entropy

MDPI

Article

Hybrid Control of Digital Baker Map with Application to Pseudo-Random Number Generator

Yuhui Shi and Yashuang Deng *

The School of Information and Safety Engineering, Zhongnan University of Economic and Law, Wuhan 430073, China; 202011200015@stu.zuel.edu.cn

* Correspondence: dys0377@zuel.edu.cn; Tel.: +86-151-7253-0160

Abstract: Dynamical degradation occurs when chaotic systems are implemented on digital devices, which seriously threatens the security of chaos-based cryptosystems. The existing solutions mainly focus on the compensation of dynamical properties rather than on the elimination of the inherent biases of chaotic systems. In this paper, a unidirectional hybrid control method is proposed to improve the dynamical properties and to eliminate the biases of digital chaotic maps. A continuous chaotic system is introduced to provide external feedback control of the given digital chaotic map. Three different control modes are investigated, and the influence of control parameter on the properties of the controlled system is discussed. The experimental results show that the proposed method can not only improve the dynamical degradation of the digital chaotic map but also make the controlled digital system produce outputs with desirable performances. Finally, a pseudorandom number generator (PRNG) is proposed. Statistical analysis shows that the PRNG has good randomness and almost ideal entropy values.

Keywords: chaos; digital Baker map; dynamical degradation; hybrid control; entropy

Citation: Shi,Y.; Deng,Y. Hybrid control of digital Baker map with application to pseudo-random number generator. *Entropy* **2021**, *23*, 578. https://doi.org/10.3390/e23050578

Academic Editor: Ravi P. Agarwal and Maria Alessandra Ragusa

Received: 3 April 2021
Accepted: 30 April 2021
Published: 8 May 2021

1. Introduction

Chaos was first discovered by accident in 1961 while Lorenz was researching weather forecasting simulations [1]. However, the term "chaos" was only officially defined in 1975. Chaos is widely used in communication, mathematics, biology, information technology, economics, etc. primarily due to its distinct characteristics, such as sensitivity to an initial value, topological transitivity, ergodicity, unpredictability, etc. Specifically, the high consistency between chaos and cryptographic design criteria allowed for large numbers of chaos-based secure applications to emerge. Since the first chaotic stream cipher scheme was proposed in 1989 [2], chaotic encryption technology has been of great concern. Meanwhile, the design and analysis of chaotic cipher have been carried out one after another. Thus far, many secure communication systems have been proposed, including multimedia digital encryption [3], data watermarking, synchronization security systems, and data hiding systems based on chaos, etc.

Existing chaotic cryptography schemes are mostly based on chaotic systems implemented on digital devices with limited precision, namely digital chaotic systems. However, chaos collapses in the digital world, specifically, chaotic systems display dynamical degradation behaviors, such as short periodic orbits, low complexity, strong correlation, uneven distribution, etc. The occurrence of these situations make the output of the chaotic system reflect these system characteristics. Due to these system characteristics, the attacker can effectively capture the system orbit information to analyze the chaotic system; therefore, the chaotic system can be attacked and the chaotic cryptographic system poses a great safety hazard. Therefore, estimating these biases of the chaotic system is the core of ensuring the security of the chaotic cryptographic system. The "bias" is mainly observed from a security point of view, which refers to these non-random features of the original chaotic system such as the uneven distribution of outputs, the obvious attractor structure, among others. Such

bias of a chaotic system often allows its outputs to reflect the system characteristics (such as information about the system parameters). In conclusion, an anti-degradation chaotic system plays an important role in the fields of cryptography and secure communication and it is of great significance to guarantee the security of chaotic security systems.

In view of the finite precision effect of digital chaotic systems, some solutions have been proposed to combat the degradation of digital chaotic systems. The first is to use high finite precision [4]. Wheeler and Matthews [5] proposed that the use of supercomputers and other hardware devices with higher computational accuracies would increase the period of the digital chaotic sequence but could not solve the essential problem. The second is to cascade multiple chaotic systems [6–9]. Multiple identical or different chaotic systems are cascaded to extend the period of a digital chaotic sequence and to resist predictability [10]. It is more unpredictability and more complex compared with the original chaotic system and has a larger parameter space. However, this method cannot entirely solve the problem of a short orbital period and the distribution of the output is not uniform. The third solution is to switch between multiple chaotic systems, which can indeed increase the average period duration but performs poorly in the improvement of the distribution [11]. More importantly, the final effect of this scheme depends on the switching rule and the switching system to a great extent, such that it is difficult to guarantee universality. The fourth is the perturbation mechanism [12–22]. Liu and Lin [23] created perturbation chaotic systems to perturb state variables and system parameters with a logistic map. Liu and Luo [24] proposed a continuous Chen system to perturb both the parameters and the inputs of the Chebyshev system. The results showed that the chaotic performance of the perturbed system is indeed enhanced, but there are still some problems such as unbalanced distribution. The fifth solution is a coupling mechanism [25–28]. Coupling can be single coupling or bidirectional coupling (two chaotic systems coupled to one another). The chaotic system can be analog or digital. Additionally, an external nonlinear source can be coupled to the chaotic system, such as a pseudorandom sequence or linear feedback shift register (LFSR) sequence or nonlinear feedback shift register (NFSR). Chen [29] proposed a state feedback control method that can be applied not only to one-dimensional but also multidimensional chaotic mapping. Deng [30] put forward an effect chaotification method for digital chaotic systems based on the differential mean value theorem and state feedback technology that can produce the desirable dynamical behaviors in terms of cryptography; however, it has a limitation with regard to the dimensions of chaotic systems. Zhang [31] proposed using piecewise linear chaotic mapping and cubic S-box coupling. Liu [32] proposed that the state variables of one digital chaotic map can be used to control the parameters of another digital chaotic map. In general, the coupling method has a good effect on the improvement of system performance.

It is clear from existing research that improvements in the performance of controlled systems depend on the control source and control mode. Indeed, continuous chaotic systems can preserve their good dynamical properties; however it is difficult to maintain long-term, stable synchronization owing to parameter uncertainties. Most chaotic cryptographic algorithms are designed based on digital chaotic systems mainly due to its reproducibility and stability. Unfortunately, although digital chaotic systems can easily retain synchronization for a long time given the same system and initial value, they often suffer from dynamical degradation due to finite computing precision. Additionally, such degeneration still exists for many autonomous digital chaotic systems, which means that an external control is needed to obtain a digital chaotic system with desirabled performance. From the above consideration, we discuss the unidirectional hybrid control model by introducing a continuous chaotic system. This paper introduces a continuous system to exert feedback control for the given digital chaotic map, where a Chen system [33] and a Baker system are chosen here. As a two-dimensional system, the Baker system is widely used in image encryption. Therefore, it is necessary to improve the digital system. We present the related literature on Baker maps [34]. The authors of [35] controlled Baker mapping based on the probabilistic coupling of controlled dynamics and control systems, and the

subsequent improvement of coupled dynamics in a suitable functional space. The lifted dynamics is governed by linear Perron-Frobenius and Koopman operators. The novelty of [36] is that they described linear systems as microchaos. They showed that these vibrations may be related to the deterministic chaotic dynamics caused by sampling and quantization. In addition, they gave a detailed chaotic analysis as proof for the PD controlled oscillator. In this case, they developed a method to accurately calculate the average lifetimes of chaotic transients. Three control modes were investigated, and the effect of the control parameter on system performance was also discussed. Their experimental simulations showed that not only was the skewness in dynamic performance of the controlled system eliminated but also the desired dynamic performance was presented. In particular, it is worth mentioning that the outputs displayed almost ideal information entropy, approximate entropy, and permutation entropy. Finally, a novel PRNG was constructed based on the controlled digital Baker map. Statistical tests along with other analyzes were carried out to show the randomness of the generated sequences.

This paper is organized as follows. Section 2 briefly introduces the degradation phenomenon of the digital Baker map. Section 3 discusses three control modes and analyzes the effect of control gain coefficient on the output control mode. Section 4 gives a performance comparison with existing methods. Section 5 presents a novel PRNG and analyzes its randomness and security.

2. Dynamical Degradation of Digital Baker Map

The Baker chaotic map can be written as follows:

$$(x_{i+1}, y_{i+1}) = \begin{cases} (\frac{x_i}{u}, uy_i) & 0 < x_i, y_i \leq u \\ (\frac{x_i - u}{1-u}, (1-u)y_i + u) & u < x_i, y_i \leq 1 \end{cases} \quad (1)$$

where $x_i, y_i \in [0, 1]$ are state variables of the system and $u \in (0, 1]$ is the system parameter.

When the Baker chaotic map is realized with finite computing precisions, it degrades into the following digital map:

$$(x^*_{i+1}, y^*_{i+1}) = \begin{cases} (\frac{x^*_i}{u}, uy^*_i) & 0 < x^*_i, y^*_i \leq u \\ (\frac{x^*_i - u}{1-u}, (1-u)y^*_i + u) & u < x^*_i, y^*_i \leq 1 \end{cases} \quad (2)$$

where $x^*_{i+1} = f(x^*_i)$ and $x^*_i = FL(x_i)$. $x^*_i \in \Omega_p$ is a digital variable with p bit precision, and $x_i \in \Omega$ is a real-intermediate variable. $\Omega_p = \{x_i = k \times 2^{-p} | k = 0, 1, 2, ..., 2^{p-1}\}$. p is the computing precision. $f : \Omega \to \Omega$ is a nonlinear function. $FL : \Omega \to \Omega_p$ is a quantization function, and it is defined as $FL(x) = \lfloor x \cdot 2^p \rfloor \cdot 2^{-p}$. The quantification method of variable y is the same as that of variable x.

We set p = 8. Indeed, the precision can, of course, be selected several times larger in practical applications. There are two reasons why we chose a precision of 8. First, the lower the precision, the more obvious the degeneration behavior of the chaotic system. Our solution can still maintain good chaotic performance even under low-precision situations, which will undoubtedly show the effectiveness of our method. Second, the higher the precision, the longer it takes to implement with digital equipment. Therefore, it is necessary to study the realization of digital chaotic system with low precision. We choose parameter and initial values u = 0.49, x_0 = 0.2, and y_0 = 0.29 randomly. These parameters and initial values were only randomly selected by us, and the effect of our scheme is the same for other values. We observed the dynamical properties of the digital Baker map.

It is clear from Figure 1a that the digital map enters a periodic loop state only after nearly 40 iterations. As shown in Figure 1b,c, the digital map has obvious distribution characteristics and architectural features. Such dynamical biases often make the system vulnerable to attacks. Meanwhile, it can be seen from Figure 1d that two orbits meet only after 10 iterations, which indicates that the system has no sensitivity to initial values.

Moreover, both the bad auto-correlation shown in Figure 1e and the cross-correlation shown in Figure 1f indicate that strong correlations between different outputs of the system exist.

