x^T(t)f(t, x(t)) + |g(t, x(t))|^2 \geq \mu(t)|x(t)|^2, \ t \geq t_0, \tag{20}$$

$$|I_k(t_k, x(t_k))|^2 \geq e^\nu |x(t_k)|^2, \ k \in \mathbb{N}. \tag{21}$$

If there exists a constant M such that $\nu N(t, s) + \int_s^t \mu(s)ds \geq M$ for $t_0 \leq s < t$, system (1) is unstable in probability; If there exists a function $\phi \in \mathcal{K}_\infty$ such that $\nu N(t, s) + \int_s^t \mu(s)ds \geq \ln \phi(t - s)$ for $t_0 \leq s < t$, system (1) is asymptotically unstable in probability.

Proof. Define a Lyapunov function by $V(t, x) = p|x(t)|^2$ with $p > 0$. From the conditions of this corollary, we see that

$$\mathcal{L}V(t, x(t)) = 2px^T(t)f(t, x(t)) + p|g(t, x(t))|^2 \geq \mu(t)V(t, x(t)), \tag{22}$$

$$V(t_k, I_k(t_k, x(t_k))) = p|I_k(t_k, x(t_k))|^2 \geq pe^\nu |x(t_k)|^2 = e^\nu V(t_k, x(t_k)). \tag{23}$$

Thus, all the conditions of Corollary 1 and 2 are satisfied to complete the proof.

$\square$

Remark 5. Noted that the existing studies [21, 34, 35] have given the stability conditions of ISSs. For instance, it follows from Theorem 1 of [35] that the ISSs are asymptotically stable in probability if the reverse of (20)-(21) and $\nu N(t, s) + \int_s^t \mu(s)ds \leq -\ln \phi(t-s)$ hold for $t_0 \leq s < t$ and $\nu < 0$. If the sufficient stability conditions are not satisfied, the ISSs may be stable or unstable. At this time, if the conditions of Corollary 3 are satisfied, we can claim the instability of the system. Therefore, the obtained results present how to determine instability when stability conditions fails. It is quite a pity that the derived instability conditions and the existing stability conditions cannot be transformed because of the sufficiency of these conditions, and it is interesting to establish sufficient and necessary conditions to bridge instability and stability, which will be the future work.

Remark 6. Although Ref. [20] has studied the instability of impulsive differential systems with stabilizing impulses, the generalization is far from being

11

trivial because the system considered here includes stochastic factor and the results are suitable for both the stabilizing and destabilizing impulses.

Remark 7. It is interesting to note that, if we establish upper comparison system along the same fashion of Lemma 1 and derive stability conditions of ISSs, the conclusion agrees with the results in [34, 35] (see Appendix for details).

4. Applications

To show the effectiveness of theoretical results, we give two numerical examples and apply the signals generated by ISSs to image encryption.

4.1. Numerical Examples

Example 1. Consider the following scalar stochastic system

$$dx(t) = a(t)x(t)dt + b(t)x(t)dw(t), \ t \geq 5, \tag{24}$$

where $a(t) = -1 + \frac{\cos(t)}{t} - \frac{1+\sin(t)}{t^2}$ and $b(t) = \frac{\sqrt{2}}{t}$. Fig. 1(a) depicts the stable stochastic continuous dynamics with initial conditions $x_0 = -5, -4, \cdots, 5$. Then, the impulse $x(t_k^+) = ex(t_k)$ $(t_k = k, \ k \in \mathbb{N})$ is imposed into the system.

Claim 1. The trivial solution to system (24) with the above impulse is unstable in probability, as shown in Fig. 1(b).

Proof. Denote the solution of system (24) with impulse by $x(t)$, a simple computation yields

$$2x(t)f(t, x(t)) + |g(t, x(t))|^2 = 2(-1 + \frac{\cos(t)}{t} - \frac{\sin(t)}{t^2})x^2(t), \tag{25}$$

which results in $\mu(t) = 2(-1 + \frac{\cos(t)}{t} - \frac{\sin(t)}{t^2})$ and $v = 2$. From Corollary 3, there exists $M = -\frac{14}{5}$ such that $\nu N(t, s) + \int_s^t \mu(s)ds \geq 2(-1 + \frac{\sin(t)}{t} - \frac{\sin(s)}{s}) \geq M$ for $5 \leq s < t$, indicating the instability in probability. $\square$

