electronics

MDPI

Article

Design of High-Security USB Flash Drives Based on Chaos Authentication

Teh-Lu Liao [1], Pei-Yen Wan [1], Pin-Cheng Chien [1], Yi-Chieh Liao [2], Liang-Kai Wang [3] and Jun-Juh Yan [4,*]

1 Department of Engineering Science, National Cheng Kung University, Tainan 701, Taiwan; tlliao@mail.ncku.edu.tw (T.-L.L.); s16637113@stu.edu.tw (P.-Y.W.); s12115125@stu.edu.tw (P.-C.C.)
2 Department of Computer Science and Information Engineering, Chang Gung University, Taoyuan 333, Taiwan; liao1230ho123@gmail.com
3 Department of Electrical Engineering, National Yunlin University of Science and Technology, Yunlin 640, Taiwan; m10512023@yuntech.edu.tw
4 Department of Computer and Communication, Shu-Te University, Kaohsiung 824, Taiwan
* Corresponding Author: jjyan@stu.edu.tw; Tel: +886-7-6158000 (ext. 4806)

Received: 13 May 2018; Accepted: 24 May 2018; Published: 26 May 2018

Abstract: This paper aims to propose a novel design of high-security USB flash drives with the chaos authentication. A chaos authentication approach with the non-linear encryption and decryption function design is newly proposed and realized based on the controller design of chaos synchronization. To complete the design of high-security USB flash drives, first, we introduce six parameters into the original Henon map to adjust and obtain richer chaotic state responses. Then a discrete sliding mode scheme is proposed to solve the synchronization problem of discrete hyperchaotic Henon maps. The proposed sliding mode controller can ensure the synchronization of the master-slave Henon maps. The selection of the switching surface and the existence of the sliding motion are also addressed. Finally, the obtained results are applied to design a new high-security USB flash drive with chaos authentication. We built discrete hyperchaotic Henon maps in the smartphone (master) and microcontroller (slave), respectively. The Bluetooth module is used to communicate between the master and the slave to achieve chaos synchronization such that the same random and dynamical chaos signal can be simultaneously obtained at both the USB flash drive and smartphone, and pass the chaos authentication. When users need to access data in the flash drive, they can easily enable the encryption APP in the smartphone (master) for chaos authentication. After completing the chaos synchronization and authentication, the ARM-based microcontroller allows the computer to access the data in the high-security USB flash drive.

Keywords: chaos synchronization; Henon map; discrete sliding mode control; high-security USB flash drive; chaos authentication

1. Introduction

As USB flash drive development has matured, it has become the popular device for data file storage. Because USB flash drives are small and easy to carry, users can enjoy greater mobility. However, the risk of information security has also risen relatively. It is well known, from the perspective of information security, that the principle of mutual exclusivity between safety and convenience is often mentioned; the more convenient, the more insecure, and the more secure, the more inconvenient. As a result, easy-to-use products like USB flash drives must be classified as high-security risk products and many businesses are also aware that USB flash drives are the culprit for data breaches. Therefore, many vendors take advantage of this opportunity and launch

their encrypted USB flash drives. From the current market, the common encryption USB flash drives can be classified as software-based and hardware-based encryption. For software-based encryption, there exists some disadvantages including the inconvenience of installing specified encryption software and poor performance compared with hardware encryption products. Configuration complexity and the time needed to set up the software are also disadvantages [1]. For hardware-based encrypted USB flash drives, it is generally implemented with a high-price hardware security module responsible for data encryption. Therefore, hardware-based encrypted USB flash drives offer better security and data access speed than software-based one. However, it is very inconvenient because the user still needs to remember to input a password each time before using the device.