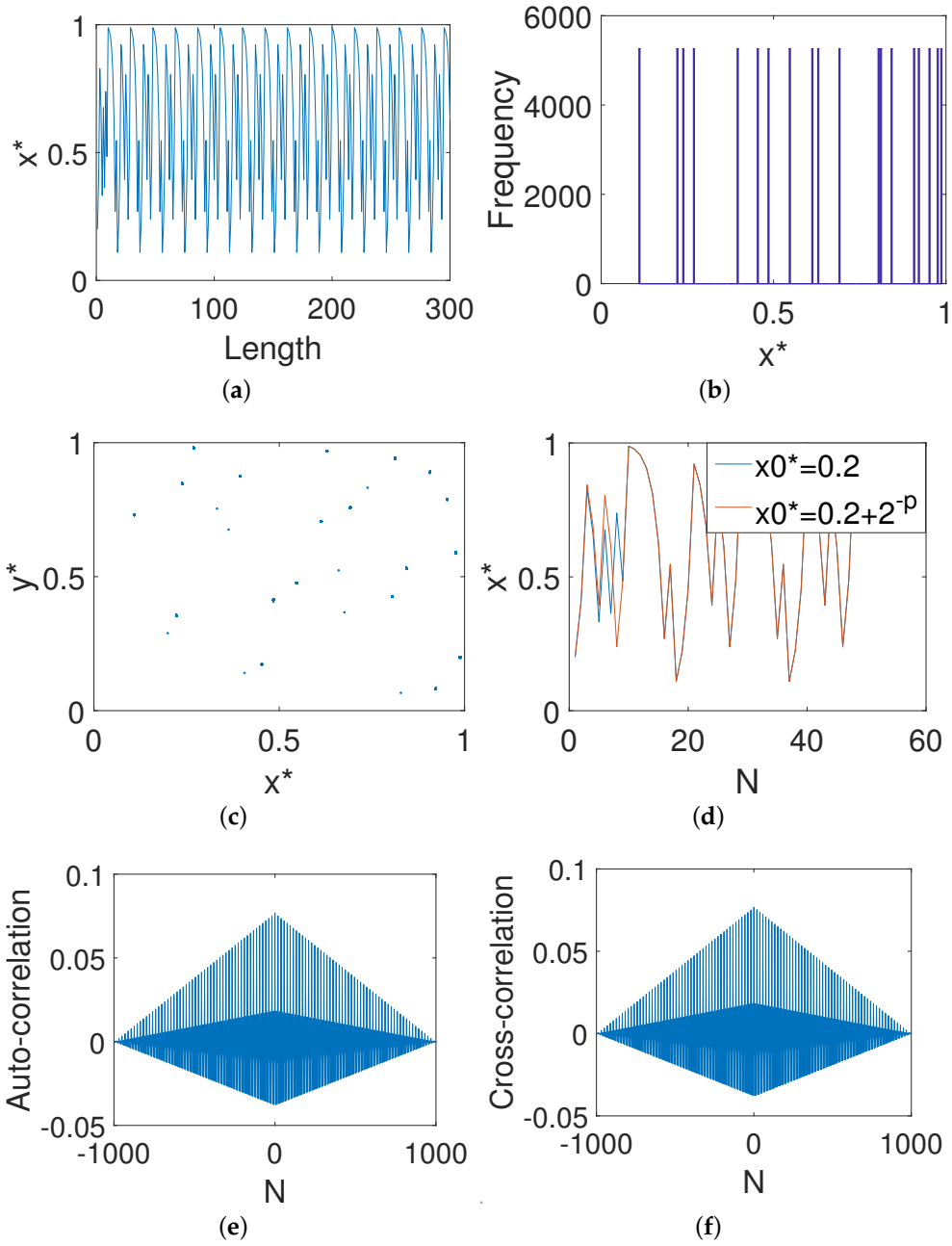

Figure 1. The dynamical properties of the digital Baker map. (**a**) The x-dimensional output. (**b**) The x-dimensional distribution. (**c**) Phase diagram. (**d**) Initial value sensitivity. (**e**) Auto-correlation. (**f**) Cross-correlation.

Moreover, three typical types of entropy indicators are applied to investigate the complexity of the digital Baker system from different aspects. Information entropy measures the uncertainty or unpredictability of a time series. Approximate entropy primarily measures the probability of generating a new pattern in a time series. Permutation entropy depicts the structural complexity of a time series: the closer the permutation entropy is to 1, the better the randomness of the sequence. In general, the smaller the entropy is, the simpler and more regular the time series. On the contrary, the larger the entropy value, the more complex and random the time series.

It can be seen from Figure 2a that the approximate entropy of the digital Baker system at different precisions (except 8–12 bits) is about 0.7. This shows that the complexity of the system is low and that the regularity is strong. Under the precison of 8, the closer the information entropy is to 8, the better the randomness of the sequence. Figure 2b shows that the information entropy of the digital Baker system is about 4.2, which means that it has poor randomness. Figure 2c shows that the permutation entropy of the digital Baker mapping at different precisions is almost 0.4 to 0.8.

From the above analysis, it can be included that the original good characteristics disappear indeed and that some dynamical degradation behaviors occur when the Baker chaotic map is implemented with finite computing precisions, including the periodic orbit, low complexity and strong correlation, uneven distribution, etc.

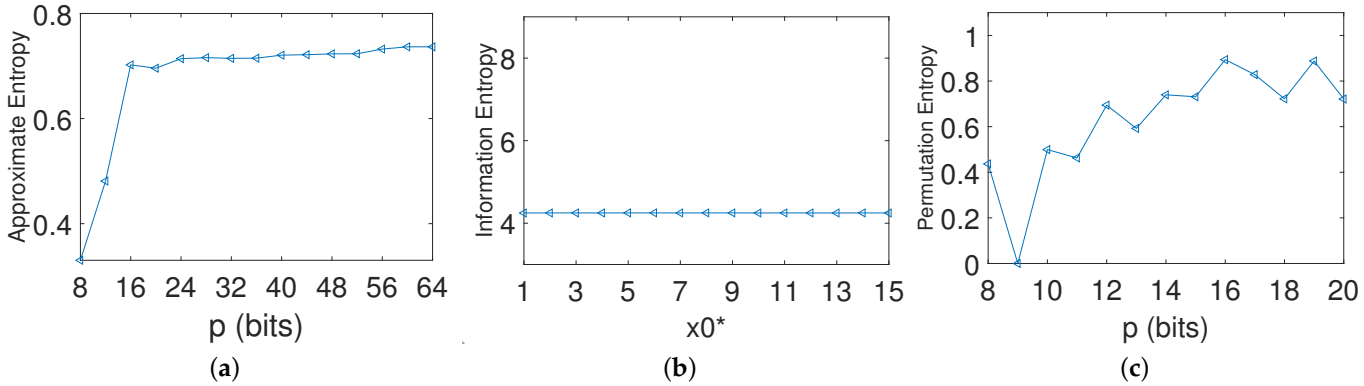

Figure 2. Entropy analysis of the digital Baker map. (**a**) Approximate entropy. (**b**) Information entropy. (**c**) Permutation entropy.

3. A Unidirectional Hybrid Control Scheme

In this section, a unidirectional hybrid control scheme is set up, where a continuous Chen chaotic system is introduced to control external state feedback for the digital Baker map.

3.1. Chen Chaotic System

A continuous Chen system can be defined as follows:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = xy - bz \end{cases} \tag{3}$$

It is well known that the system has a chaotic attractor when $a = 35$, $b = \frac{8}{3}$ and $c = 28$, as shown in Figure 3.

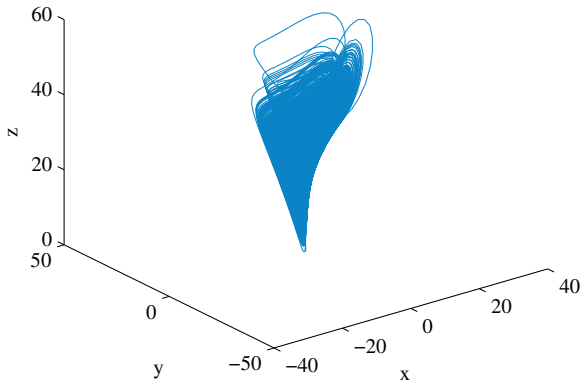

Figure 3. Chen chaotic attractor.

3.2. Three Control Modes

In this part, we first investigate the performances of three control modes, including parameter control, input control, and output control of the digital Baker map. Then, the optimal control mode is chosen to construct the final control model.

The first control mode controls the parameter u of the digital map, which can be represented as follows:

$$u \to u_i : u_{i+1} = u_i + \tilde{z}_i \mod 1 \tag{4}$$

where $\tilde{z}_i$ denotes the sampling state of a Chen chaotic system in z dimension.

Then, the parameter-controlled digital Baker map (PCB) is expressed as Equation (5):

$$(x_{i+1}, y_{i+1}) = \begin{cases} (\frac{x_i^*}{u_i}, y_i^* \cdot u_i) & 0 < x_i^*, y_i^* \le u_i \\ (\frac{x_i^* - u_i}{1-u_i}, y_i^* \cdot (1-u_i) + u_i) & u_i < x_i^*, y_i^* \le 1 \\ x_i^* = FL(x_i) & \\ y_i^* = FL(y_i) & \end{cases} \tag{5}$$

The second control mode controls the inputs x and y of the digital map, which can be represented as follows:

$$\bar{x}_i = x_i^* + \tilde{x}_i \mod 1 \tag{6}$$

$$\bar{y}_i = y_i^* + \tilde{y}_i \mod 1 \tag{7}$$

where $\tilde{x}_i$ and $\tilde{y}_i$ denote the sampling states of a Chen chaotic system in the x and y dimensions.

Then, the input-controlled digital Baker map (ICB) is expressed as follows:

$$(x_{i+1}, y_{i+1}) = \begin{cases} (\frac{\bar{x}_i}{u}, \bar{y}_i \cdot u) & 0 < \bar{x}_i, \bar{y}_i \le u \\ (\frac{\bar{x}_i - u}{1-u}, \bar{y}_i \cdot (1-u) + u & u < \bar{x}_i, \bar{y}_i \le 1 \\ \bar{x}_i = FL(x_i) & \\ \bar{y}_i = FL(y_i) & \end{cases} \tag{8}$$

The third control mode controls the outputs of the digital map, and the output-controlled Baker chaotic system (OCB) is expressed as follows:

$$(x_{i+1}, y_{i+1}) = \begin{cases} (\frac{x_i^*}{u} + \tilde{x}_i, y_i^* \cdot u + \tilde{y}_i) \mod 1 & 0 < x_i^*, y_i^* \le u \\ (\frac{x_i^* - u}{1-u} + \tilde{x}_i, y_i^* \cdot (1-u) + u + \tilde{y}_i) \mod 1 & u < x_i^*, y_i^* \le 1 \\ x_i^* = FL(x_i) & \\ y_i^* = FL(y_i) & \end{cases} \tag{9}$$

3.3. Performance Comparison of Three Control Modes

Set the precision p = 8, system parameter u = 0.49, and initial values x_0 = 0.81 and y_0 = 0.29. Then, we compared three control modes by analyzing the dynamical properties of three controlled digital Baker maps including the orbit, distribution, phase diagram, sensitivity to initial states, correlation, and entropy of the control systems.

3.3.1. Trajectory

As shown in Figure 4a, the trajectory of Equation (5) quickly converges to a fixed point after almost 90 iterations, which is slightly better than the original digital map. Figure 4b shows that the trajectory of Equation (8) converges to a cycle or a fixed point after a few iterations. By contrast, it is obvious from Figure 4c that it is difficult to find a period in the trajectory of Equation (9) that shows that the OCB mode can greatly extend the period of the digital system and that performs better than the other two control modes.

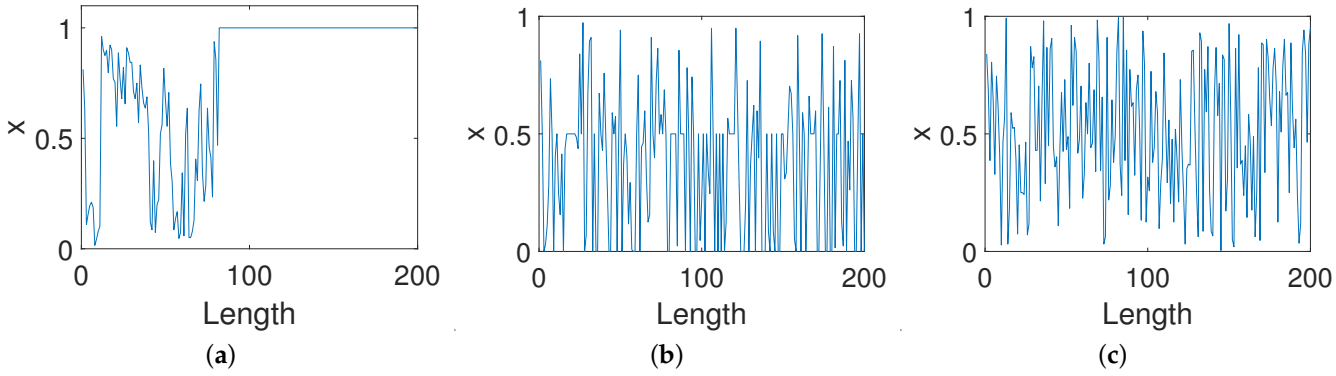

Figure 4. Trajectories of systems under three control modes. (**a**) PCB. (**b**) ICB. (**c**) OCB.