Remark 8. In the literatures [36, 37], the stochastic noise was shown to destabilize a stable system. As the example suggests, the impulse can also destabilize a stable stochastic system.
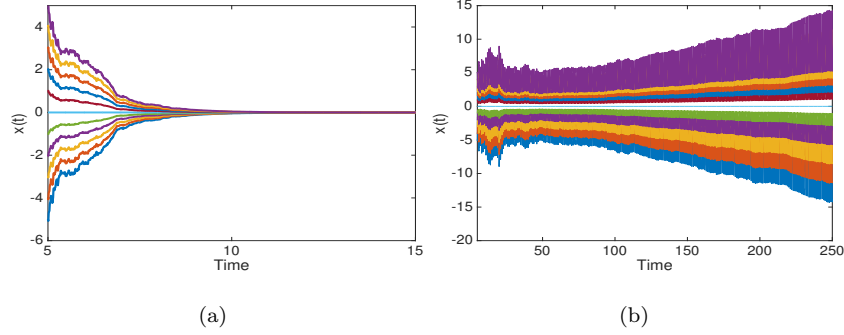
Figure 1: Trajectory simulation of system (24) without impulse (a) and with impulse (b) in Example 1.

Example 2. Consider the following 2-D impulsive stochastic system

$$
\begin{cases}
dx(t) = Ax(t)dt + Dx(t)dw(t), & t \geq 0, \ t \neq t_k, \\
x(t_k^+) = Jx(t_k), & t_k = k, \ k \in \mathbb{N},
\end{cases}
\tag{26}
$$

where $x(t) = [x_1(t), x_2(t)]^T$.

Claim 2. The trivial solution to system (26) is asymptotically unstable in probability, if there exist constants $\mu, \alpha > 0$ and matrix $P > 0$ such that $\alpha > e^{-\mu}$,

$$
PA + A^T P + D^T PD - \mu P \geq 0, \ J^T PJ - \alpha P \geq 0.
\tag{27}
$$

Proof. Since $\alpha > e^{-\mu}$, there exists $a > 0$ such that $\mu > a - \ln \alpha$. If we consider the Lyapunov function defined by $V(t, x) = x^T Px$, the Itô operator, associated with system (26), is given by

$$
\mathcal{L}V(t, x) = x^T PAx + x^T A^T Px + \mathrm{tr}(x^T D^T PDx).
\tag{28}
$$

When $t \neq t_k$, we have that $\mathcal{L}V(t, x) \geq \mu V(t, x)$. When $t = t_k$, $V(t_k^+, x(t_k^+)) = x^T J^T PJx \geq \alpha V(t_k, x(t_k))$. Then, there exist $\mu(t) = \mu$, $q_k = \alpha$ and $\phi(t) = e^{at}$ such that $\int_0^t \mu(s)ds + \sum_{i=1}^{k} \ln q_i \geq (a - \ln \alpha)t + k \ln \alpha \geq at = \ln \phi(t)$, so the trivial solution to system (26) is asymptotically unstable in probability based on Corollary 2. $\square$

13

Remark 9. As Refs. [11, 21] stated, the impulse controller is effective to stabilize an unstable system. From this example, we see that the stability of the system with impulsive controller cannot be ascertained if the stabilizing impulse is not visited frequently enough.

4.2. Application to Image Encryption

From theoretical results and numerical examples, we obtain the conditions for instability and asymptotic instability in probability. The instability in probability implies that ISSs are unstable for a large set of initial conditions, which ensures that the initial condition can be used as encryption key for image encryption. The asymptotic instability in probability implies that the signals generated by system (26) fall into unstable orbit or even chaotic orbit in almost every simulation, which implies that the unstable ISSs may generate unpredictable numerical signals. To generate signals for encryption, system (26) is numerically discretized by the method in [38] to be expressed by

$$
\begin{cases}
x(n+1) = x(n) + Ax(n)\Delta t + Dx(n)\Delta w^n, & n \neq n', \\
x(n+1) = Jx(n), & n = n',
\end{cases} \tag{29}
$$

where $n = 1, 2, \cdots$, $n' = 1 \times 10^4, 2 \times 10^4, \cdots$, $\Delta t = 10^{-4}$, and $\{\Delta w^n\}$ are the simulated values of independent random variables of the form $\sqrt{\Delta t}N(0,1)$. The parameters are chosen by

$$
A = \begin{bmatrix} 3 & 1 \\ 0 & 1 \end{bmatrix}, \ D = \begin{bmatrix} 1.8 & 0.12 \\ -1.2 & 0.6 \end{bmatrix}, \ J = \begin{bmatrix} 0.096 & 0 \\ 0 & 0.096 \end{bmatrix}.
$$

