SCIENTIFIC REPORTS

OPEN

A new switching parameter varying optoelectronic delayed feedback model with computer simulation

Lingfeng Liu[1], Suoxia Miao[2], Mengfan Cheng[3] & Xiaojing Gao[4]

In this paper, a new switching parameter varying optoelectronic delayed feedback model is proposed and analyzed by computer simulation. This model is switching between two parameter varying optoelectronic delayed feedback models based on chaotic pseudorandom sequences. Complexity performance results show that this model has a high complexity compared to the original model. Furthermore, this model can conceal the time delay effectively against the auto-correlation function, delayed mutual information and permutation information analysis methods, and can extent the key space, which greatly improve its security.

Optical chaos systems have superior advantages of generating wide-frequency spectrum, low attenuation and high transmission rate, and thus raising wide attention of researchers and engineers[1–3]. At present, one of the two major methods to generate optical chaotic signal is based on the inner nonlinear effects of semiconductor lasers[4–6] including all-optical feedback, optical injection and optoelectronic feedback. Theoretically, these systems can be characterized by the rate equations. Another method is based on the nonlinear effects of external nonlinear devices, among which Mach-Zehnder modulator (MZ) may be the most common device used in this implementation[7–10]. The optoelectronic delayed feedback system based on MZ modulator has high modulation speed, good stability, large Lyapunov dimension, low cost in experimental and predominance in optical chaos communications. These great advantages make it receive extensively investigated. In theory, this second method can be modeled by Ikeda's delay differential equations.

Although the optoelectronic delayed feedback system based on MZ modulator are proved to have high dynamical complexity, many studies also show that these systems are still vulnerable to attackers[11,12], which are not suitable for some applications, especially for secure communications. Optical chaos systems have two major security deficiencies that the key space is not large enough to resist brute-force attacks[13] and that the output signals carry certain characteristics of the original optical systems, causing time-delay disclosure. Currently, five alternative methods have been proposed to detect the time-delay, including auto-correlation function (ACF)[13,14], delayed mutual information (DMI)[15], permutation information analysis (PIA)[16], extrema statistics[17], and filling factor[18]. Among these methods, ACF, DMI and PIA are the most effective due to non-sensitiveness to noise.

The most effective method treat the first deficiency is to increase the number of tunable parameters in the system[19,20]. To remedy the second shortcoming, the most widely used method is to adjust the parameter of original optical system. Generally, three kinds of parameters can be selected, including time-delay[21,22], gain coefficient[23] and phase[24]. Among them, varying the phase needs to generate a pseudorandom number sequence with a generation rate no less than 3Gb/s, which is difficult to implement. Therefore, varying time-delay or gain coefficient may be the most useful and common methods to conceal the time-delay.

In this paper, we propose a new switching parameter varying optoelectronic delayed feedback model by computer simulation. Our model is to switch between two parameters varying optoelectronic delayed feedback models based on chaotic pseudorandom sequences. Based on digital chaotic map, we vary the gain coefficient of one sub-model and the time-delay of the other sub-model. The trajectory diagram, bifurcation diagram, approximate entropy (ApEn) and permutation entropy (PE) are used for illustrate the model performance. Results indicate that this model has a high complexity compared to the original systems in ref. 9. Thus we conclude that our new model can reduce the time delay more effectively compare to the ACF, DMI and PIA methods. Furthermore, tunable

[1]School of Software, Nanchang University, Nanchang, 330031, PRC. [2]Faculty of Science, Nanchang Institute of Technology, Nanchang, 330029, PRC. [3]School of Optical and Electronic Information, Huazhong University of Science & Technology, Wuhan, 430074, PRC. [4]School of Automation, Huazhong University of Science & Technology, Wuhan, 430074, PRC. Correspondence and requests for materials should be addressed to L.L. (email: vatanoilcy@163.com)

parameters can be used to extent the key space to resist brute-force attacks. This new model has varies applications in many fields such as computer secure communication, random sequence generator and cryptography.

The rest of this paper is organized as follows. In Section 2, the new switching model is introduced. The complexity performance of this model is introduced in Section 3. The time-delay concealment is analyzed in Section 4. Finally, Section 5 concludes the whole paper.

New switching parameter varying optoelectronic delayed feedback model. The original optoelectronic delayed feedback system in ref. 9 can be modeled by the following integro-differential delayed equation:

$$x + \tau\frac{dx}{dt} + \frac{1}{\theta}\int_{t_0}^{t} x(s)ds = \beta\cos^2[x(t-T) + \Phi]$$

(1)

where $\beta = \pi gAGP/2V_\pi$, $\Phi = \pi V_B/2V_{dc}$, $\theta = 1/2\pi f_L$, and $\tau = 1/2\pi f_H$. V_π and V_{dc} are radio-frequency and dc half-wave voltages of MZ modulator; V_B is the biased voltage; P is the power of semiconductor laser source; T is the time-delay; g and G are the gain coefficients of photodiode and ratio-frequency amplifier, respectively. A is the overall attenuation of feedback loop; f_L and f_H are low and high cutoff frequencies, respectively.