3.3.2. Frequency Distribution

As shown in Figure 5a, the frequency distribution of the PCB system becomes worse than the original digital system since there is a fixed point. Meanwhile, it is clear from Figure 5b that there is an obvious characteristic in the frequency distribution of the ICB system. On the contrary, the frequency distribution of the OCB system reveals an almost even distribution (see Figure 5c), which indicates the OCB behaves better than the other two control modes in this case.

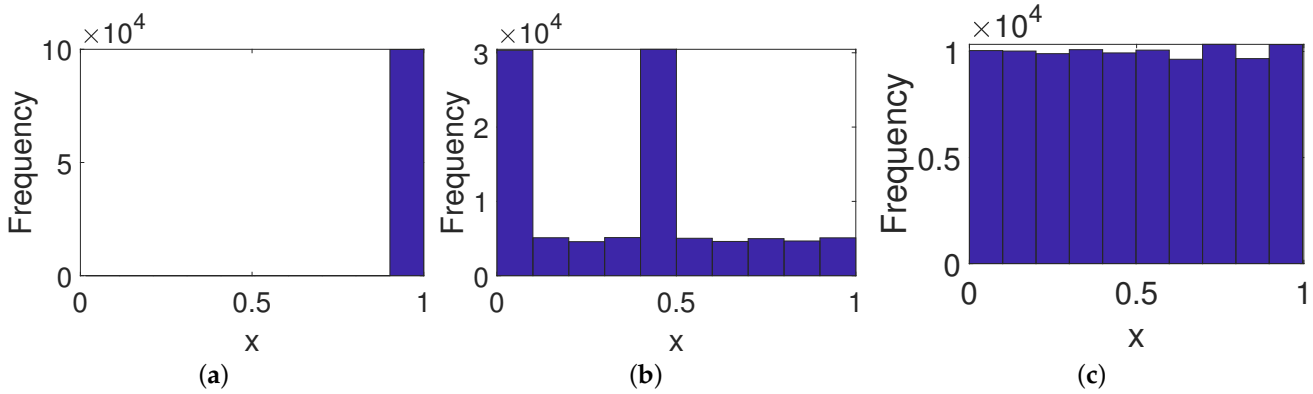

Figure 5. Frequency distributions of systems under three control modes. (**a**) PCB. (**b**) ICB. (**c**) OCB.

3.3.3. Phase Diagram

As shown in Figure 6a, the PCB mode does not seem to improve the phase space of digital system. It can be seen from Figure 6b that the states cannot go through the entire phase space. Meanwhile, no pattern exists and only a noise-like phenomenon in the phase diagram of OCB system exists (see Figure 6c), which prevents any relevant information from the phase diagram. In this way, the OCB mode behaves better than two other control modes.

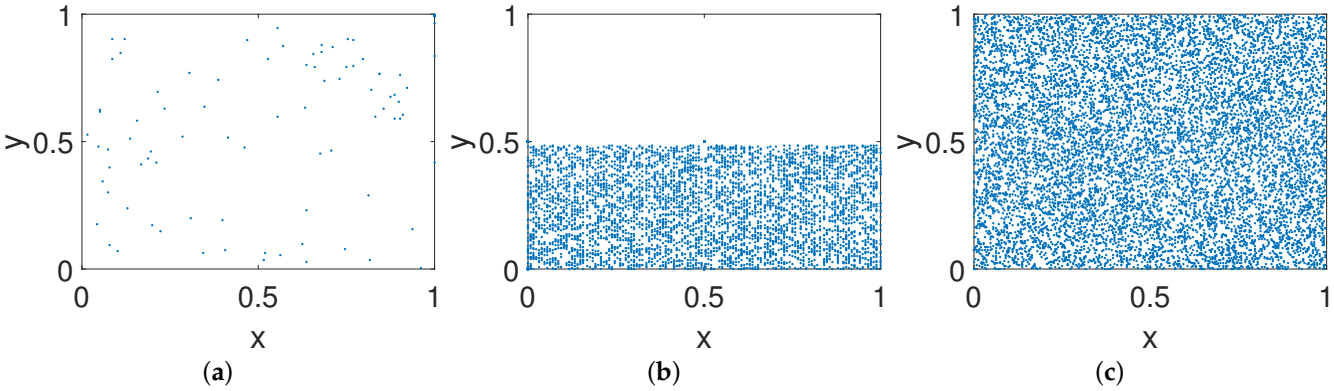

Figure 6. Phase diagrams of systems under three control modes. (**a**) PCB. (**b**) ICB. (**c**) OCB.

3.3.4. Auto-Correlation

We investigated the auto-correlation of output generated from three controlled systems; the result is shown in Figure 7. Obviously, all three control modes performed well in improving the correlation between outputs of the systems due to the delta-like auto-correlation.

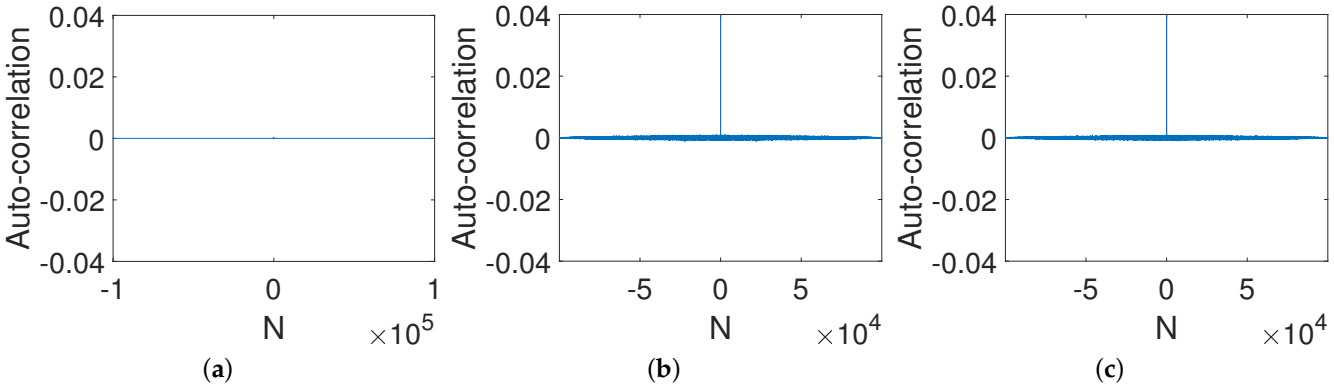

Figure 7. Auto-correlations of systems under three control modes. (**a**) PCB. (**b**) ICB. (**c**) OCB.

3.3.5. Sensitivity to Initial Condition

We are also concerned with the performances of the three control modes in improving the property of sensitivity to the initial conditions of digital systems. Consider two different orbits generated from two slightly different initial values of 0.84 and $0.84 + 2^{-8}$. It can be seen from Figure 8a that two orbits converge after 80 iterations for the PCB system. Figure 8b shows that two orbits overlap for the ICB system. Figure 8c shows that these are two completely different orbits for the OCB system. This means that the OCB system clearly conforms to the characteristics of a chaotic system.

According to the above analysis, it can be concluded that OCB performs better than the other two control modes in improving the dynamical properties of the digital Baker map. The authors of [17] also proved that the disturbance of the output is more effective than the disturbance of the input and the parameters. Therefore, we use the OCB mode to carry out our work in the following sections.

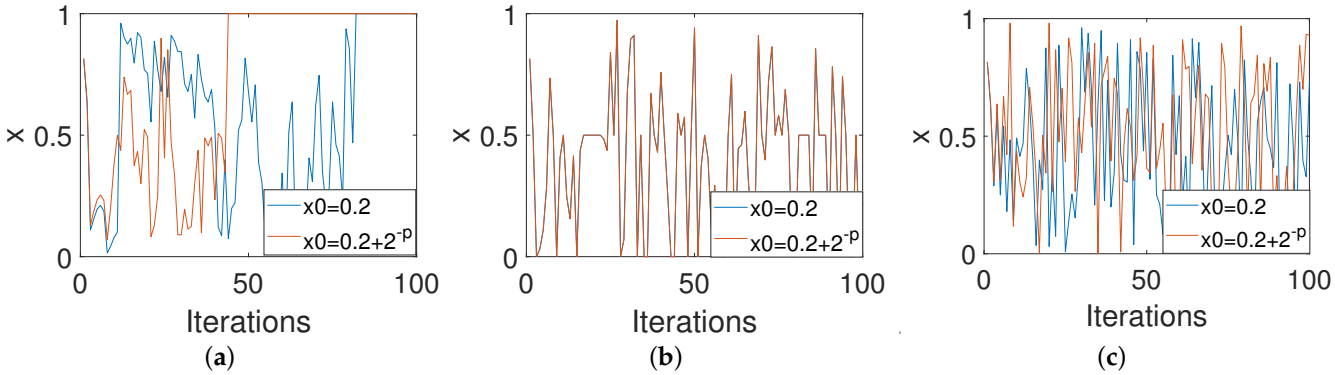

Figure 8. The sensitivity properties to the initial values of systems under three control modes. (**a**) PCB. (**b**) ICB. (**c**) OCB.

3.4. Model Optimization

In this section, we try to add a control gain coefficient d to the OCB mode to obtain the optimal control model. The new system is defined as Equation (10):

$$(x_{i+1}, y_{i+1}) = \begin{cases} (\frac{x_i^*}{u} + d \cdot \tilde{x}_i, y_i^* \cdot u + d \cdot \tilde{y}_i) & \text{mod} 1 \quad 0 < x_i^*, y_i^* \leq u \\ (\frac{x_i^* - u}{1-u} + d \cdot \tilde{x}_i, y_i^* \cdot (1-u) + u + d \cdot \tilde{y}_i) & \text{mod} 1 \quad u < x_i^*, y_i^* \leq 1 \\ x_i^* = FL(x_i) \\ y_i^* = FL(y_i) \end{cases} \tag{10}$$

Set $p = 8$, $x_0 = 0.2$, $y_0 = 0.29$, and $u = 0.49$. We then analyze the dynamical properties of the digital OCB system qualitatively and quantitatively using various of indicators, including the frequency distribution, auto-correlation, cross-correlation, approximate entropy, information entropy, and permutation entropy.

3.4.1. Frequency Distribution

As shown in Figure 9, the distribution seems to depend only on the absolute value of the gain coefficient rather than its sign. Additionally, the distribution becomes almost uniform and essentially does not change anymore when the absolute value of gain coefficient is greater than 0.01.