Obviously, the conditions in Claim 2 are satisfied with $\mu = 2.3449$, $\alpha = 0.096$ and $P = I$, so system (26) is asymptotically unstable in probability. From Fig. 2, we can see that the system indeed generates unstable chaotic signals. Then, the chaotic signals are used to cipher plain images by an image cryptosystem which includes bit-level permutation inspired by [28] and pixel-level diffusion as follows:

Bit-Level Permutation. First, the plain image $(M \times N \times K)$ is divided into $KM \times 8N$ groups by bits and columns where each group has KM bits and the
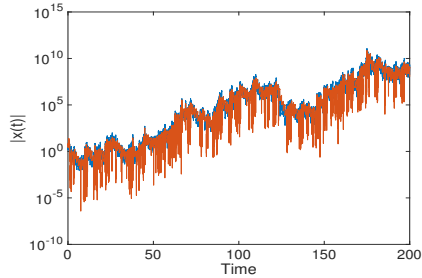
14

Figure 2: Trajectory simulation of system (26) in Example 2.

chaotic signals are processed by $x = \text{floor}(|\text{signal}[H : H + MNK]|)$ where H is used to discard former H values. Then, the bit groups are permuted by the processed signals and Arnold cat map defined by

$$
\begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} i \\ i \end{bmatrix} \text{mod} \begin{bmatrix} 8N \\ 8N \end{bmatrix}, \tag{30}
$$

where $p = x[i]$, $q = x[\text{end} - i]$, i represents the original bit group index, m represents the new bit group index after permutation, and n is the circle shift number of m bit group. Further, the bit groups are combined to generate a permuted image.

Pixel-Level Diffusion. For pixel-level diffusion, the steps are as follows:

Step 1: the pixels in permuted image are scanned from upper-left to lower-right and form a permuted sequence p.

Step 2: set the initial value of ciphered sequence by $c[1] = C \sum_{i=1}^{MNK} p[i]$ where C is a positive constant.

Step 3: each pixel in ciphered sequence c is calculated by

$$
c[i + 1] = \{p[i] + c[i] + x[i]\text{mod}256\}\text{mod}256.
$$

where $i = 1, 2, \cdots, MNK$.

Step 4: the ciphered sequence is reshaped to be a ciphered image.

The decryption procedures are the reverse scenario of encryption. For color image $(K = 3)$, 24 bits in pixels are extracted from red, green and blue components to generate $3M \times 8N$ bit groups for permutation and the permuted

15

image is reshaped to form the permuted sequence of size $3MN$ for diffusion. Through this procedures, the pixels of color images can move from one component to another component. Therefore, the encryption scheme for color images are inter-component encryption instead of intra-component encryption.

Remark 10. Even though the stochastic factor exists in system (26), the corresponding discretized system (29) for encryption and decryption is self-synchronized because the simulated value of stochastic factor is pre-generated, deterministic, and open to public.

4.3. Experimental Results

To testify the workable cryptosystem, we perform experiments on several standard images and USC-SIPI database [39] (e.g. Fig. 3) including key analysis, statistical analysis and differential analysis as follows.

Figure 3: Some representative images from USC-SIPI database [39].

Key analysis. The parameters A, D, J and the initial condition $x(0)$ of ISSs are choosen as secret keys. To test the key sensitivity, the original images are ciphered to form ciphered images, which are further decrypted by secret keys and several wrong keys slight different from secret keys. The decrypted results and their histograms are shown in Figs. 4 and 5 where the decrypted image by secret keys is identical with the original image while all the decryption attempts by wrong keys fail, indicating that the encryption algorithm is sensitive to secret keys.