Model (1) has been proved to be unsecure[21,23]. Here, we propose a new switching model with varying parameters, which can be written as:

$$\begin{cases} x_1 + \tau_1\frac{dx_1}{dt} + \frac{1}{\theta_1}\int_{t_0}^{t} x_1(s)ds &= \beta_1(t)\cos^2[x_1(t-T) + \Phi_1] \\ x_2 + \tau_2\frac{dx_2}{dt} + \frac{1}{\theta_2}\int_{t_0}^{t} x_2(s)ds &= \beta\cos^2[x_2(t-T_2(t)) + \Phi_2] \\ y_{i+1} &= ry_i(1-y_i) \\ y(t) &= y_{\text{floor}(t/u)} \\ z(t) &= \begin{cases} x_1(t), & y(t) \leq U \\ x_2(t), & y(t) > U \end{cases} \end{cases}$$

(2)

where x_1 and x_2 are the output signals of sub-model 1 and 2. $\tau_{1,2}$, $\theta_{1,2}$, $\Phi_{1,2}$, T, $T_2(t)$, $\beta_1(t)$ and β are the parameters of the two sub-models, respectively. r is the control coefficient of the logistic map with output y_i. U is the switching threshold. u is the time interval, and operating floor (t/u) changes the completely discrete signal y_i into signal $y(t)$. $y(t)$, a step signal with time interval u, is not continuous. $z(t)$ is the final output signal of this model.

As for sub-models 1 and 2 shown in Eq. (2), the parameters of sub-models 1 and 2 are both varying. For sub-model 1, the gain coefficient β is varying; and for sub-model 2, the time-delay T is varying. The varying strategy is as follows.

$$\begin{aligned} \beta_1(t) &= \beta(1 + y(t)) \\ T_2(t) &= T + \text{floor}(5 \cdot y(t)) \end{aligned}$$

(3)

Also, $\beta(t)$ and $T(t)$ are modified every u time rather than continuously. $\beta(t)$ and $T(t)$ will remain the same when $ku \leq t < (k+1)u$, $(k = 0, 1, 2, \ldots)$. In Eq. (3), 5 refers to 5 ns.

As explained ealier, the transfer frequency of output signal $z(t)$ and the parameter varying signal $\beta(t)$, $T(t)$ are all determined by time interval u. The larger the time u is, the slower transfer frequency is take $u = 5$ ns as an example, set $r = 3.9999$, $y_0 = 0.1$, $U = 0.5$, $\beta = 4.5$, $T = 30$ ns, the switching signal $z(t)$ and parameter varying signal $\beta(t)$, $T(t)$ are shown in Fig. 1.

Evidently, the tunable parameters of this new model include β, T, r, U and three initial values. Compare to the original model (1), the parameter r and initial value y_0 of digital chaotic map are newly introduced. Assume the precision is 10^{-16}, the key space will increase more than $0.4 \times 10^{32} \approx 2^{105}$ approximately, which greatly extent the key space of original model.

Furthermore, by analyzing the sensitivity on small key differences, we focus on the newly introduced parameters r and y_0, and change these parameters by 10^{-16}. With different parameters, we can get different trajectories. Then we get the differences between these two trajectories, the results are shown in Fig. 2. Figure 2 indicates that the trajectories are completely different with a small difference of parameter after about 100 ns, which means that the newly brought in secret keys are rather sensitive.

Complexity performances. In this section, we will illustrate the complexity performance of our new model Eq. (2). The parameters are selected as $\tau_{1,2} = 25$ ps, $\theta_{1,2} = 5$ μs, $\Phi_{1,2} = -\pi/4$, $u = 1$ ns, $T = 30$ ns, $U = 0.5$, $r = 3.9999$ and $y_0 = 0.1$. In the experimentation, we use the Matlab R2014a to simulate a theoretical model. The five-order Dormand-Prince method is used here, where 1 ns is divided into 40 iterative steps.