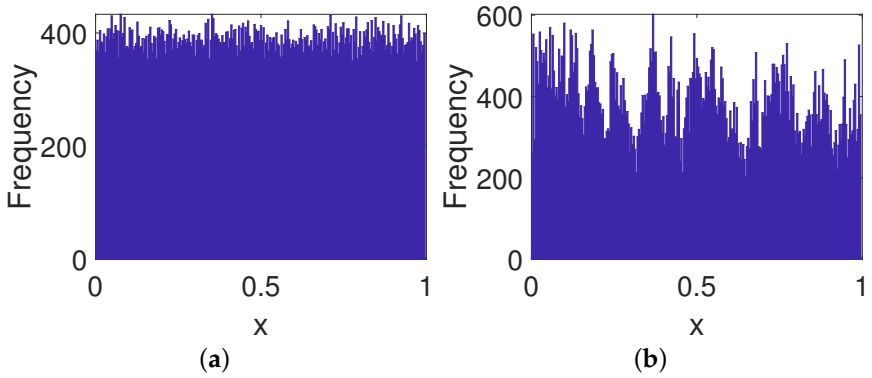

Figure 9. *Cont.*

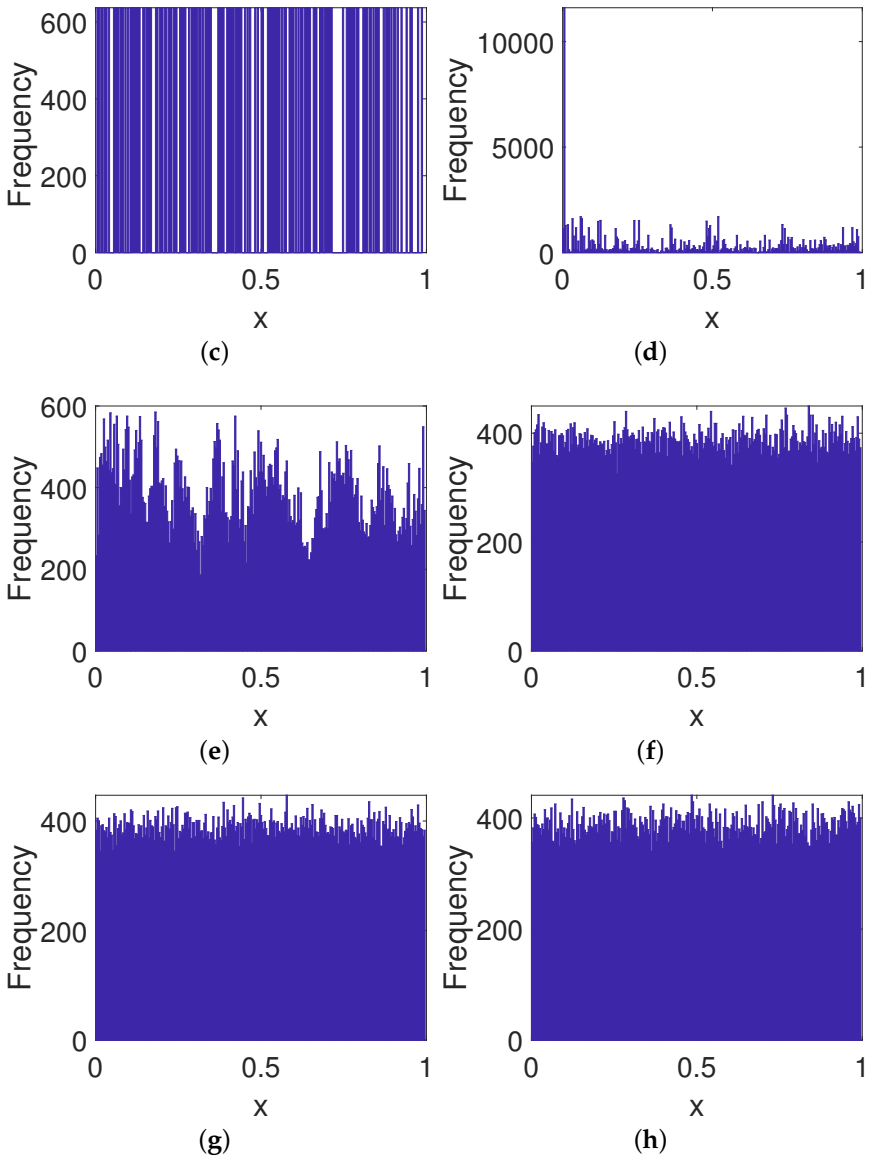

Figure 9. Frequency distributions of digital OCB systems with different gain coefficients. (**a**) $d = -10$. (**b**) $d = -0.001$. (**c**) $d = 0$. (**d**) $d = 0.0001$. (**e**) $d = 0.001$. (**f**) $d = 0.01$. (**g**) $d = 1$. (**h**) $d = 10$.

3.4.2. Auto-Correlation

It is easy to see from Figure 10 that the auto-correlation is close to a delta-like function even through the gain coefficient is small, i.e., $d = 0.0001$ (Figure 10d). In general, the larger the gain coefficient, the more uniform the distribution.

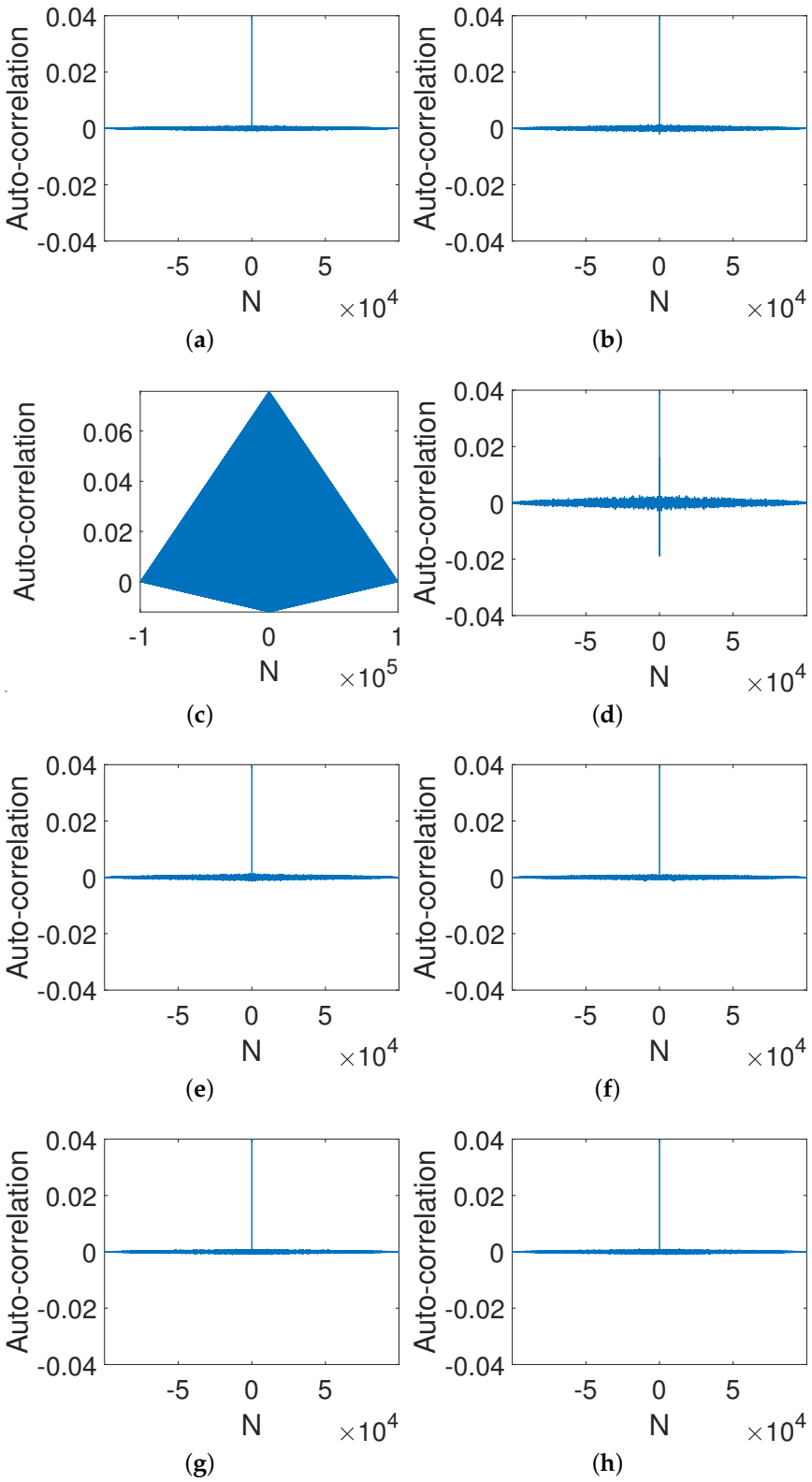

Figure 10. Auto-correlations of digital OCB systems with different gain coefficients. (**a**) $d = -10$. (**b**) $d = -0.001$. (**c**) $d = 0$. (**d**) $d = 0.0001$. (**e**) $d = 0.001$. (**f**) $d = 0.01$. (**g**) $d = 1$. (**h**) $d = 10$.

3.4.3. Cross-Correlation

Figure 11 shows the correlation of two orbits with two slightly different initial values, i.e., $x_0 = 0.2$ and $x_0 = 0.2 + 2^{-p}$. It is clear that the cross-correlation of the two

sequences can be improved as long as the gain coefficient is not zero. Additionally, the cross-correlation reaches almost zero when $d = 10$, as we expected.

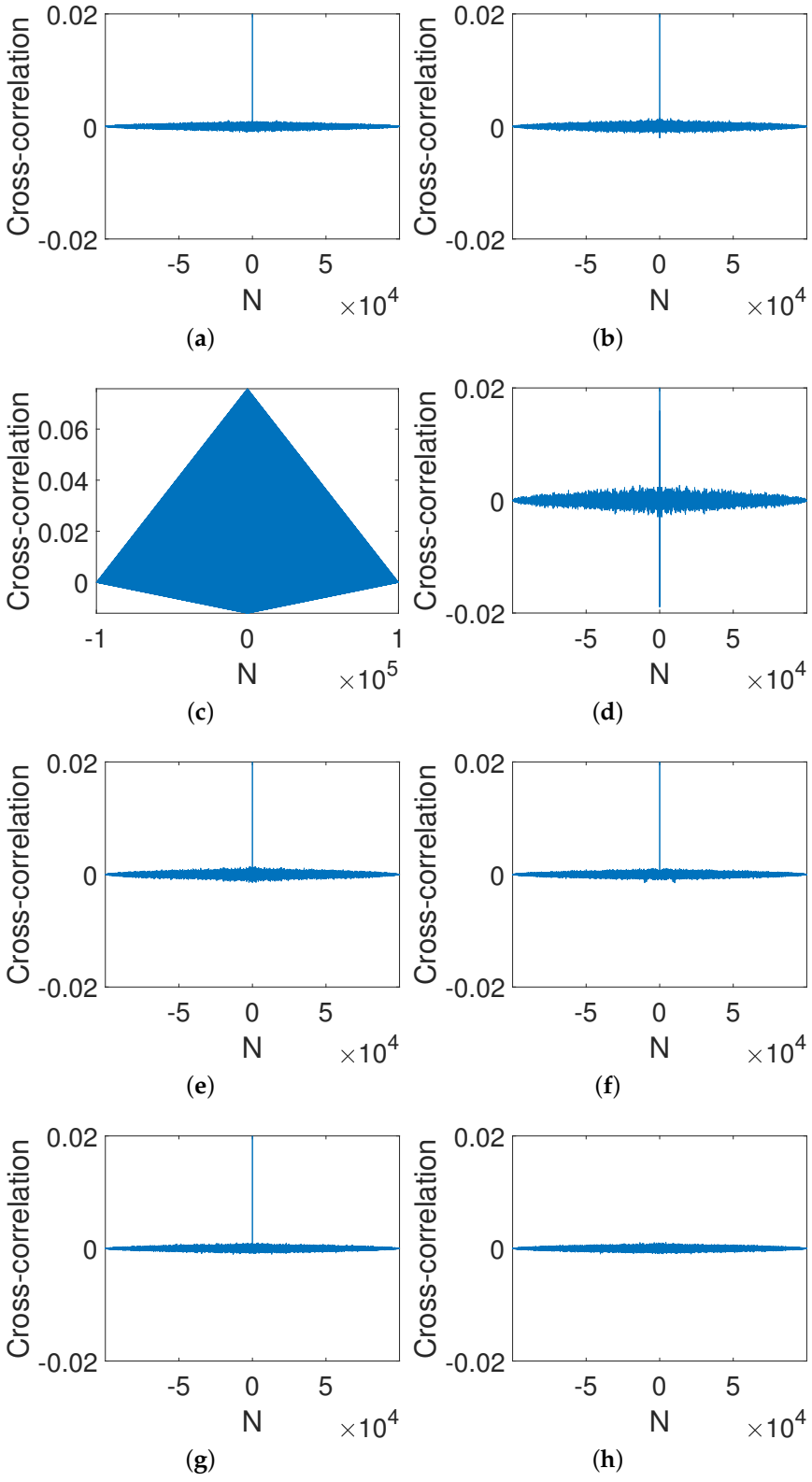

Figure 11. Cross-correlation of digital OCB systems with different gain coefficients. (**a**) $d = -10$. (**b**) $d = -0.001$. (**c**) $d = 0$. (**d**) $d = 0.0001$. (**e**) $d = 0.001$. (**f**) $d = 0.01$. (**g**) $d = 1$. (**h**) $d = 10$.