16
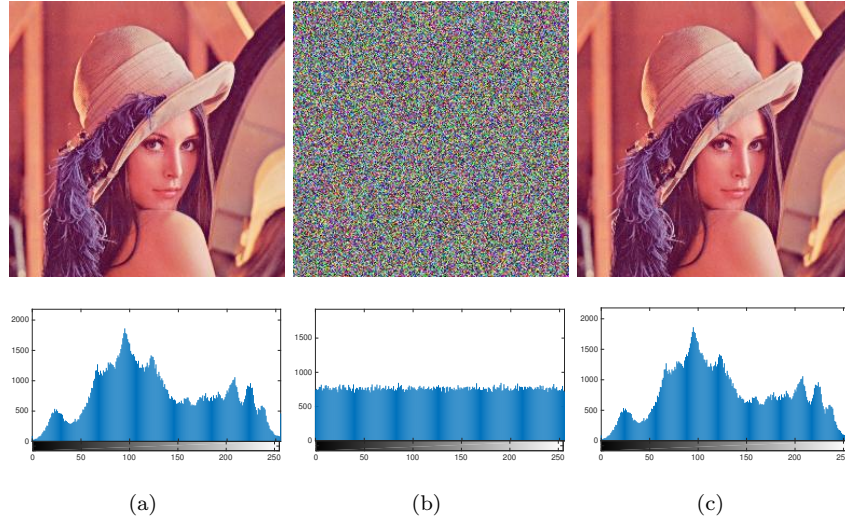
Figure 4: Images and their corresponding histograms. (a) Plain image. (b) Ciphered image. (c) Decrypted image by using secret keys.
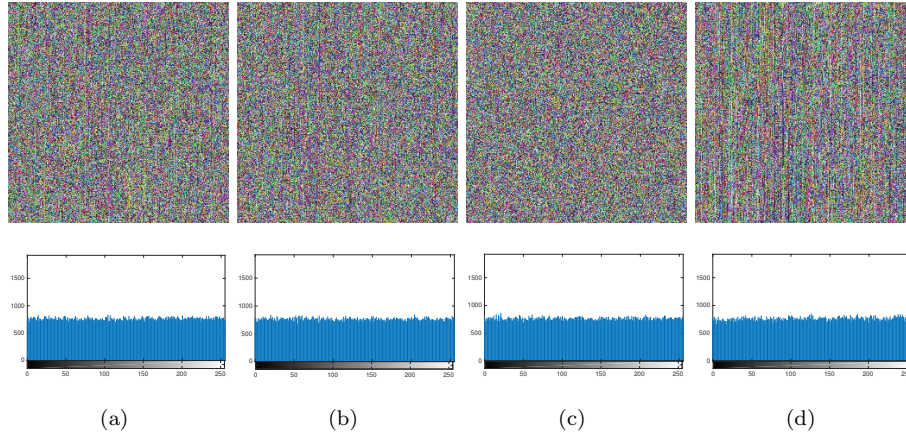
Figure 5: Decrypted images by using wrong keys where $\tilde{A} = A$, $\tilde{D} = D$, $\tilde{J} = J$, $\tilde{x}(0) = x(0)$ except (a) $\tilde{A}_{11} = A_{11} + 10^{-6}$; (b) $\tilde{D}_{11} = D_{11} + 10^{-6}$; (c) $\tilde{J}_{11} = J_{11} + 10^{-6}$; (d) $\tilde{x}_1(0) = x_1(0) + 10^{-6}$.

₂₂₀ **Statistical analysis.** To demonstrate the resistance to attacks, statistical properties of plain images and ciphered images are analyzed including histogram, entropy, and correlation of plain images and ciphered images. If the

17

Table 1: Variances of Histograms Compared with Ref. [40].

Image	Lena (g)	Pepper	Lady	Clock
Original	6.37e5	3.31e6	9.09e5	2.40e4
Ciphered	9.22e2	2.69e3	7.52e2	6.17e1
Ref. [32]	1.04e3	3.41e3	8.77e2	5.60e1

plain images are ciphered by a good encryption scheme, the variances of histograms ought to decrease significantly, as shown in Table 1 for the test images
[225] compared with Ref. [40]. Moreover, the entropies of ciphered images are also calculated and presented in Table 2 and 3 compared with Refs. [30, 31, 40]. The closeness of entropy to 8 implies the random-like appearance of ciphered images and the proposed method achieves almost the best entropy and variances of histograms.

Table 2: Entropy compared with Refs. [30, 31].

Algorithm	Image	Red	Green	Blue	Image	Red	Green	Blue
Proposed		7.9993	7.9992	7.9994		7.9993	7.9993	7.9993
Ref. [30]	Baboon	7.9982	7.9984	7.9980	House	7.9983	7.9979	7.9980
Ref. [31]		7.9992	7.9993	7.9991		7.9966	7.9972	7.9967
Proposed	F-16	7.9993	7.9993	7.9993	Lake	7.9993	7.9994	7.9994
Ref. [30]		7.9980	7.9980	7.9978		7.9978	7.9976	7.9978
Proposed	Lena	7.9976	7.9970	7.9972	Tiffany	7.9993	7.9992	7.9993
Ref. [30]		7.9978	7.9976	7.9979		7.9977	7.9979	7.9978
Proposed	Tree	7.9971	7.9968	7.9972	Splash	7.9993	7.9994	7.9993
Ref. [31]		7.9972	7.9969	7.9968		7.9993	7.9991	7.9988
Proposed	Peppers	7.9993	7.9993	7.9993	Lady	7.9968	7.9973	7.9973
Ref. [31]		7.9992	7.9993	7.9992		7.9971	7.9972	7.9965

[230] The correlations of adjacent pixels of plain images and ciphered images are also evaluated in horizontal, vertical and diagonal directions, because an ideal encryption algorithm can remove the high relation of adjacent pixels of plain

Table 3: Entropy compared with Ref. [40].