To solve the above problems, we present a novel chaos authentication to construct high-security USB flash drives and cancel the traditional encrypted USB flash drives complex encryption and decryption operation. It is well known that the chaotic system is a very complex nonlinear system. Chaos properties, such as broadband noise-like waveform, and depending on the sensitivity of the system's precise initial conditions, etc., have generally been studied. These properties offer some advantages for applications in many important research topics, for example, secure communication [2–4], chemical reactions, and artificial neural networks [5,6]. For applications, synchronization of master-slave chaotic systems is very important; therefore, many control approaches have been proposed to solve the problem of synchronization for chaotic systems, such as the backstepping technique [7,8], fuzzy sliding mode control and optimal control [9–11], etc. Recently, due to the remarkable progress of digital signal processing (DSP) technology, the researchers often implement the controllers by the microcontroller with DSP technology for better reliability, lower cost, smaller size, more flexibility and better performance. Therefore, research into discrete-time control has become intensified in recent years [12–14].

Motivated by the aforementioned, this study aims to design a discrete-time sliding mode control and utilize the synchronization of the master-slave Henon maps to provide dynamical random numbers for the chaos authentication. In order to obtain the richer chaotic state responses for authentication, we first introduce six parameters into the original Henon map. Then according to the sliding mode control design, a discrete controller is proposed to cope with the synchronization problem of discrete master-slave hyperchaotic Henon maps [15]. The selection of the switching surface and the existence of the discrete sliding manifold are also addressed. After achieving the chaos synchronization, a chaos authentication approach based on the non-linear encryption and decryption function design are proposed. Then the obtained results are applied to design a new high-security USB flash drive. In this design, we built discrete hyperchaotic Henon maps in the microcontroller (slave) and the smartphone (master), respectively. The new chaos authentication is to authenticate the dynamic random numbers generated by the master chaotic system in the user's USB flash drive and the user's smartphone. Such authentication methods not only solve the defect in the traditional encryption USB flash drive which is easy to crack when inputting a password but also eliminates the inconvenience that the user needs to remember and input the password. To our best knowledge, this is an unprecedented authentication method in the market.

This paper is organized as follows. In Section 2, we first formulate the problem of chaos synchronization. The discrete sliding mode control (DSMC) design for synchronization of discrete master-slave hyperchaotic Henon Maps and the experimental simulations are proposed. In Section 3, the high-security USB flash drive based on chaos authentication is constructed. The structure of USB flash drives and the authentication mechanism between USB flash drive and user's smartphone are also addressed. Finally, a concise conclusion and future work are given in Section 4.

2. Synchronization of Discrete Hyperchaotic Henon Maps

In this paper, we will discuss the design of a high-security USB flash drive based on the technology of chaos synchronization. Before constructing the design, the first problem undertaken was to solve the synchronization problem of the master-slave hyperchaotic Henon Maps. Then we aim to propose

a DSMC to solve the chaos synchronization problem. In the following, we first introduce some parameters into the original Henon map, such that richer chaotic state responses can be obtained for authentication. The dynamic equations of the hyperchaotic Henon Maps [15] are described as follows:

$$x_1(k+1) = 1.76 - x_2^2(k) - 0.1x_3(k)x_2(k+1) = x_1(k)x_3(k+1) = x_2(k) \tag{1}$$

where, $x_i, i = 1, 2, 3$ is the state variable. The strange attractor of Equation (1) is shown as Figure 1.

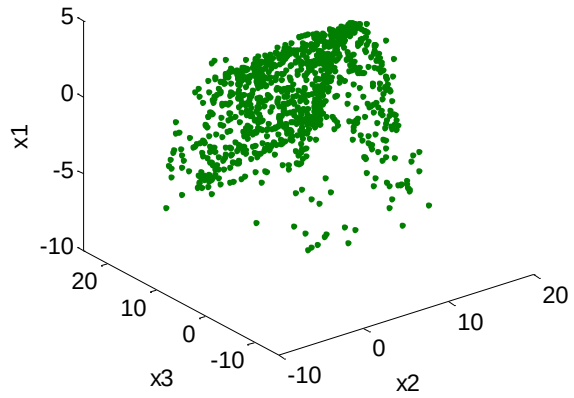

Figure 1. Strange attractor of hyperchaotic system.