Chaotic trajectories. Figure 3 shows the trajectories of model (2) for $\beta = 4.5$, indicating that our model is chaotic under these parameters and has good pseudorandom property. Furthermore, based on Fig. 3, the trajectory has a drift during the first 50 μs before $z(t)$ enters the chaotic attractor. As time extends, the region of $z(t)$ gradually approaches the chaotic attractor. This drift is not relevant to the delay time but induced by the model (2). After this drift, the trajectory will distribute in the whole chaotic attractor, showing that the model has a good ergodicity.
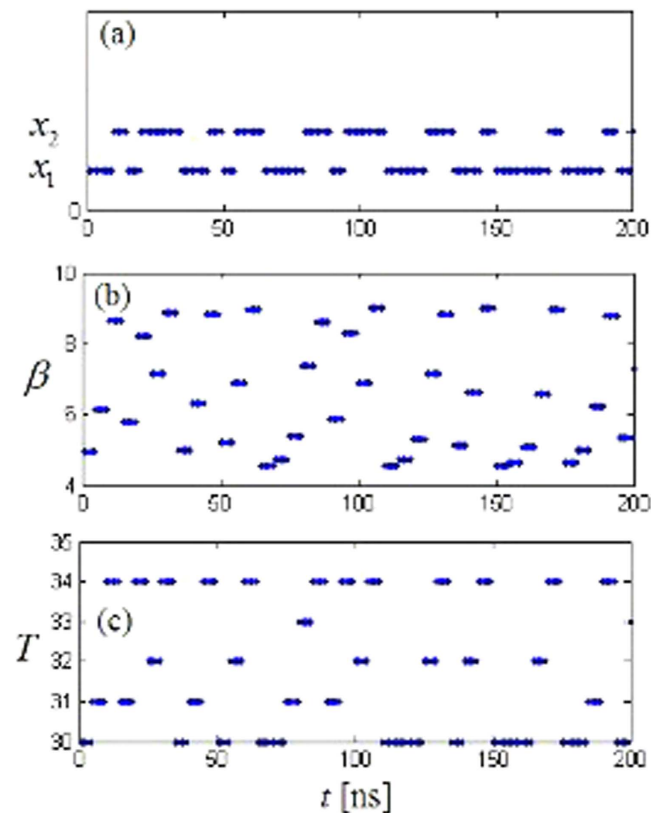
Figure 1. The transfer signal (**a**) $z(t)$; (**b**) $\beta(t)$; and (**c**) $T(t)$.
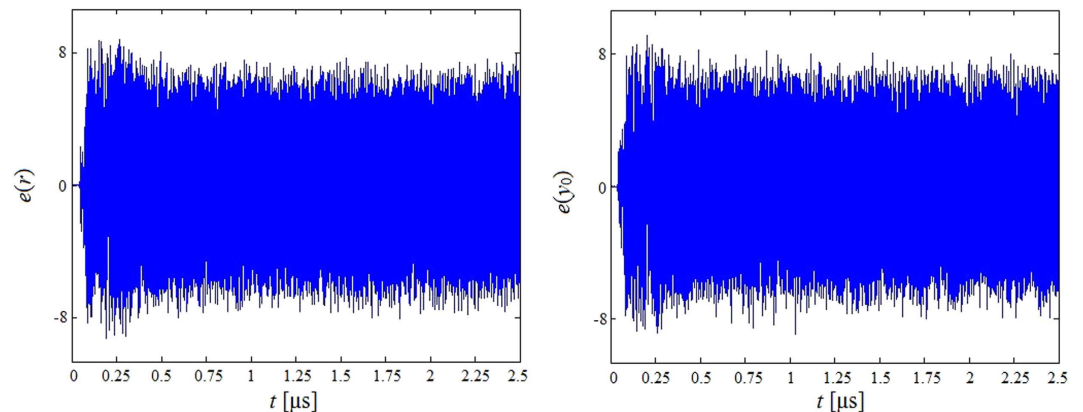

Figure 2. The differences between the trajectories with small difference of parameters (**a**) r; (**b**) y_0.

Bifurcation and amplitude. Figure 4 shows the bifurcation behavior of model (2) with bifurcation parameter β. When $\beta = 0$, the trajectory is a fixed point. As β increases, the trajectory will soon become chaotic. The simulation result indicates that our model can enter chaos region with a lower β than model (1), and other recently proposed systems in refs 14,21,23. This feature will enlarge the chaotic key space of parameter β. Figure 5 shows the amplitude in the asymptotic regime at each value of the bifurcation parameter. As β increases, the amplitude will gradually increase, resulting in a larger range of signal $z(t)$.