Algorithm	Lena (g)	Pepper	Lady	Clock
Proposed	7.9994	7.9998	7.9991	7.9891
Ref. [32]	7.9993	7.9993	7.9971	7.9901

images. As shown in Fig. 6, the pixels in plain images diffuse uniformly to form the ciphered image. The quantification of correlations on USC-SIPI database is
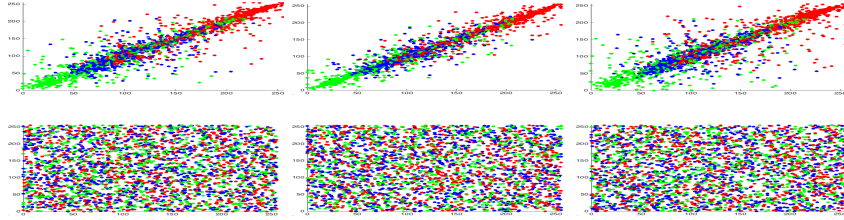

Figure 6: Correlation plots of plain image (top) and ciphered image (bottom) in horizontal direction (left), vertical direction (mid), and diagonal direction (right).

presented in Table 4 where the correlations of color images are absolute averages of three directions and RGB components. The absolute average correlation of six images from USC-SIPI database is 2.10e-3 which is smaller than 1.63e-2 of Ref. [30] and the correlation of baboon, house, tree, splash, peppers and lady images is 1.85e-3 which is also smaller than 2.67e-3 of Ref. [31]. Thus, the proposed encryption scheme is robust to chosen-plaintext or known-plaintext attacks.

Differential analysis. To resist the differential attack, the encryption scheme should force the minor change in plain images to diffuse in the whole ciphered images. Generally, the number of pixels change rate (NPCR) and unified average changing intensity (UACI) are employed to test the encryption scheme's resistance to differential attack. The NPCR and UACI are calculated by

$$\text{NPCR} = \frac{\Sigma_{i,j} D(i,j)}{M \times N} \times 100\%, \ \text{UACI} = \frac{\Sigma_{i,j} |c(i,j) - c'(i,j)|}{255 \times M \times N} \times 100\%,$$

where c and c' are two ciphered images, (i,j) represents the coordinate, and

19

Table 4: Correlation performance on USC-SIPI database [39].

Image	Original ($\times 10^{-1}$)			Ciphered ($\times 10^{-3}$)		
	Red	Green	Blue	Red	Green	Blue
Baboon	8.81	7.89	8.76	2.08	0.70	1.20
F-16	9.55	9.52	9.38	1.10	2.17	2.34
House	9.46	9.23	9.62	1.07	1.43	0.93
Lake	9.51	9.63	9.64	1.94	2.06	0.72
Lena	9.35	9.39	8.80	6.45	2.65	3.61
Tiffany	9.40	8.99	9.01	2.82	2.34	1.89
Average	9.35	9.11	9.20	2.58	1.89	1.78
SIPI-Color	9.49	9.40	9.42	2.74	2.48	2.36
SIPI-Gray	9.21	9.07	8.60	1.56	2.07	1.76

$D(i, j)$ is defined by

$$D(i,j) = \begin{cases} 1, & c(i,j) \neq c'(i,j), \\ 0, & \text{otherwise.} \end{cases}$$

Two plain images differ by one bit at only one position, which are further ciphered by the same keys to calculate NPCR and UACI. The four corners and the centre in images are chosen as the different position separately to calculate the average UPCR and UACI. The results on USC-SIPI database are listed in Table 5 which shows that NPCR and UACI can reach 0.99 and 0.33 after first round, indicating that the proposed scheme has a good ability to resist differential attack. Furthermore, since the proposed scheme is inter-component encryption for color images, we also calculate the inter-NPCR (INPCR) and inter-UACI (IUACI) defined by

$$\text{INPCR} = \frac{\Sigma_{i,j,k} D(i,j,k)}{3 \times M \times N} \times 100\%, \ \text{IUACI} = \frac{\Sigma_{i,j,k} |c(i,j,k) - c'(i,j,k)|}{255 \times 3 \times M \times N} \times 100\%,$$

where c and c' are two ciphered images, (i, j) represents the coordinate, $k =$

Table 5: NPCR and UACI performance on USC-SIPI database [39].