3.4.4. Approximate Entropy

As shown in Table 1, there is a growing trend in the approximate entropy value with an increase in the gain coefficient d. Specifically, the approximate entropy is just as bad as that of the digital Baker system when d is small (such as for $d = -0.001$ and $d = 0.001$) and exceeds two when the absolute value of d is larger than 10.

Table 1. Approximate entropy of digital OCB systems with different gain coefficients.

d	-10	-0.001	0	0.0001	0.001	0.01	1	10
Approximate Entropy	2.1656	0.6936	0.7002	0.6043	0.6929	1.0552	2.1719	2.1615

3.4.5. Information Entropy

It can be seen from Table 2 that the information entropy was significantly improved (except when $d = 0.0001$) compared with the digital system before control and almost reaches the maximum value 8 under the current computing precision. In this way, the complexity is improved greatly via hybrid output feedback control.

Table 2. Information entropy of digital OCB systems with different gain coefficients.

d	-10	-0.001	0	0.0001	0.001	0.01	1	10
Information Entropy	7.9985	7.9961	7.2946	6.9404	7.9656	7.9980	7.9984	7.9980

3.4.6. Permutation Entropy

Permutation entropy depicts the structural complexity of a time series, and the value is usually between 0 and 1. It can be concluded from Table 3 that the greater the absolute value of the gain coefficient, the closer the entropy is to 1 and the more complex the sequence.

Table 3. Permutation entropy of digital OCB systems with different gain coefficients.

d	-10	-0.001	0	0.0001	0.001	0.01	1	10
Permutation Entropy	0.9994	0.9962	0.7388	0.8571	0.9970	0.9994	0.9995	0.9994

4. Dynamical Performance Comparison

4.1. Performance Comparison of the Systems before and after Control

Set $p = 8$, $x_0 = 0.2$, $y_0 = 0.29$, $u = 0.49$, and $d = 10$. Then, we can observe the dynamical performance of the digital Baker map (2) and the final controlled system (10).

4.1.1. Trajectories and Phase Diagrams

Figure 12 shows the trajectories and phase diagrams of the digital Baker map before and after output feedback control. Obvious short-period behaviors exist for the digital Baker map, but such a phenomenon can be eliminated after control. Meanwhile, the phase space of the digital OCB system is much more complex than that of the system before control. As shown in Figure 12d, there is no obvious structural patterns and seems completely "random" for the phase space of the system after control. In this way, we can say that the structural bias has been eliminated via the OCB mode with the selected control gain coefficient.

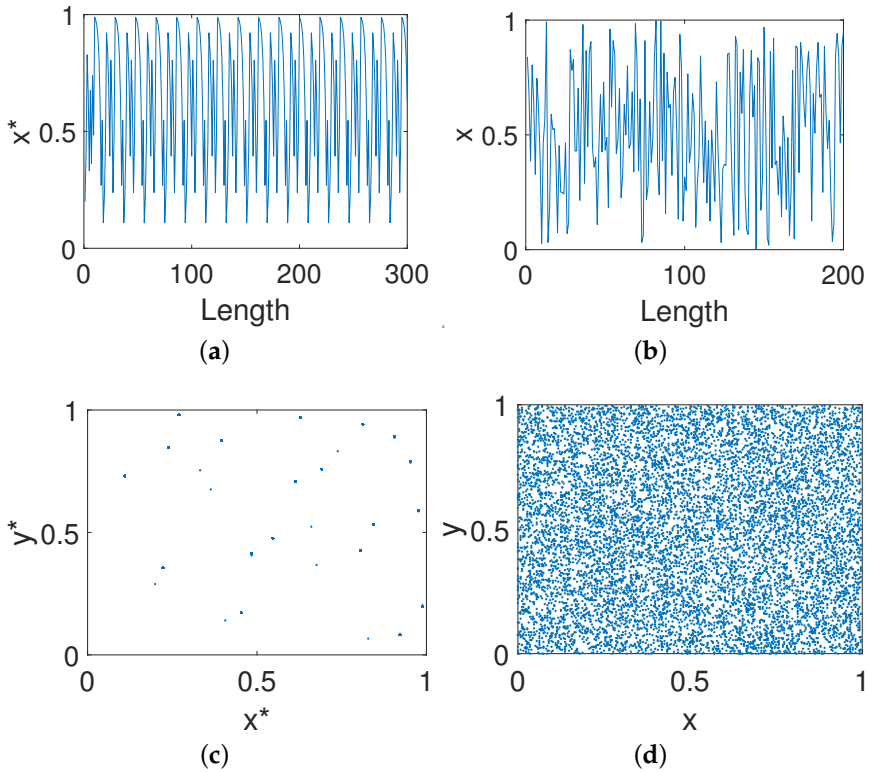

Figure 12. Trajectories and phase diagrams. (**a**) The x-dimensional trajectory of the digital Baker system. (**b**) The x-dimensional trajectory of the controlled system. (**c**) The phase diagram of the digital Baker system. (**d**) The phase diagram of the controlled system.

4.1.2. Frequency Distribution

It can be seen from Figure 13b that the digital Baker map displays almost uniform distribution even with lower precision after output feedback control, which undoubtedly enhances the resistance to statistical analysis.

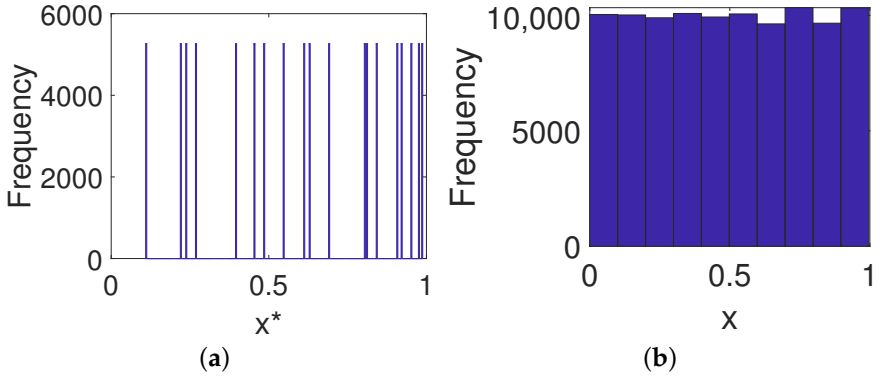

Figure 13. Frequency distribution. (**a**) Digital Baker system. (**b**) The controlled system.

4.1.3. Correlation

It is clear that the original strong correlation of the digital Baker map shown in Figure 14a was eliminated via output feedback control (see Figure 14b). More importantly, the controlled system displays desired correlation functions, i.e., a impulse-like auto-correlation function (see Figure 14c) and a close-to-zero cross-correlation function (see Figure 14d). This implies that the ability of the controlled system to resist a correlation attack can be enhanced greatly.

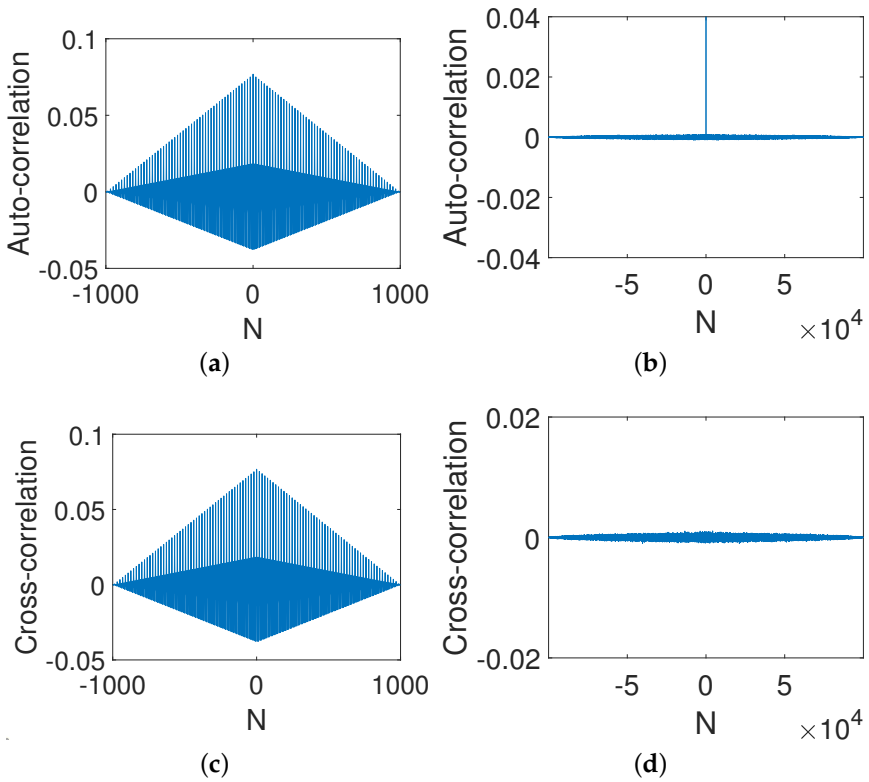

Figure 14. Auto-correlation and cross-correlation. (**a**) Auto-correlation of a digital Baker system. (**b**) Auto-correlation of a controlled system. (**c**) Cross-correlation of a digital Baker system. (**d**) Cross-correlation of a controlled system.

4.1.4. Lyapunov Exponent

Lyapunov exponent refers to the average rate of exponential separation or convergence of two close orbits in phase space over time. It is one of the features used to identify several values of chaotic motion. A negative lyapunov exponent indicates convergence, while a positive lyapunov exponent demonstrates divergence and chaos. Divergence of the exponential law of the orbit means that the almost indistinguishable difference of the initial conditions is displayed quickly, thus quickly losing the possibility of the future state of the system being predicted. A lyapunov exponent greater than 0 means that the system is in a chaotic state. After testing, the maximum lyapunov exponen of our system in the x-direction is 1.518 and the maximum lyapunov exponent in the y-direction is 1.6952. This shows that our system is chaotic and has good initial sensitivity. However, the maximum lyapunov exponent of the digital Baker system is still negative, -0.0011 and -0.0035, respectively, which indicates that it is a periodic system.

4.1.5. Entropy Analysis

We further observe the effect of computing precision and initial value on the complexity of the digital Baker map before and after control, respectively, by using approximate entropy, information entropy, and permutation entropy.

It can be seen from Figure 15 that the approximate entropy becomes twice the original digital one. Meanwhile, all of the information entropy values of the controlled system reach the ideal value of 8 with different initial values, which are much higher than these of the original digital system, as depicted in Figure 16a. Moreover, as shown in Figure 16b, there is a growing trend in the permutation entropy of the original digital system with an increase in precision, but a big deviation from the ideal value of 1 still exists. However, the permutation entropy of the controlled system is close to 1 even with low computing

precisions, which means that the complexity of the controlled system is much higher than that of the original digital system under any circumstances.

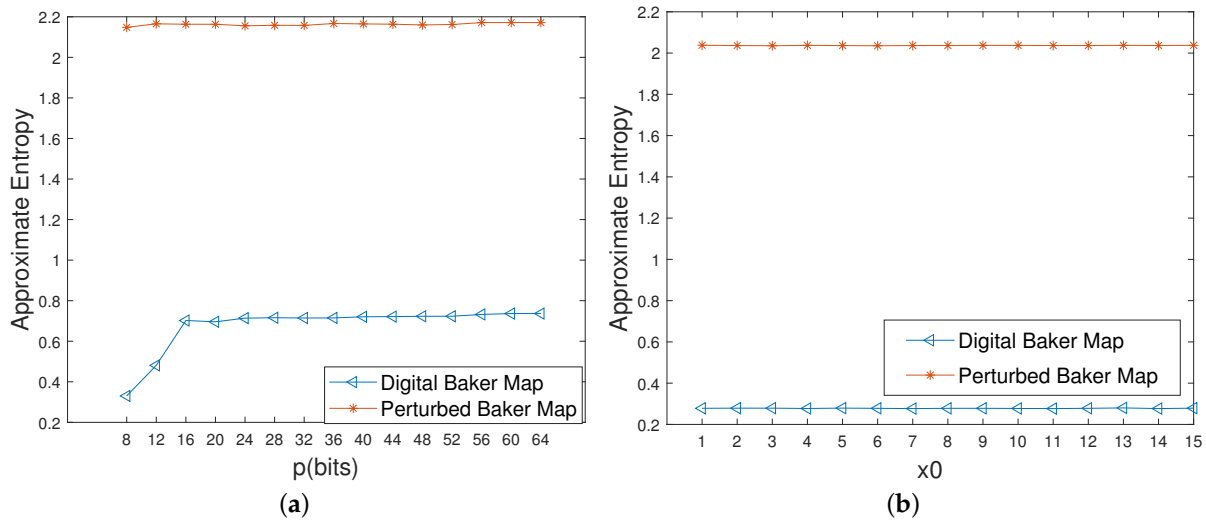

Figure 15. Approximate entropy of the digital Baker maps before and after control. (**a**) Different precisions. (**b**) Different initial values.