Approximate entropy. ApEn was first proposed by Pincus[25] to measure the complexity of time-series, which is closely related to the system distribution and correlation characteristics. The ApEn of the signals of this new model is shown in Fig. 6. As the gain coefficient β increases, the dynamical complexity will improve. As a result, ApEn will increase accordingly. From Fig. 6, we know that both ApEn of models (1) and (2) are positive correlated with β. Evidently, ApEn of this new model is larger than the ApEn of model (1) for the same coefficient β. For a relatively small β, the gap is larger. Furthermore, we compare the ApEn of our model with some proposed systems by setting $\beta = 4.5$. The ApEns of systems in refs 14,21,23 are 1.6373, 1.6510 and 1.7034, respectively, which are all
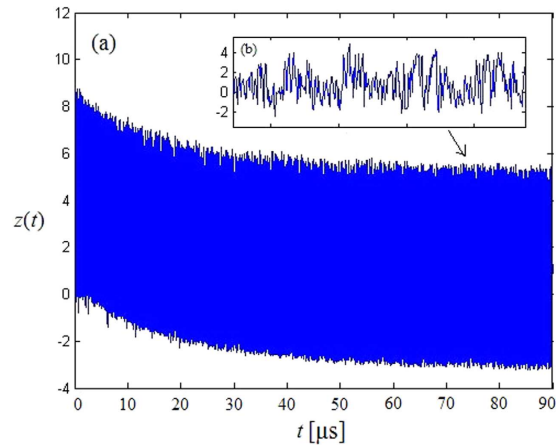
Figure 3. (**a**) The trajectories of our new model; (**b**) Enlargement of (**a**).
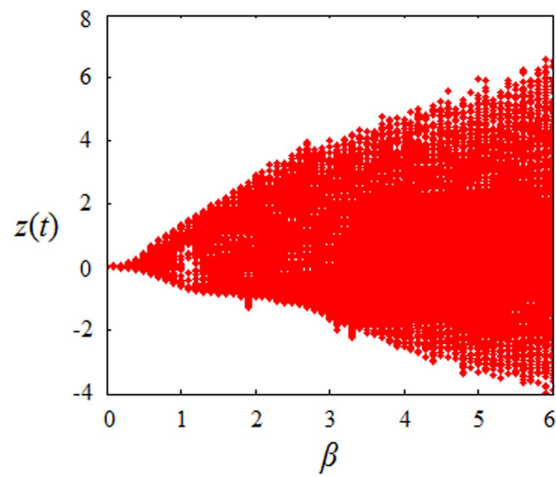

**Figure 4.** Bifurcation diagram of model (2).
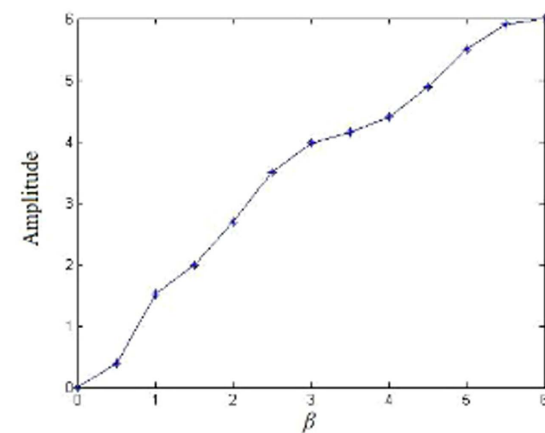
Figure 5. Amplitude at each value of the bifurcation parameter of model (2).

smaller than the ApEn of our model. Therefore, our model is more complex than the original model (1) and other proposed systems in this sense.

Permutation entropy.   PE is a complexity measure which was introduced in ref. 26 by Bandt *et al.* PE compares the size of some consecutive values in the sequence, and summed up different order types, then use Shannon's
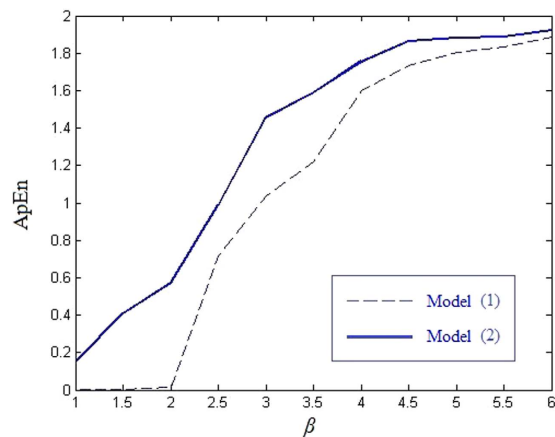
Figure 6. Approximate entropy comparison.
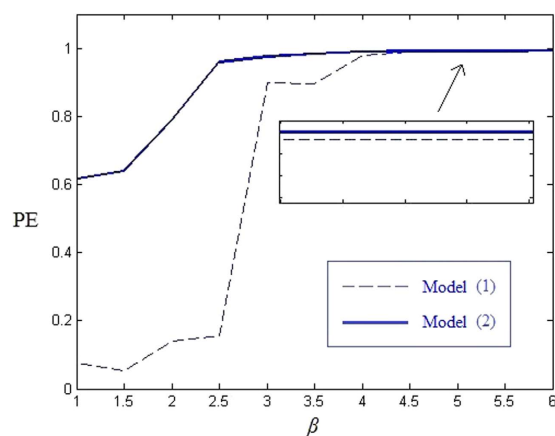
**Figure 7. Permutation entropy comparison.**