Image	NPCR			UACI		
	Red	Green	Blue	Red	Green	Blue
Baboon	0.9958	0.9940	0.9949	0.3368	0.3346	0.3348
Lena	0.9949	0.9947	0.9939	0.3349	0.3341	0.3341
Lake	0.9959	0.9952	0.9955	0.3350	0.3351	0.3347
SIPI-Color	0.9952	0.9947	0.9946	0.3359	0.3350	0.3343
SIPI-Gray		0.9950			0.3355	

red, blue, or green, and $D(i, j, k)$ is defined by

$$D(i, j, k) = \begin{cases} 1, & c(i, j, k) \neq c'(i, j, k), \\ 0, & \text{otherwise.} \end{cases}$$

The INPCR and IUACI are calculated by changing one bit in one component. As shown in Table 6, INPCR and IUACI also reach 0.99 and 0.33 respectively, which implies the resistance of the proposed scheme to differential attack because the tiny change in one component causes significant change of the whole three components of color images.

Table 6: INPCR and IUACI performance on USC-SIPI database [39].

Image	INPCR			IUACI		
	Red	Green	Blue	Red	Green	Blue
Baboon	0.9952	0.9947	0.9951	0.3353	0.3351	0.3348
Lena	0.9947	0.9945	0.9944	0.3350	0.3338	0.3338
Lake	0.9956	0.9953	0.9953	0.3349	0.3341	0.3345
SIPI-Color	0.9950	0.9947	0.9947	0.3353	0.3348	0.3345

5. Conclusion

This paper investigates instability of ISSs with application to image encryption. First, asymptotic behaviours of an impulsive system and its lower contin-

uous comparison system are studied to build up comparison principle. Based on the novel comparison results, instability in probability of ISSs is established by stochastic analysis. The effectiveness of theoretical results is verified by two numerical examples and the application to image encryption.

In most of literatures about image encryption based on nonlinear systems [29–31], the delays are usually added into models to generate chaotic signals. And, it is more chanllenging to investigate instability properties of impulsive stochastic delayed systems (ISDSs), since the moment estimate of ISDSs is difficult and most of the existing inequalities on stability will be invalid. Therefore, the future work will focus on instability analysis of ISDSs and their application to secure communication.

On the other hand, even though the unstable ISSs are shown to generate chaotic numerical signals suitable for image encryption, there is a gap between the dynamical analysis of ISSs and the application to image encryption, since the discretized ISSs are the practical systems to generate chaotic signals and the chaotic behaviour is the desirable property for image encryption. But the instability properties of ISSs are necessary for chaos analysis, because an ISS must be unstable if it is chaotic. If we try to investigate the chaotic properties of ISSs, more strong conditions are recommended than the established conditions. The chaotic properties of ISSs will be another future work.

Acknowledgement

Appendix: Upper Comparison System

To establish the upper comparison system, the following notations are additionally specified. $PC'(I,T) = \{\phi : I \to T$ is piecewise continuous and $\phi(t^+) = \phi(t)\}$. $PC^{**} = \{\phi \in PC'(\mathbb{R}^+, \mathbb{R}^+) | \phi$ is discontinuous only at points $\{t_k\}_{k=1}^{\infty}\}$. For a function $\phi : \mathbb{R}^+ \to \mathbb{R}^+$, $D^+\phi(t) \triangleq \limsup_{\Delta t \to 0^+} \frac{\phi(t+\Delta t)-\phi(t)}{\Delta t}$ is the upper-right Dini derivative of $\phi(t)$. Along the same line of Section 2, consider the following impulsive system and continuous system

$$
\mathcal{S}_3: \begin{cases} D^+\overline{m}(t) \leq \overline{\mu}(t)\overline{m}(t), \ t \in [t_{k-1}, t_k), \\ \overline{m}(t_k^+) \leq \overline{q}_k \overline{m}(t_k), \ k \in \mathbb{N}, \\ \overline{m}(t_0) = \overline{m}_0 \in \mathbb{R}^+, \end{cases} \tag{31}
$$

$$
\mathcal{S}_4: \begin{cases} \dot{\overline{r}}(t) = \overline{\lambda}(t)\overline{r}, \ t \geq t_0, \\ \overline{r}(t_0) = \overline{r}_0 \in [\overline{m}_0, \infty), \end{cases} \tag{32}
$$

where $\overline{m} \in PC^{**}$, $\overline{r}, \overline{\mu}, \overline{\lambda} \in C(\mathbb{R}^+, \mathbb{R})$ and $\{\overline{q}_k\}_{k \in \mathbb{N}}$ are some positive constants.