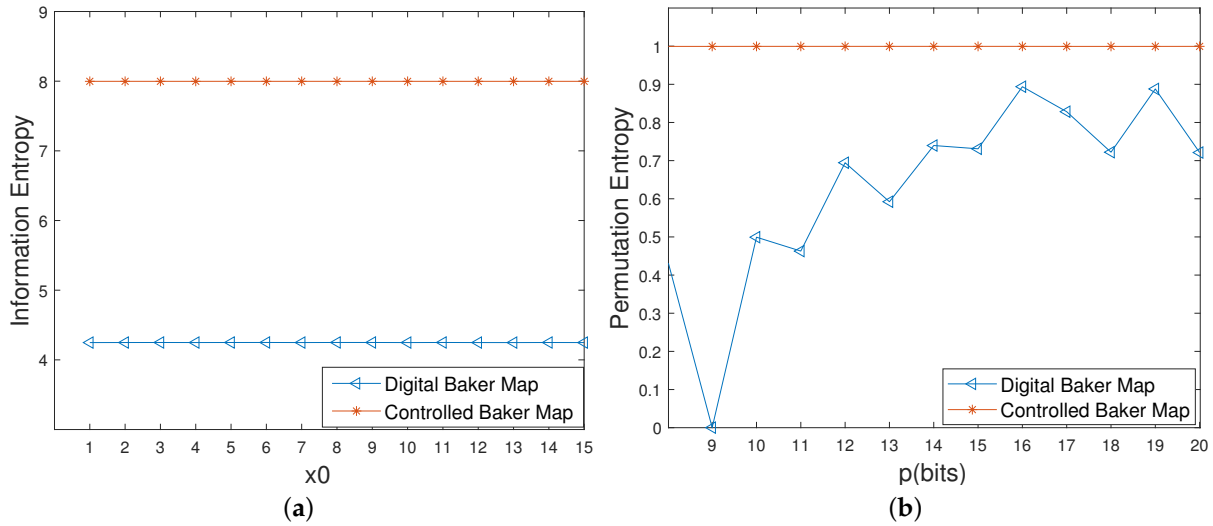

Figure 16. Information entropy and permutation entropy of the digital Baker maps before and after control. (**a**) Information entropies with different initial values. (**b**) Permutation entropies with different precisions.

4.2. Comparison of the Proposed Control Scheme with Existing Methods

Some typical approaches to degradation of the digital chaotic system are introduced here to further show the efficiency of the proposed control method, including the novel double perturbation method (DPM) in [23], the dual perturb method (CCM) in [24], the delay-introducing method (DIM) in [26], the coupled chaotic model (CPM) in [32], the bit reversal method (BRM) in [15], the nested coupling models (2D-SCS) in [6], and the stochastic jumps model (SJM) in [13]. We set the precision to $p = 8$, and we observed the performances of these methods.

4.2.1. Trajectories

Figure 17 shows the trajectories of eight improved systems using existing methods and our scheme. It can be seen from Figure 17d,e that two improved systems converge

to a fixed point 0 after a few hundred iterations via DIM and CPM. Additionally, there are obvious cycle phenomena in two improved systems, BRM and 2D-SCS, as shown in Figure 17f,g. Moreover, there is no discernible difference for other methods in extending the orbit of the system with the precision of 8 bits.

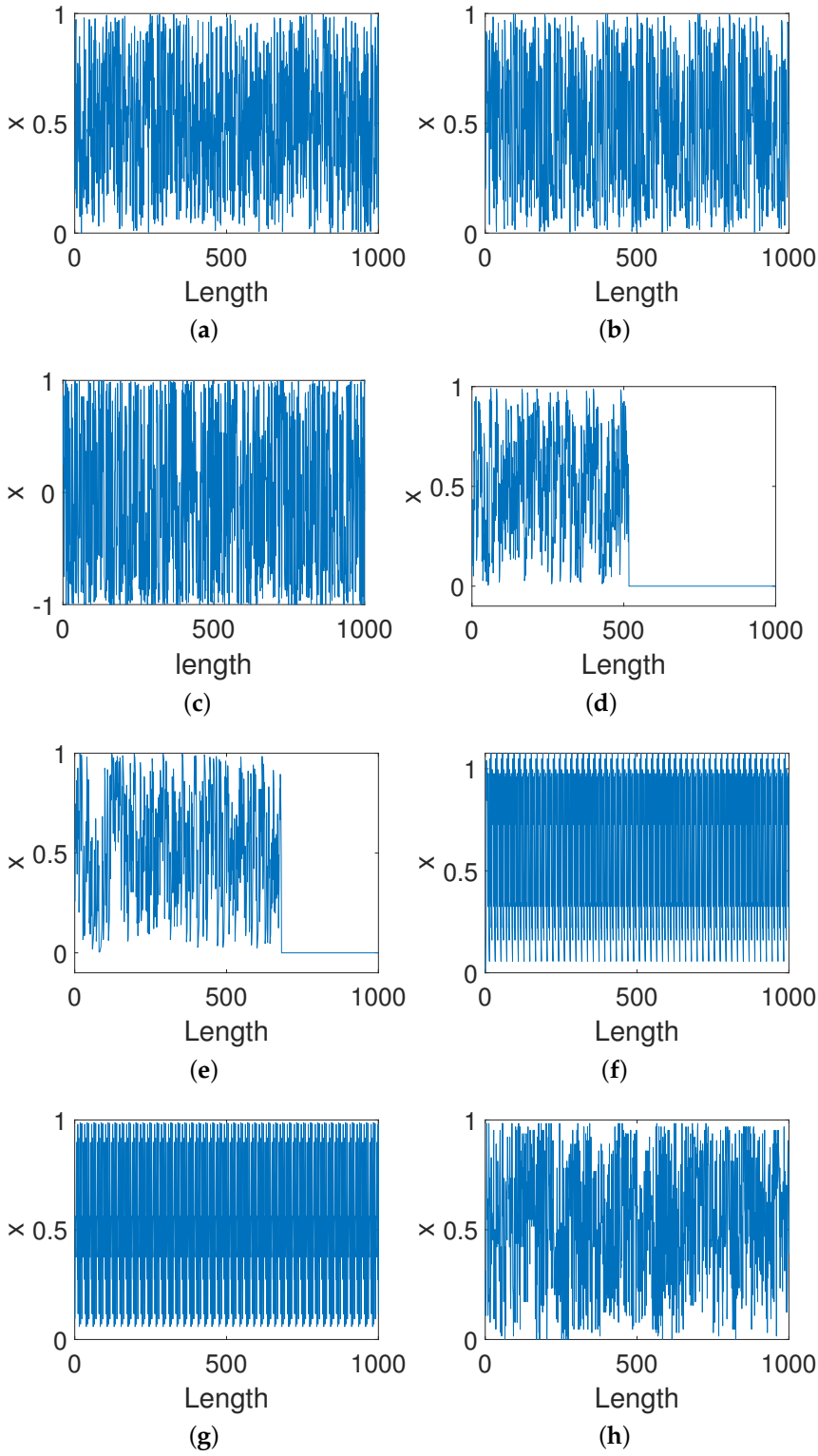

Figure 17. Trajectories of improved systems for different methods. (**a**) Our method. (**b**) DPM. (**c**) CCM. (**d**) DIM. (**e**) CPM. (**f**) BRM. (**g**) 2D-SCS. (**h**) SJM.

4.2.2. Frequency Distribution

It can be observed from Figure 18 that the controlled system obtained using our method has an almost uniform distribution even with lower precision, which greatly improves the ability to resist attacks. By contrast, the improved system for the method of CCM shows a U-shaped distribution, i.e., an almost uniform distribution except for at both ends of the domain. Moreover, the improved systems for other methods show relatively poorer distributions. These significant distribution biases often make the system vulnerable to statistical attacks. Hence, our method has a better performance than others when enhancing the security of digital systems.

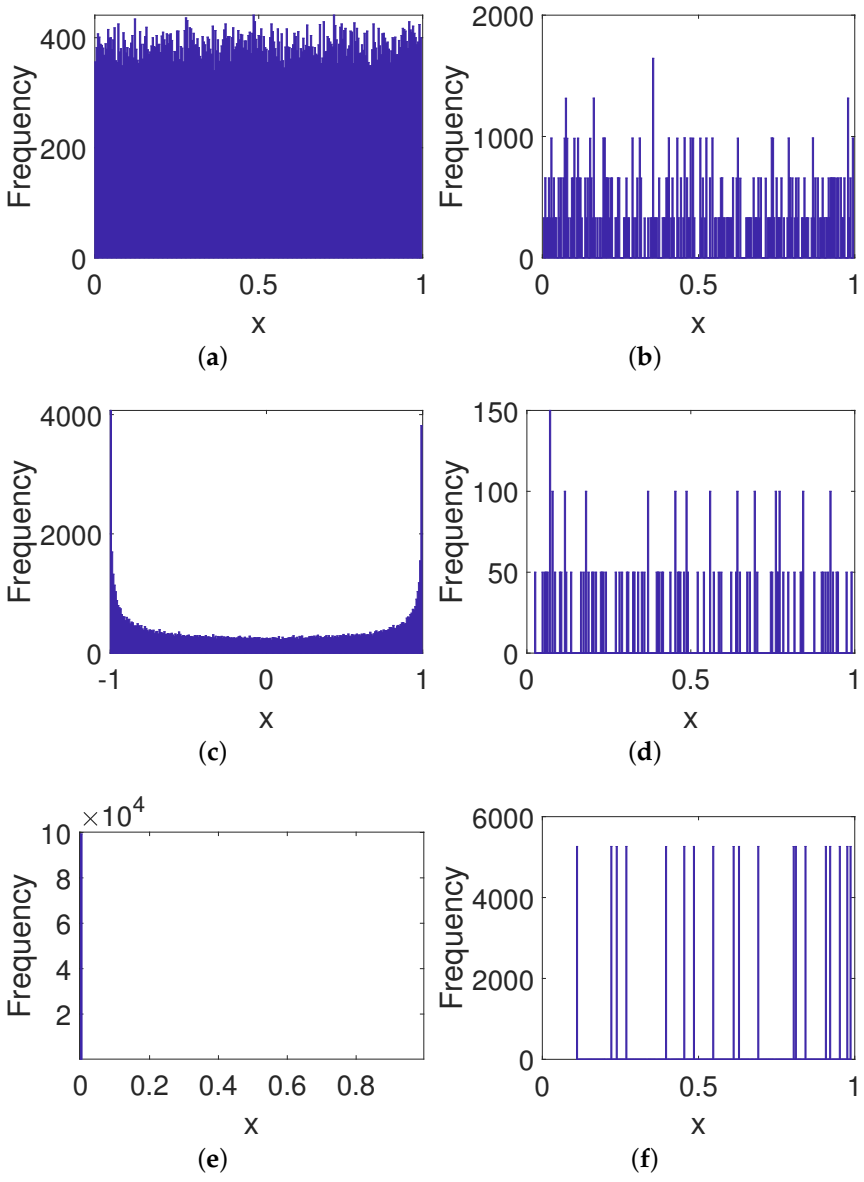

Figure 18. *Cont.*

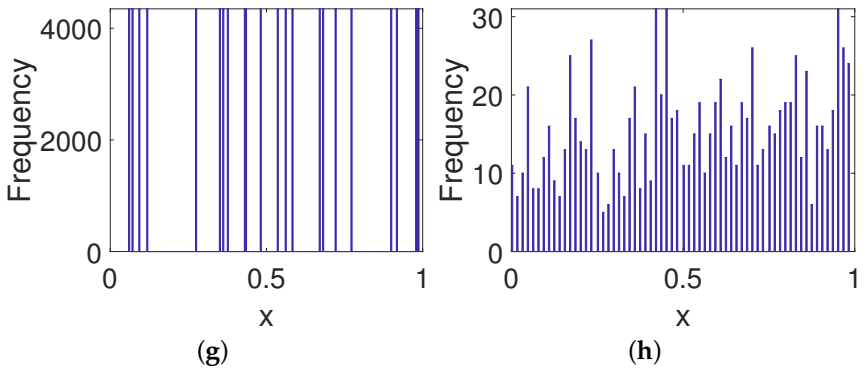

Figure 18. Frequency distributions of improved systems for different methods. (**a**) Our method. (**b**) DPM. (**c**) CCM. (**d**) DIM. (**e**) CPM. (**f**) BRM. (**g**) 2D-SCS. (**h**) SJM.