entropy to measure the uncertainty of these ordering. PE is easily implemented and is computationally much faster than other comparable methods, such as Lyapunov exponents, while also being robust to noise[27]. As suggest in ref. 26, we select the ordinal pattern length $m = 6$, the embedding delay $D = 2$, and the length N of time series be 1.2×10^5. Figure 7 compares the PE of model (1) and (2). From Fig. 7 we find out that the PE of our model (2) is larger than 0.99 when $\beta > 4$, indicating that the model (2) is relatively complex. By comparing the PE of model (2) and (1), the PE of model (2) is larger than the PE of model (1) when $\beta \leq 4$. For $\beta > 4$, and the PE curves are very close with each other, because as β increases, the PE of original model (1) has already approached the ideal value 1. Although the gap is quite small, the PE has still been increased. Take $\beta = 4.5$ as an example, the PE of model (1) and (2) are 0.9884 and 0.9975 respectively. Comparing to the PE with other systems in refs 13,21,23. For $\beta = 4.5$, the PE of systems in these references are 0.9930, 0.9890 and 0.9910, respectively. Therefore, our model is evidently more complex.

Time-delay concealment. A secure optoelectronic delayed feedback system should conceal time-delay signature against other existing methods. Currently, ACF, DMI and PIA are the three most effective methods for identifying the time-delay. In this section, we will prove that our model (2) can effectively conceal the time-delay against these three methods.

ACF method. Figure 8 show the results of both models (1) and (2) by using ACF method for $\beta = 4.5$. For model (1), there is an obvious extrema at $t = 30$ ns, suggesting that the time-delay has been identified. While for model (2), there is no obvious extrema, showing that the time-delay has been concealed effectively.

The effect of parameter β on the time-delay concealment is further analyzed. First, we define the background Q_{ACF} as

$$
\begin{aligned}
Q_{\text{ACF}} &= [\underline{P}_{\text{ACF}}(\beta), \overline{P}_{\text{ACF}}(\beta)] \\
\underline{P}_{\text{ACF}}(\beta) &= mean\{\text{ACF}(z(\beta))\} - SD(\text{ACF}(z(\beta))) \\
\overline{P}_{\text{ACF}}(\beta) &= mean\{\text{ACF}(z(\beta))\} + SD(\text{ACF}(z(\beta)))
\end{aligned}
\tag{4}
$$
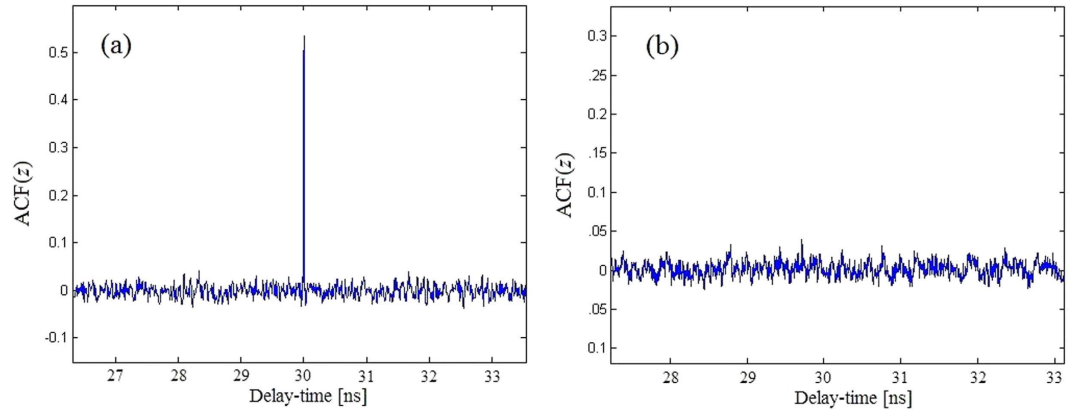
Figure 8. ACF(z). (**a**) Model (1); (**b**) Model (2).
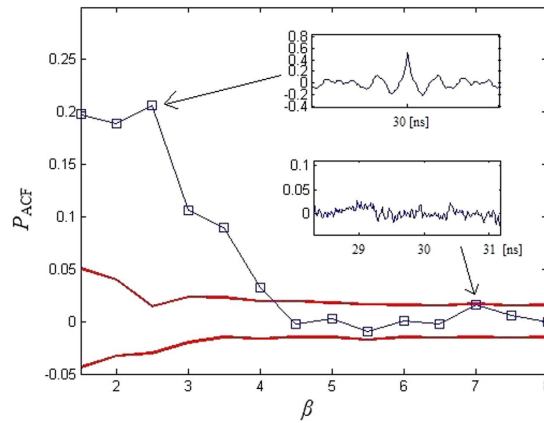
Figure 9. Value of the peaks in ACF(z) at $T = 30$ ns. The red lines correspond to the background Q_{ACF}.

where SD is the standard deviation. For each β, $z(\beta)$ is the output signal of model (2). The peak size at the relevant time-delay is defined as

$$P_{ACF}(\beta) = ACF(z(\beta), T) \tag{5}$$

Figure 9 shows the size of the peak at the relevant time-delay $T = 30$ ns from the background (red lines) Q_{ACF} in ACF(x_1). Figure 9 shows that the peaks are not apparent from the background Q_{ACF} once β increases to the approximate critical value 4.5. For $\beta \geq 4.5$, the time-delay can be concealed using ACF method.