In order to adjust the amplitude and DC level for obtaining richer chaotic responses, we let:

$$y_1(k) = a_1x_1(k) + d_1y_2(k) = a_2x_2(k) + d_2y_3(k) = a_3x_3(k) + d_3 \tag{2}$$

where, $a_i, i = 1, 2, 3$ is the amplitude parameters for adjusting the amplitudes and $d_i, i = 1, 2, 3$ are those for DC level. From Equation (2), we can get:

$$x_i(k) = \frac{y_i(k) - d_i}{a_i}; i = 1, 2, 3 \tag{3}$$

Substituting Equation (3) into Equation (1) yields a new type of hyperchaotic system that can be modulated as shown in Equation (4):

$$y_1(k+1) = \lambda_1 y_2^2(k) + \lambda_2 y_2(k) + \lambda_3 y_3(k) + \lambda_4 y_2(k+1) = \beta_1 y_1(k) + \beta_2 y_3(k+1) = \eta_1 y_2(k) + \eta_2 \tag{4a}$$

where:

$$\begin{gathered} \lambda_1 = -\frac{a_1}{a_2^2}, \lambda_2 = \frac{2a_1d_2}{a_2^2}, \lambda_3 = -\frac{0.1a_1}{a_3} \\ \lambda_4 = a_1\left(1.76 - \frac{d_2^2}{a_2^2} + 0.1\frac{a_1d_3}{a_3}\right) + d_1 \\ \beta_1 = \frac{a_2}{a_1}, \beta_2 = -\frac{a_2}{a_1}d_1 + d_2 \\ \eta_1 = \frac{a_3}{a_2}, \eta_2 = -\frac{a_3}{a_2}d_2 + d_3 \end{gathered} \tag{4b}$$

From the above inferences, we have introduced a hyperchaotic Henon Map with a variable amplitude and DC levels. With six configurable parameters, we can arbitrarily adjust the generation of random numbers to increase the complexity of random numbers. In the following, we show the simulation analysis. When we give the modulation parameters $a_1 = 1, a_2 = 2, a_3 = 3, d_1 = 2, d_2 = 4, d_3 = 6$. The simulation results are shown in Figures 2 and 3.

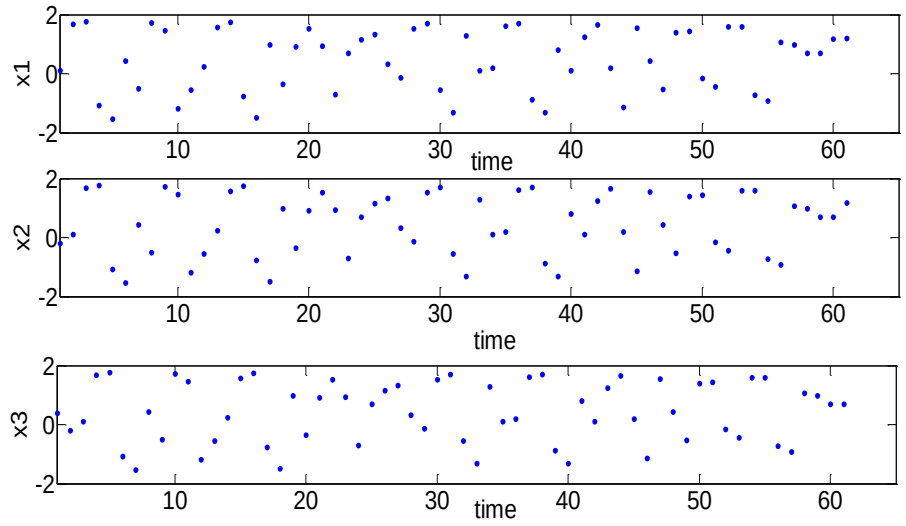

Figure 2. State responses of the original Henon Map system.