Claim 3. Suppose that the following conditions are satisfied

$$
\rho_s(\overline{q}_k) + \int_{t_k}^t \overline{\mu}(s)ds \leq \int_{t_k}^t \overline{\lambda}(s)ds, \tag{33}
$$

$$
\rho_s(\overline{q}_k) + \rho_d(\overline{q}_{k+1}) + \int_{t_k}^{t_{k+1}} \overline{\mu}(s)ds \leq \int_{t_k}^{t_{k+1}} \overline{\lambda}(s)ds, \tag{34}
$$

for $t \in [t_k, t_{k+1})$ and $k+1 \in \mathbb{N}$ where $\overline{q}_0 = 1$. Then, $\overline{m}(t) \geq \overline{r}(t)$ for $t \geq t_0$.

Claim 4. There exists a function $\overline{\lambda} \in C(\mathbb{R}^+, \mathbb{R})$ such that conditions (33)-(34) are satisfied and the solution to impulsive system $\mathcal{S}_3$ satisfies that $\overline{m}(t) \leq \overline{r}_0 \exp\left(\int_{t_0}^t \overline{\lambda}(s)ds\right)$ for $t \geq t_0$ where $\overline{r}_0$ is a positive constant related to $\overline{m}_0$.

Based on the comparison results established here, one can derive stability conditions of ISSs, which will agree with recent studies [34, 35].

References

[1] G. D. Nunno, T. Meyer-Brandis, B. Øksendal, F. Proske, Optimal portfolio for an insider in a market driven by Lévy processes, Quant. Finance 6 (1) (2006) 83–94.

[2] D. Antunes, J. Hespanha, C. Silvestre, Stability of networked control systems with asynchronous renewal links: an impulsive systems approach, Automatica 49 (2) (2013) 402–413.

[3] D. J. Wilkinson, Stochastic modelling for quantitative description of heterogeneous biological systems, Nat. Rev. Genet. 10 (2009) 122–133.

[4] M. Prandini, J. Hu, Application of reachability analysis for stochastic hybrid systems to aircraft conflict prediction, IEEE Trans. Autom. Control 54 (4) (2009) 913–917.

[5] C. L. P. Chen, Y.-J. Liu, G.-X. Wen, Fuzzy neural network-based adaptive control for a class of uncertain nonlinear stochastic systems, IEEE Trans. Cybern. 44 (5) (2013) 583–593.

[6] H. Shen, S. Huo, J. Cao, T. Huang, Generalized state estimation for Markovian coupled networks under round-robin protocol and redundant channels, IEEE Trans. Cybern. 49 (4) (2019) 1292–1301.

[7] X. Mao, Stochastic Differential Equations and Applications, Horwood Publishing, Chichester, UK, 2007.

[8] H. Zhang, Y. Wang, D. Liu, Delay-dependent guaranteed cost control for uncertain stochastic fuzzy systems with multiple time delays, IEEE Trans. Syst., Man, Cybern. B, Cybern., 38 (1) (2008) 126–140.

[9] A. R. Teel, A. Subbaraman, A. Sferlazza, Stability analysis for stochastic hybrid systems: a survey, Automatica 50 (10) (2014) 2435–2456.

[10] W. He, B. Zhang, Q.-L. Han, F. Qian, J. Kurths, J. Cao, Leader-following consensus of nonlinear multiagent systems with stochastic sampling, IEEE Trans. Cybern. 47 (2) (2016) 327–338.

[11] S. Luo, F. Deng, W.-H. Chen, Stability analysis and synthesis for linear impulsive stochastic systems, Int. J. Robust Nonlinear Control 28 (15) (2018) 4424–4437.

24

[12] Y. Shen, Z.-G. Wu, P. Shi, Z. Shu, H. R. Karimi, H_∞ control of Markov jump time-delay systems under asynchronous controller and quantizer, Automatica 99 (2019) 352–360.

[13] T. Huang, C. Li, S. Duan, J. A. Starzyk, Robust exponential stability of uncertain delayed neural networks with stochastic perturbation and impulse effects, IEEE Trans. Neural Netw. Learn. Syst. 23 (6) (2012) 866–875.

[14] X. Li, J. Shen, H. Akca, R. Rakkiyappan, LMI-based stability for singularly perturbed nonlinear impulsive differential systems with delays of small parameter, Appl. Math. Comput. 250 (2015) 798–804.

[15] W.-H. Chen, W. X. Zheng, X. Lu, Impulsive stabilization of a class of singular systems with time-delays, Automatica 83 (2017) 28–36.

[16] W. Ren, J. Xiong, Stability analysis of impulsive stochastic nonlinear systems, IEEE Trans. Autom. Control 62 (9) (2017) 4791–4797.