DMI method.   Figure 10 shows the results of model (1) and (2) by using DMI method for $\beta = 4.5$. Figure 10 shows that there is an obvious peak at $t = 30$ ns, the exact time delay of model (1). While for model (2), there is no obvious extrema along the evolution, indicating that the time-delay cannot be identified.

We further analyze the influence of parameter β on the time-delay concealment. The background Q_{DMI} is defined as

$$
\begin{aligned}
Q_{DMI} &= [\underline{P}_{DMI}(\beta), \overline{P}_{DMI}(\beta)] \\
\underline{P}_{DMI}(\beta) &= \frac{mean\{DMI(z(\beta))\} - SD(DMI(z(\beta)))}{mean\{DMI(z(\beta))\} - SD(DMI(z(\beta)))} \\
\overline{P}_{DMI}(\beta) &= \frac{mean\{DMI(z(\beta))\} + SD(DMI(z(\beta)))}{mean\{DMI(z(\beta))\} - SD(DMI(z(\beta)))}
\end{aligned}
\tag{6}
$$

and the peak size at the relevant time-delay is defined as

$$P_{DMI}(\beta) = \frac{DMI(z(\beta), T)}{mean\{DMI(z(\beta))\} - SD(DMI(z(\beta)))} \tag{7}$$

The peak size at the relevant time-delay $T = 30$ ns and the background (red lines) Q_{DMI} are shown in Fig. 11. From Fig. 11 we know that, when $\beta \geq 4.5$, all the peak sizes are located in the background Q_{DMI}, indicating that the time-delay will be concealed for $\beta \geq 4.5$.
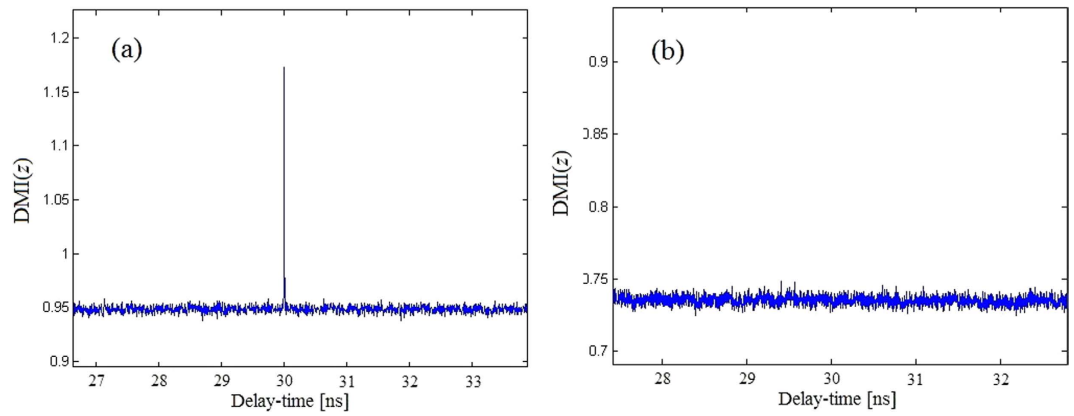
Figure 10. DMI(z). (**a**) Model (1); (**b**) Model (2).
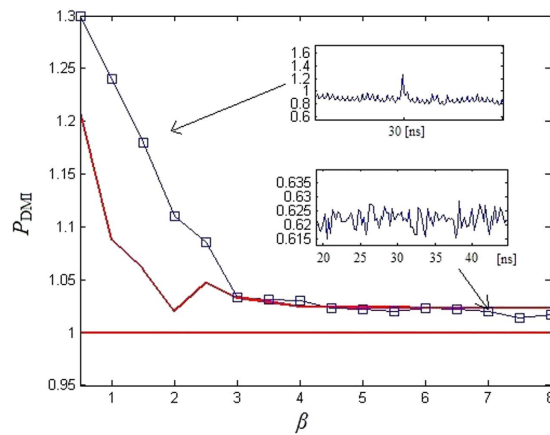
Figure 11. Value of the peaks in DMI(z) at $T = 30$ ns. The red lines correspond to the background Q_{DMI}.
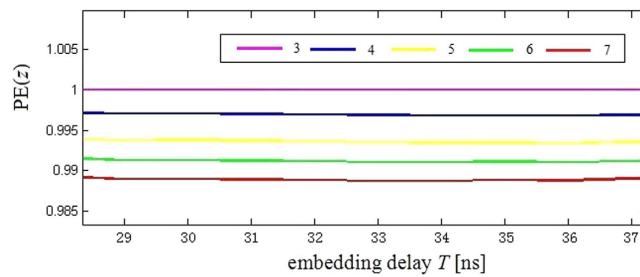
Figure 12. PE(z) with ordinal pattern lengths $L = 3, 4, 5, 6$ and 7, respectively.