4.2.3. Phase Diagram

As shown in Figure 19a, the phase diagram of the controlled system for our method is a noise-like diagram, which can improve the security of the system indirectly. Meanwhile, the distributions shown in Figure 19b,c are relatively dense, but both still present specific distribution characteristics. Figures 19d–h are relatively scattered with low ergodicity. Hence, our method has better performance than others when eliminating the structural features of the given systems.

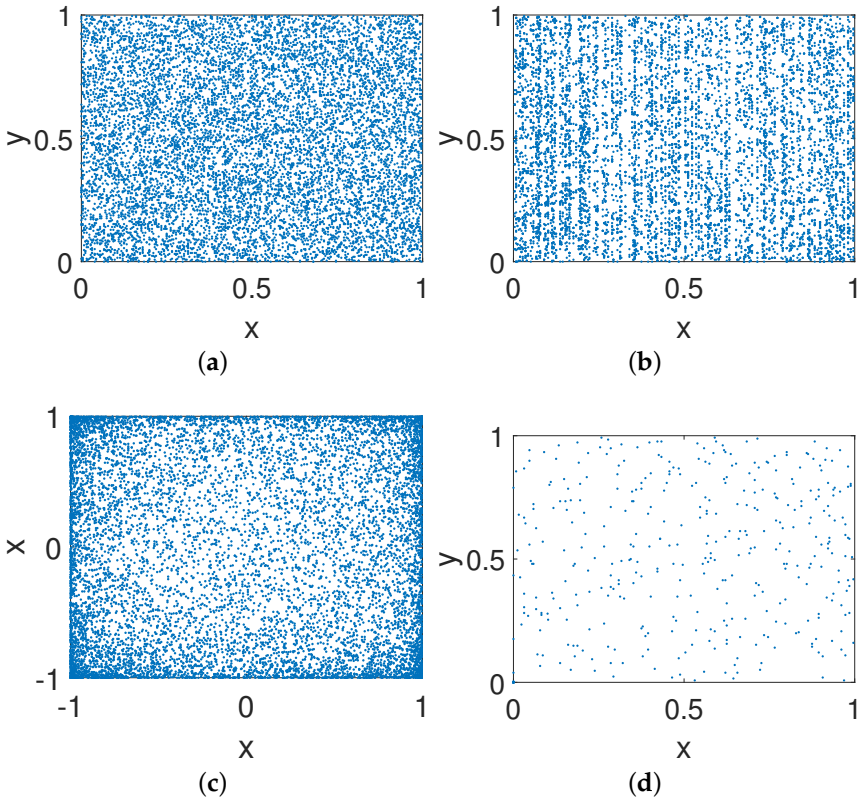

Figure 19. *Cont.*

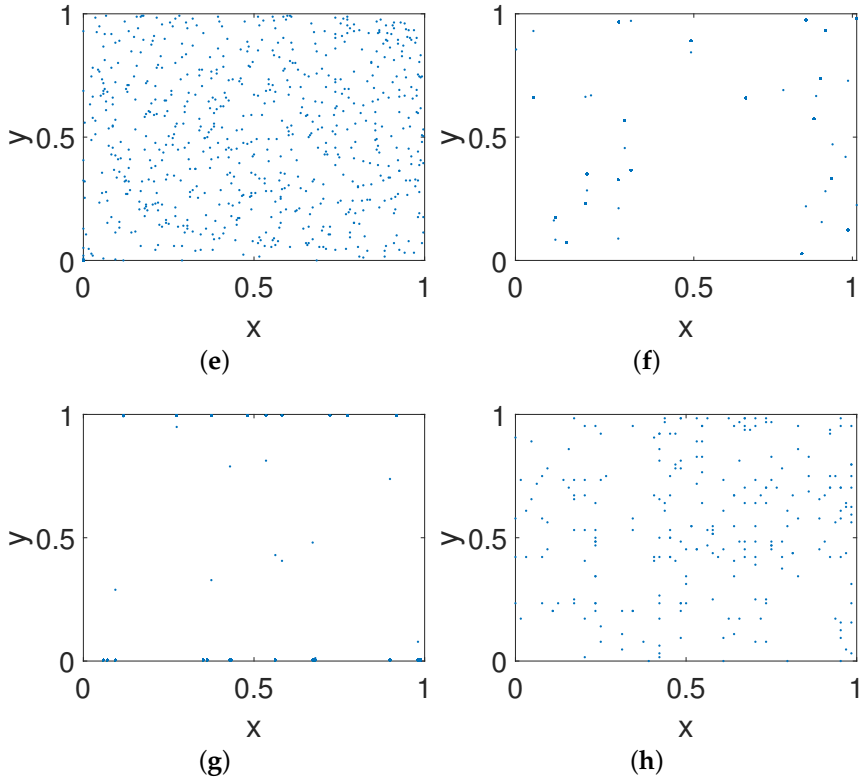

Figure 19. Phase diagrams of improved systems for different methods. (**a**) Our method. (**b**) DPM. (**c**) CCM. (**d**) DIM. (**e**) CPM. (**f**) BRM. (**g**) 2D-SCS. (**h**) SJM.

4.2.4. Entropy Analysis

Given that the increase in the complexity of the system can be used as another effective indicator to evaluate different solutions to degradation, three entropy indicators are applied here to compare the efficiency of different methods.

As shown in Table 4, the information entropy of the controlled system via our method is extremely close to the ideal value of 8 under the precision of 8, which means that our system has greater uncertainty than other systems. It is clear from Figure 20 that the four improved systems using SJM, our method, DPM, and CCM not only have higher approximate entropy values but also entropy values that cannot change much with increasing in computing precision. This means that we can obtain stable entropy values even with lower precisions, which can reduce the implementation cost to some extent. By contrast, the improved systems for the other four methods—BRM, CPM, DIM, and 2D-SCS—display relatively lower and unstable approximate entropy values. Moreover, the permutation entropy of our controlled system is larger than others and extremely close to 1 (see Table 5), which means that the system has higher structural complexity.

Table 4. Information entropy values of improved systems for different methods.

System	Information Entropy
Our method	7.9980
DPM	7.3559
CCM	7.6917
DIM	0.0858
CPM	0.1114
BRM	4.2490
2D-SCS	4.5244
SJM	5.8792

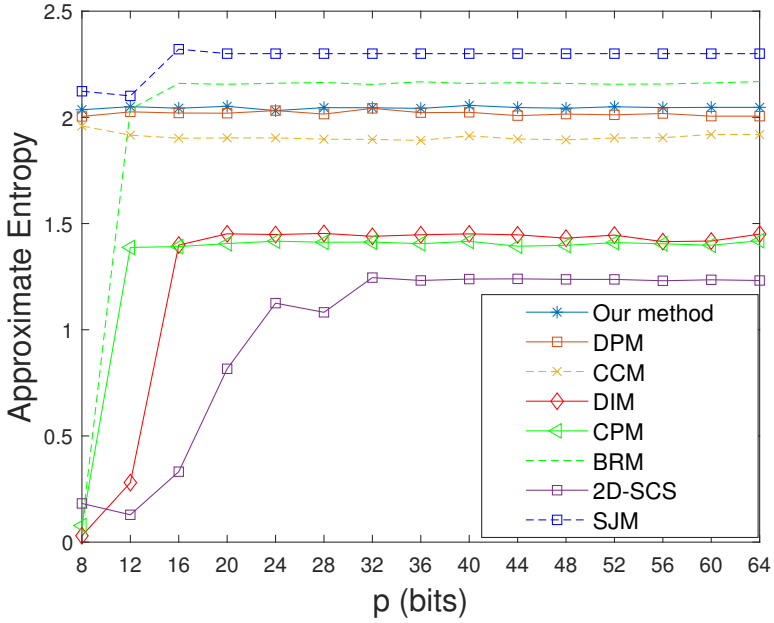

Figure 20. Approximate entropy values of improved systems for different methods.

Table 5. Permutation entropy values of improved systems for different methods.

System	Permutation Entropy
Our method	0.9994
DPM	0.9942
CCM	0.9994
DIM	0.0095
CPM	0.0123
BRM	0.4476
2D-SCS	0.4675
SJM	0.9278

From the above analysis, the conditions we set are relatively harsh, and our scheme can still maintain relatively good chaotic characteristics in this case, which highlights the advantages of our solution. However, it should be mentioned that the implementation complexity may be a little less than that for other methods due to the involvement of a continuous chaotic system. We discuss the balance between performance and implementation costs below.

5. Proposed Pseudorandom Bit Generator

In this section, we propose a new pseudorandom bit generator (PRBG) based on the above digital OCB system (Equation (10)). The binary sequence can be generated by the following:

$$\mathrm{b}(x_i) = \begin{cases} 0 & 0 < x_i \leq 0.5 \\ 1 & otherwise \end{cases} \tag{11}$$

5.1. Security Analysis of PRBG

5.1.1. Key Space

To resist brute-force attacks, the key space should not be less than 2^{128}. In the proposed PRBG, the parameter u and initial conditions x_0 and y_0 can be selected as secret keys. Given that $0 < u < 1, 0 < x_0 < 1, 0 < y_0 < 1$, the key space is approximately equal to $10^{42} \approx 2^{140}$, which is enough to withstand all types of brute-force attacks.

5.1.2. Key Sensitivity Analysis

Suppose that we only change the last digit of one of the keys and the other keys remain unchanged. Then, we observe its impact on the generated PRNG. We used the correlation coefficient and variance ratio to measure key sensitivity (as shown in Tables 6 and 7). We made slight changes to the initial value of the system to generate two PRNGs. Table 6 shows that the correlation between the two PRNGs is very low, and Table 7 shows that their variance ratios are both close to 50%. Then, it turns out that, when the key is slightly changed, the generated sequence is very different from the previous one, which means that it has high key sensitivity when resisting brute-force attack.

Table 6. Correlation coefficients of the generated pseudo-random sequences with slightly different initial keys.

Initial Keys	Changed Keys	Correlation-Coefficient
$x_0 = 0.2$	$x_0' = 0.2 + 2^{-8}$	$C_{xy} = -9.8654 \times 10^{-4}$
$y_0 = 0.29$	$y_0' = 0.29 + 2^{-8}$	$C_{xy} = 0.0011$
$u_0 = 0.49$	$u_0' = 0.49 + 2^{-8}$	$C_{xy} = -0.1111 \times 10^{-4}$

Table 7. Variance ratio when the key is changed by 1 bit.

Parameter	Variance Ratio
x_0	50.04%
y_0	49.93%
u_0	49.96%

5.1.3. Linear Complexity

Linear complexity is an important indicator to measure the randomness of pseudo-random sequences. The expectation of the linear complexity for a PRNG of length n is $n/2$. Figure 21 shows that the linear complexity of a binary sequence is approximately equal to the straight line $n/2$, which means that the generated sequence has a large linear complexity.