[17] W. Hu, Q. Zhu, H. R. Karimi, On the pth moment integral input-to-state stability and input-to-state stability criteria for impulsive stochastic functional differential equations, Int. J. Robust Nonlinear Control 29 (16) (2019) 5609–5620.

[18] C. Yi, J. Feng, J. Wang, C. Xu, Y. Zhao, Synchronization of delayed neural networks with hybrid coupling via partial mixed pinning impulsive control, Appl. Math. Comput. 312 (2017) 78–90.

[19] X. Yang, X. Li, Q. Xi, P. Duan, Review of stability and stabilization for impulsive delayed systems, Math. Biosci. Eng. 15 (6) (2018) 1495–1515.

[20] X. Li, W.-H. Chen, W. X. Zheng, Q.-G. Wang, Instability and unboundedness analysis for impulsive differential systems with applications to Lurie control systems, Int. J. Control Autom. Syst. 16 (4) (2018) 1521–1531.

[21] B. Liu, Stability of solutions for stochastic impulsive systems via comparison approach, IEEE Trans. Autom. Control 53 (9) (2008) 2128–2133.

[22] F. Yao, F. Deng, Exponential stability in terms of two measures of impulsive stochastic functional differential systems via comparison principle, Stat. Probab. Lett. 82 (6) (2012) 1151–1159.

[23] M. S. Alwan, X. Liu, W.-C. Xie, Stability properties of nonlinear stochastic impulsive systems with time delay, Stoch. Anal. Appl. 34 (1) (2016) 117–136.

[24] X. Li, J. Shen, H. Akca, R. Rakkiyappan, Comparison principle for impulsive functional differential equations with infinite delays and applications, Commun. Nonlinear Sci. Numer. Simul. 57 (2018) 309–321.

[25] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, Int. J. Bifurcat. Chaos 8 (06) (1998) 1259–1284.

[26] L. Kocarev, Chaos-based cryptography: a brief overview, IEEE Circ. Syst. Mag. 1 (3) (2001) 6–21.

[27] Z.-L. Zhu, W. Zhang, K.-W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, Inf. Sci. 181 (6) (2011) 1171–1186.

[28] Y.-Q. Zhang, X.-Y. Wang, A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice, Inf. Sci. 273 (2014) 329–351.

[29] W.-H. Chen, S. Luo, W. X. Zheng, Impulsive synchronization of reaction–diffusion neural networks with mixed delays and its application to image encryption, IEEE Trans. Neural Netw. Learn. Syst. 27 (12) (2016) 2696–2710.

[30] K. Ratnavelu, M. Kalpana, P. Balasubramaniam, K. Wong, P. Raveendran, Image encryption method based on chaotic fuzzy cellular neural networks, Signal Process. 140 (2017) 87–96.

[31] L. Shanmugam, P. Mani, R. Rajan, Y. H. Joo, Adaptive synchronization of reaction-diffusion neural networks and its application to secure communication, IEEE Trans. Cybern. 50 (3) (2020) 911–922.

26

[32] B. Liu, X. Liu, X. Liao, Existence and uniqueness and stability of solutions for stochastic impulsive systems, J. Syst. Sci. & Complexity 20 (1) (2007) 149–158.

[33] J. Luo, J. Zou, Z. Hou, Comparison principle and stability criteria for stochastic differential delay equations with Markovian switching, Sci. China 46 (1) (2003) 129–138.

[34] D. Xu, B. Li, S. Long, L. Teng, Moment estimate and existence for solutions of stochastic functional differential equations, Nonlinear Anal.: TMA 108 (2014) 128–143.

[35] X. Fu, Q. Zhu, Stability of nonlinear impulsive stochastic systems with Markovian switching under generalized average dwell time condition, Sci. China Inf. Sci. 61 (2018) 112211.

[36] X. Mao, G. G. Yin, C. Yuan, Stabilization and destabilization of hybrid systems of stochastic differential equations, Automatica 43 (2) (2007) 264–273.

[37] X. Zhao, F. Deng, A new type of stability theorem for stochastic systems with application to stochastic stabilization, IEEE Trans. Autom. Control 61 (1) (2016) 240–245.

[38] D. J. Higham, An algorithmic introduction to numerical simulation of stochastic differential equations, SIAM Rev. 43 (3) (2001) 525–546.

[39] The USC-SIPI image database, `http://sipi.usc.edu/database/database.php?volume=misc`, accessed Januarary 11, 2019.

[40] T. Wei, P. Lin, Y. Wang, L. Wang, Stability of stochastic impulsive reaction-diffusion neural networks with S-type distributed delays and its application to image encryption, Neural Netw. 116 (2019) 35–45.