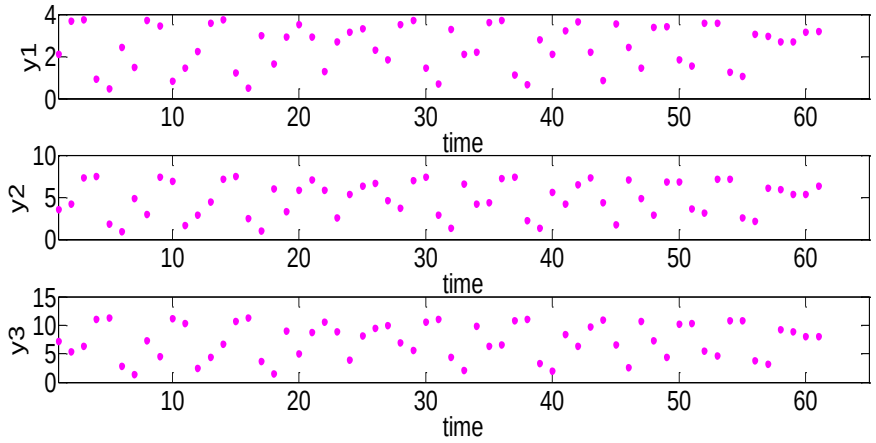

Figure 3. State responses of the adjusted Henon Map system.

As mentioned above, synchronization of the master and slave chaotic systems are a key technology for generating identical random signals for authentication. The master-slave hyperchaotic Henon maps are defined as below, respectively.

Master system:

$$x_1(k+1) = \lambda_1 x_2^2(k) + \lambda_2 x_2(k) + \lambda_3 x_3(k) + \lambda_4 x_2(k+1) = \beta_1 x_1(k) + \beta_2 x_3(k+1) = \eta_1 x_2(k) + \eta_2 \quad (5)$$

Slave system:

$$y_1(k+1) = \lambda_1 y_2^2(k) + \lambda_2 y_2(k) + \lambda_3 y_3(k) + \lambda_4 + u(k) y_2(k+1) = \beta_1 y_1(k) + \beta_2 y_3(k+1) = \eta_1 y_2(k) + \eta_2 \quad (6)$$

where, x_i and y_i are the state vectors of the master system and the slave system, respectively. The control input $u(k)$ is introduced to achieve synchronization. By defining the error vector $e_i(k) = y_i - x_i(k), i = 1, 2, 3$, the dynamics of synchronization error can be described as:

$$e_1(k+1) = \lambda_1 \left(y_2^2(k) - x_2^2(k) \right) + \lambda_2 e_2(k) + \lambda_3 e_3(k) + u(k) e_2(k+1) = \beta_1 e_1(k) e_3(k+1) = \eta_1 e_2(k) \quad (7)$$

From the error dynamics (Equation (7)), it is clear that the synchronization problem becomes the equivalent problem of stabilization of the error dynamics (Equation (7)). Therefore, to synchronize

the master–slave chaotic systems defined in Equations (5) and (6), we must design a sliding mode controller such that the resulting error vector satisfies:

$$\lim_{k\to\infty} \| \, e_1(k) \; e_2(k) \; e_3(k) \, \| = 0 \tag{8}$$

To make master–slave hyperchaotic system, Equations (5) and (6) must reach synchronization, we must design a robust synchronization controller. A discrete sliding mode control (DSMC) design is used here. To complete the control design, firstly the switching surface is given as:

$$\mathrm{s}(k) = e_1(k) + c_1 e_2(k) + c_2 e_3(k) \tag{9}$$

Suppose $\mathrm{s}(k) = 0$ (in the sliding manifold), we can get:

$$e_1(k) = -c_1 e_2(k) - c_2 e_3(k) \tag{10}$$

Substituting (9) into (7), we obtain:

$$\begin{bmatrix} e_2(k+1) \\ e_3(k+1) \end{bmatrix} = \begin{bmatrix} -c_1\beta_1 & -c_2\beta_1 \\ \eta_1 & 0 \end{bmatrix} \begin{bmatrix} e_2(k) \\ e_3(k) \end{bmatrix} = Me(k) \tag{11}$$

From Equation (11), we can see that if we choose c_1, c_2 such that the eigenvalues of M in Equation (11) can be limited in the unit circle, i.e., $|\lambda_i(M)| < 1$, then e_2, e_3 can converge to zero. Furthermore, according to $e_1(k) = -c_1 e_2(k) - c_2 e_3(k)$, we obtain $e_1 = 0$ when e_2, e_3 have converged to zero.