PIA method. Figure 12 shows the PE(z) of the embedding delay T is shown for $\beta = 4.5$ with ordinal pattern lengths $L = 3, 4, 5, 6$ and 7, respectively (The selection of L is suggest in ref. 26). Figure 12 suggests that there is no local extrema in PE(z), and that the time-delay can be concealed.

In order to analyze the influence of parameter β on the time-delay concealment, we define the background Q_{PIA} and the peak size at the relevant time-delay as

$$
\begin{aligned}
Q_{PIA} &= [\underline{P}_{PIA}(\beta), \overline{P}_{PIS}(\beta)] \\
\underline{P}_{PIA}(\beta) &= mean\{PE(z(\beta))\} - SD(PE(z(\beta))) \\
\overline{P}_{PIA}(\beta) &= mean\{PE(z(\beta))\} + SD(PE(z(\beta)))
\end{aligned}
\tag{8}
$$

$$
P_{PIA}(\beta) = PE(z(\beta), T) \tag{9}
$$
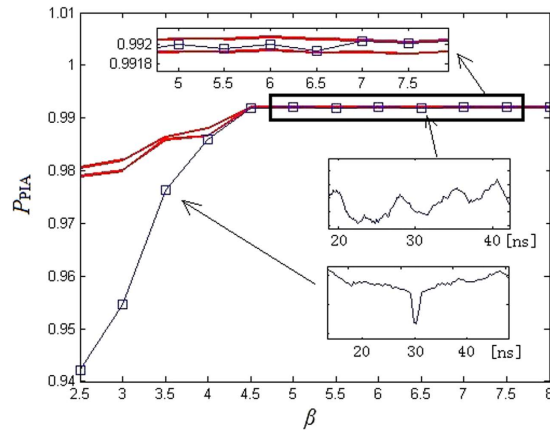
Figure 13. Value of the peaks in PE(z). The red lines correspond to the background Q_{PIA}.

Figure 13 shows the peak size at relevant time-delay of 30 ns from the background (red lines) Q_{PIA} in $PE(x_1)$. As shown in Fig. 13, when $\beta \geq 4.5$, all peak sizes are in the Q_{PIA} interval. This result shows that the time-delay is not available by PIA method.

In summary, the time-delay signal of model (2) can be effectively concealed using the ACF, DMI and PIA methods for $\beta \geq 4.5$.

Conclusion

In this paper, we propose a new switching parameter varying optoelectronic delayed feedback model with computer simulation. This model is switching between two parameter varying optoelectronic delayed feedback models based on chaotic pseudorandom number sequences. We use the trajectory diagram, bifurcation diagram, approximate entropy and permutation entropy to illustrate its complexity. The results show that this model is more complex than the original model (1). We prove that our new model can conceal the time delay effectively against the ACF, DMI and PIA methods. Furthermore, some tunable parameters are brought in, which can extent the key space to resist brute-force attack.

As we know, chaotic systems have a widely use in many different kinds of fields, especially in cryptography. This paper discusses and proposes a new chaotic model, which has a high dynamical complexity, large key space, and proper conceal of time-delay compared to other common methods. All these characteristics show that our chaotic model is relatively secure to be applied in chaotic cryptography, including chaotic secure communication and chaotic pseudorandom sequence generator. For future work, we will study the applications based on this new chaotic model.