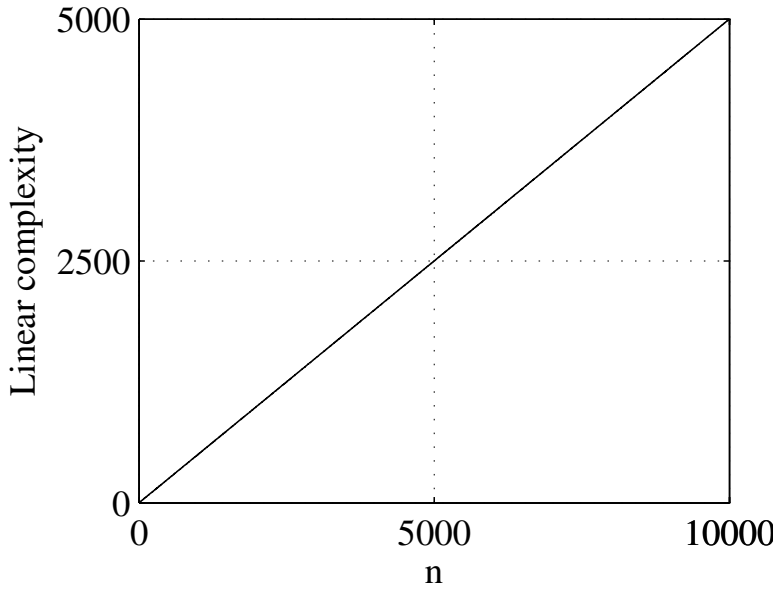

Figure 21. Linear complexity of the generated sequence.

5.1.4. Statistical Test

The NIST test suite is the most popular test suite for evaluating the randomness of pseudo-random sequences. These tests may be useful as a first step in determining whether a generator is suitable for a particular cryptographic application. Table 8 shows the NIST

SP800 test results of the proposed PRNG. The test statistic is used to calculate a p-value that summarizes the strength of the evidence against the null hypothesis. For these tests, each p-value is the probability that a perfect random number generator produces a sequence less random than the sequence that was tested given the type of non-randomness assessed by the test. If a p-value for a test is determined to be equal to 1, then the sequence appears to have perfect randomness. A p-value of zero indicates that the sequence appears to be completely non-random. Table 8 shows that the proposed PRBG successfully passes all of the test indicators in the NIST test suite, which means the proposed PRBG has a high degree of randomness.

Table 8. NIST SP800-22 test results of the proposed PRNG.

Test Index	p-Value	Results
Apen	0.5850	Success
Block-frequency	0.7221	Success
Cumulative-sums	0.5964	Success
FFT	0.8435	Success
Frequency	0.6194	Success
Linear-complexity	0.4982	Success
Longest-run	0.9853	Success
Nonperiodic-templates	0.7746	Success
Overlapping-templates	0.4532	Success
Random-excursion	0.1684	Success
Random-excursion-variant	0.5370	Success
rank	0.4137	Success
runs	0.6041	Success
serial	0.9018	Success
universal	0.1557	Success

5.1.5. Information Entropy Analysis

Table 9 presents the information entropy results with different initial values. Clearly, the information entropy is not affected by the change in initial value. Additionally, it stays close to 8, which means that the PRNG is almost impossible to leak information.

Table 9. Information entropy values of the generated sequences with different initial values.

Initial Values	0.8147	0.0034	0.1270
Information Entropy	7.9998	7.9998	7.9998

6. Conclusions

In this paper, we proposed a control method OCB for a digital Baker map based on feedback control technology. A continuous Chen chaotic system was introduced to control feedback to the digital Baker map to deal with its dynamic degradation. Three different control modes were investigated here, and it was concluded that the output control mode has a far better effect than the other two control modes in the case of low computing precisions. Then, an optimal control model was obtained by analyzing the influence of different gain coefficients on the properties of the controlled system. The optimal external feedback control can not only eliminate the dynamic bias in the system but also allows the digital system to display desirable dynamical properties, including ergodicity, a phase space with no pattern, impulse-like auto-correlation and close-to-zero cross-correlation, and ideal entropy values, etc. Performance comparisons with existing methods further showed the superiority of our method. Finally, we proposed a new PRNG with good randomness.

Author Contributions: Data curation, Y.S.; Project administration, Y.D.; Software, Y.S.; Supervision, Y.D.; Visualization, Y.S. and Y.D.; Writing—original draft, Y.S.; Writing—review & editing, Y.D. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (no.61702554) and the Fundamental Research Funds for the Central Universities, Zhongnan University of Economics and Law (202151424 and 2722021BX025).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lorenz, E.N. Deterministic nonperiodic flow. *J. Atmos. Sci.* **1963**, *20*, 130–141. [CrossRef]
2. Matthews, R. On the derivation of a "Chaotic" encryption algorithm. *Cryptologia* **1989**, *8*, 29–41. [CrossRef]
3. Sun, C.; Wang, E.; Zhao, B. Image Encryption Scheme with Compressed Sensing Based on a New Six-Dimensional Non-Degenerate Discrete Hyperchaotic System and Plaintext-Related Scrambling. *Entropy* **2021**, *23*, 291. [CrossRef]
4. Martínez-Ñonthe, J.; Castañeda-Solís, A.; Díaz-Méndez, A.; Cruz-Irisson, M.; Vazquez-Medina, R. Chaotic block cryptosystem using high precision approaches to tent map. *Microelectron. Eng.* **2012**, *90*, 168–172. [CrossRef]
5. Wheeler, D.D.; Matthews, R.A.J. Supercomputer investigations of a chaotic encryption algorithm. *Cryptologia* **1991**, *15*, 140–152. [CrossRef]
6. Hua, Z.; Zhou, Y.; Bao, B. Two-dimensional sine chaotification system with hardware implementation. *IEEE Trans. Ind. Inform.* **2019**, *16*, 887–897. [CrossRef]
7. Alawida, M.; Samsudin, A.; Teh, J.S.; Alkhawaldeh, R.S. A new hybrid digital chaotic system with applications in image encryption. *Signal Process.* **2019**, *160*, 45–58. [CrossRef]
8. Hua, Z.; Zhou, B.; Zhou, Y. Sine-Transform-Based Chaotic System With FPGA Implementation. *IEEE Trans. Ind. Electron.* **2018**, *65*, 2557–2566. [CrossRef]
9. Hua, Z.; Zhou, B.; Zhou, Y. Sine chaotification model for enhancing chaos and its hardware implementation. *IEEE Trans. Ind. Electron.* **2018**, *66*, 1273–1284. [CrossRef]
10. Zhou, Y.; Hua, Z.; Pun, C.; Philip Chen, C.L. Cascade Chaotic System With Applications. *IEEE Trans. Cybern.* **2015**, *45*, 2001–2012. [CrossRef] [PubMed]
11. Nagaraj, N.; Shastry, M.C.; Vaidya, P.G. Increasing Average Period Lengths by Switching of Robust Chaos Maps in Finite Precision. *Eur. Phys. J. Spec. Top.* **2008**, *165*, 73–83. [CrossRef]
12. Chen, C.; Sun, K.; Peng, Y.; Alamodi, A.O. A novel control method to counteract the dynamical degradation of a digital chaotic sequence. *Eur. Phys. J. Plus* **2019**, *134*, 1–16. [CrossRef]
13. Fan, C.; Ding, Q.; Tse, C.K. Counteracting the dynamical degradation of digital chaos by applying stochastic jump of chaotic orbits. *Int. J. Bifurc. Chaos* **2019**, *29*, 1930023. [CrossRef]
14. Shu-Bo, L.; Jing, S.; Zheng-Quan, X.; Jin-Shuo, L. Digital chaotic sequence generator based on coupled chaotic systems. *Chin. Phys.* **2009**, *18*, 5219. [CrossRef]
15. Alawida, M.; Samsudin, A.; Teh, J.S. Enhanced digital chaotic maps based on bit reversal with applications in random bit generators. *Inf. Sci.* **2020**, *512*, 1155–1169. [CrossRef]
16. Huang, C.; Ding, Q. Performance of Finite Precision on Discrete Chaotic Map Based on a Feedback Shift Register. *Complexity* **2020**, *2020*, 1–12. [CrossRef]
17. Li, S.; Chen, G.; Mou, X. On the dynamical degradation of digital piecewise linear chaotic maps. *Int. J. Bifurc. Chaos* **2005**, *15*, 3119–3151. [CrossRef]
18. Tao, S.; Ruli, W.; Yixun, Y. Perturbance-based algorithm to expand cycle length of chaotic key stream. *Electron. Lett.* **1998**, *34*, 873–874. [CrossRef]
19. Wang, C.; Ding, Q. Theoretical design of controlled digitized chaotic systems with periodic orbit of upper limit length in digital circuit. *Nonlinear Dyn.* **2019**, *98*, 257–268. [CrossRef]
20. Hu, H.; Xu, Y.; Zhu, Z. A method of improving the properties of digital chaotic system. *Chaos Solitons Fractals* **2008**, *38*, 439–446. [CrossRef]
21. Wang, Y.; Wong, K.W.; Liao, X.; Xiang, T.; Chen, G. A chaos-based image encryption algorithm with variable control parameters. *Chaos Solitons Fractals* **2009**, *41*, 1773–1783. [CrossRef]
22. Gábor Domokos, D.S. Ulam's scheme revisited: Digital modeling of chaotic attractors via micro-perturbations. *Discret. Contin. Dyn. Syst.* **2003**, *9*, 859–876. [CrossRef]
23. Liu, L.; Lin, J.; Miao, S.; Liu, B. A Double Perturbation Method for Reducing Dynamical Degradation of the Digital Baker Map. *Int. J. Bifurc. Chaos* **2017**, *27*, 1750103. [CrossRef]
24. Liu, Y.; Luo, Y.; Song, S.; Cao, L.; Liu, J.; Harkin, J. Counteracting Dynamical Degradation of Digital Chaotic Chebyshev Map via Perturbation. *Int. J. Bifurc. Chaos* **2017**, *27*, 1750033. [CrossRef]
25. Lin, F.; Ying, H. State-feedback control of fuzzy discrete-event systems. *IEEE Trans. Syst. Man Cybern.* **2009**, *40*, 951–956.
26. A, L.L.; B, M.S. Delay-introducing method to improve the dynamical degradation of a digital chaotic map. *Inf. Sci.* **2017**, *396*, 1–13.
27. Hu, H.; Deng, Y.; Liu, L. Counteracting the dynamical degradation of digital chaos via hybrid control. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 1970–1984. [CrossRef]

28. Deng, Y.; Hu, H.; Xiong, N.; Xiong, W.; Liu, L. A general hybrid model for chaos robust synchronization and degradation reduction. *Inf. Sci.* **2015**, *305*, 146–164. [CrossRef]
29. Peng, C.; Tian, Y.C.; Yue, D. Output Feedback Control of Discrete-Time Systems in Networked Environments. *IEEE Trans. Syst. Man Cybern.* **2011**, *41*, 185–190. [CrossRef]
30. Deng, Y.; Hu, H.; Xiong, W.; Xiong, N.N.; Liu, L. Analysis and design of digital chaotic systems with desirable performance via feedback control. *IEEE Trans. Syst. Man Cybern. Syst.* **2015**, *45*, 1187–1200. [CrossRef]
31. Zhang, Y. The unified image encryption algorithm based on chaos and cubic S-Box. *Inf. Sci.* **2018**, *450*, 361–377. [CrossRef]
32. Liu, L.; Liu, B.; Hu, H.; Miao, S. Reducing the dynamical degradation by bi-coupling digital chaotic maps. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850059. [CrossRef]
33. Chen, G.; Ueta, T. Yet another chaotic attractor. *Int. J. Bifurc. Chaos* **1999**, *9*, 1465–1466. [CrossRef]
34. Csernák, G. Quantization-induced control error in a digitally controlled system. *Nonlinear Dyn.* **2016**, *85*, 2749–2763. [CrossRef]
35. Kuperin, Y.A.; Pyatkin, D.A. Two-Dimensional Chaos: The Baker Map Under Control. *J. Math. Sci.* **2005**, *128*, 2798–2802. [CrossRef]
36. Csernák, G.; Gyebrószki, G.; Stépán, G. Multi-Baker Map as a Model of Digital PD Control. *Int. J. Bifurc. Chaos* **2016**, *26*, 1650023. [CrossRef]