References

1. Argyris, A. & Syvridis, D. Chaos-based communications at high bit rates using commercial fiber-optic links. *Nature* **438,** 343–346 (2005).
2. Xiang, S. Y. *et al.* Phase-modulated dual-path feedback for time delay signature suppression from intensity and phase chaos in semiconductor laser. *Opt. Commun.* **324,** 38–48 (2014).
3. Li, N. *et al.* Chaotic optical cryptographic communication using a three-semiconductor-laser scheme. *J. Opt. Soc. Am. B* **29,** 101–108 (2012).
4. Jiang, N. *et al.* Isochronal chaos synchronization of semiconductor lasers with multiple time-delayed couplings. *J. Opt. Soc. Am. B* **28,** 1139–1145 (2011).
5. Ohtsubo, J. Dynamics in semiconductor lasers with optical injection, in: Semi-conductor Lasers, in: Springer Ser. *Opt. Sci.* **111,** 169–204 (2013).
6. Rajesh, S. & Nandakumaran, V. M. Control of bistability in a directly modulated semiconductor laser using delayed optoelectronic feedback. *Physica D* **213,** 113–120 (2006).
7. Soriano, M. C.,Ojalvo, J. G., Mirasso, C. R. & Fischer, I., Complex photonics: Dynamics and applications of delay-coupled semiconductors lasers. *Reviews of Modern Physics.* **85,** 421–470 (2013).
8. Lavrov, R., Jacquot, M. & Larger, L. Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gb/s chaos communications. *IEEE J. Quantum Electron.* **46,** 1430–1435 (2010).
9. Kouomou, Y. C., Colet, P., Larger, L. & Gastaud, N. Chaotic breathers in delayed electro-optical systems. *Phys. Rev. Lett.* **95,** 203903 (2005).
10. Larger, L. Complexity in electro-optic delay dynamics: modeling, design and applications. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences.* **371,** 20120464 (2013).
11. Udaltsov, V. S. *et al.* Cracking chaos-based encryption system ruled by nonlinear time dealy differential equations. *Phys. Lett. A.* **308,** 54–60 (2003).
12. Udaltsov, V. S., Larger, L. & Geodgebuer, J. P. Time delay identification in chaotic cryptosystems ruled by delay-differential equations. *J. Opt. Technol.* **72,** 373–377 (2005).
13. Romain, R. M. *et al.* Digital Key for Chaos Communication Performing Time Delay Concealment. *Phys. Rev. Lett.* **107,** 034103 (2011).
14. Cheng, M., Deng, L., Li, H. & Liu, D. Enhanced secure strategy for electro-optic chaotic systems with delayed dynamics by using fractional Fourier transformation. *Opt. Express* **22,** 5241–5251 (2014).
15. Nguimdo, R. M., Verschaffelt, G., Danckaert, J. & Van der Sande, G. Loss of time-delay signature in chaotic semiconductor ring lasers. *Opt. Lett.* **37,** 2541–2543 (2012).
16. Soriano, M. C., Zunino, L., Rosso, O. A., Fischer, I. & Mirasso, C. R. Time scales of a chaotic semiconductor laser with optical feedback under the lens of a permutation information analysis. *IEEE J. Quantum Electron.* **47,** 252–261 (2011).

17. Prokhorov, M., Ponomarenko, V., Karavaev, A. & Bezruchko, B. Reconstruction of time-delayed feedback systems from time series. *Physica D* **203,** 209–223 (2005).
18. Bünner, M., Meyer, T., Kittel, A. & Parisi, J. Recovery of the time-evolution equation of time-delay systems from time series. *Phys. Rev. E* **56,** 5083 (1997).
19. Bogris, A., Rizomiliotis, P., Chlouverakis, K. E., Argyris, A. & Syvridis, D. Feedback phase in optically generated chaos: A secret key for cryptographic applications. *IEEE J. Quantum Electron.* **44,** 119–124 (2008).
20. Kye, W. H. *et al.* Synchronization of delay systems in the presence of delay time modulation. *Phys. Lett. A.* **322,** 338–343 (2004).
21. Gao, X. J., Xie, F. L. & Hu, H. P. Enhancing the security of electro-optic delayed chaotic system with intermittent time-delay modulation and digital chaos. *Optic Commun.* **352,** 77–83, (2015).
22. Kye, W. H. Information transfer via implicit encoding with delay time modulation in a time-delay system. *Physics Letters A.* **376,** 2663–2667 (2012).
23. Hu, H. P., Su, W., Liu, L. F. & Yu. Z. L. Electro-optic intensity chaotic system with varying parameters. *Physics Letters A.* **378,** 184–190 (2014).
24. Nguimdo R. M. & Colet. P. Electro-optic phase chaos systems with an internal variable and a digital key. *Opt. Express.* **20,** 25333–25344 (2012).
25. Pincus, S. M. Approximate entropy as a measure of system complexity. *Proc. Nat. Acad. Sci.* (PNAS). **88,** 2297–2301 (1991).
26. Bandt, C. & Pompe, B. Permutation Entropy: A Natural Complexity Measure for Time Series. *Phys. Rev. Lett.* **88,** 174102 (2002).
27. Toomey J. & Kane, D. Mapping the dynamic complexity of a semiconductor laser with optical feedback using permutation entropy. *Opt. Express.* **22,** 1713–1725 (2014).

Acknowledgements

Author Contributions

L.L. wrote the main manuscript text, S.M. and M.C. do the numerical experiments, L.L. and X.G. analyzed the results.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Liu, L. *et al.* A new switching parameter varying optoelectronic delayed feedback model with computer simulation. *Sci. Rep.* **6**, 22295; doi: 10.1038/srep22295 (2016).