For DSMC design, in order to ensure that the system can hit the switching surface and enter the sliding manifold ($\mathrm{s}(k) = 0$), the controller is designed as follows:

Since:

$$\begin{gathered} s(k+1) \\ = e_1(k+1) + c_1\beta_1 e_2(k+1) + c_2 e_3(k+1) \\ = \lambda_1(y_2(k) + x_2(k))e_2(k) + \lambda_2 e_2(k) + \lambda_3 e_3(k) + u(k) + c_1\beta_1 e_1(k) + c_2\eta_1 e_2(k) \end{gathered} \tag{12}$$

let the controller be:

$$u(k) = -(\lambda_1(y_2(k) + x_2(k))e_2(k) + \lambda_2 e_2(k) + \lambda_3 e_3(k) + c_1\beta_1 e_1(k) + c_2\eta_1 e_2(k)) + \alpha s(k) \tag{13}$$

Substituting Equation (13) into Equation (12) yields:

$$s(k+1) = \alpha s(k) \tag{14}$$

Then if $|\alpha| < 1$, then the system will smoothly enter the sliding mode. According to the discussion above, when in the sliding mode, we can easily ensure the stability of the error system (Equation (7)) and then the controlled master-slave hyperchaotic systems can be synchronized. When implementing the synchronization controller $u(k)$ (Equation (13)), in order to reduce the data transmission and promote the security, we divide the control input $u(k)$ into two parts of $u_m(k)$ and $u_s(k)$ satisfying $u(k) = -(\lambda_1(y_2(k) + x_2(k))e_2(k) + \lambda_2 e_2(k) + \lambda_3 e_3(k) + c_1\beta_1 e_1(k) + c_2\eta_1 e_2(k)) + \alpha s(k) = u_m(k) + u_s(k)$, where $u_m(k)$ is the combination of the states of the master systems and $u_s(k)$ is the combination of the state signal of the slave system.

In the following, we give an example to demonstrate the effectiveness of the proposed control method. The simulation results with initial conditions of $x_1 = 0.5$, $x_2 = -0.3$, $x_3 = 0.4$, $y_1 = -0.3$, $y_2 = -0.1$, $y_3 = 0.8$, $\alpha = -0.5$, $a_1 = 3$, $a_2 = 5$, $a_3 = 6$, $d_1 = 0.2$, $d_2 = 0.5, d_3 = 0.7$ are shown in Figures 4 and 5. Here, the eigenvalues of M are $(0.9, 0.8)$ satisfying $|\lambda_i(M)| < 1$ with $c_1 = -1.02$, $c_2 = 0.36$. Figure 4 shows the state response of controlled chaotic systems. Figure 5 depicts the

responses of the switching surface, control input and the synchronization error. It can be seen that the synchronization errors are regulated to zero. From the simulation results, it shows the proposed DSMC (Equation (13)) works well and the controlled master–slave hyperchaotic systems are synchronized asymptotically.

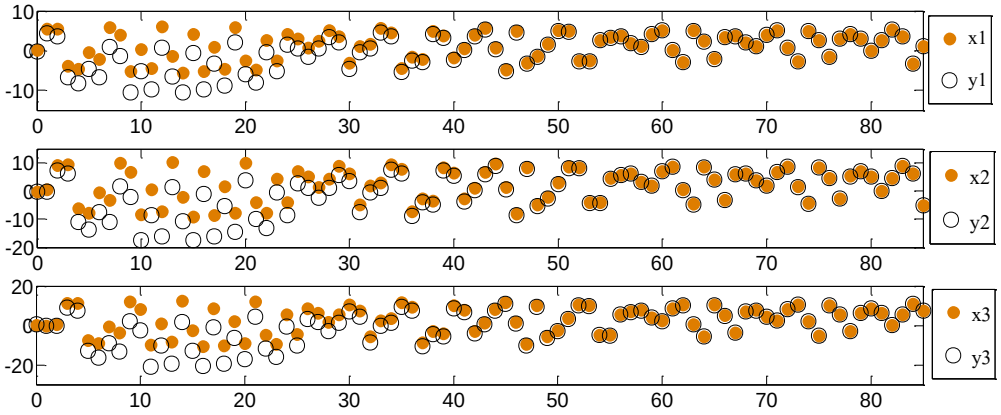

Figure 4. State responses of the controlled master–slave system.

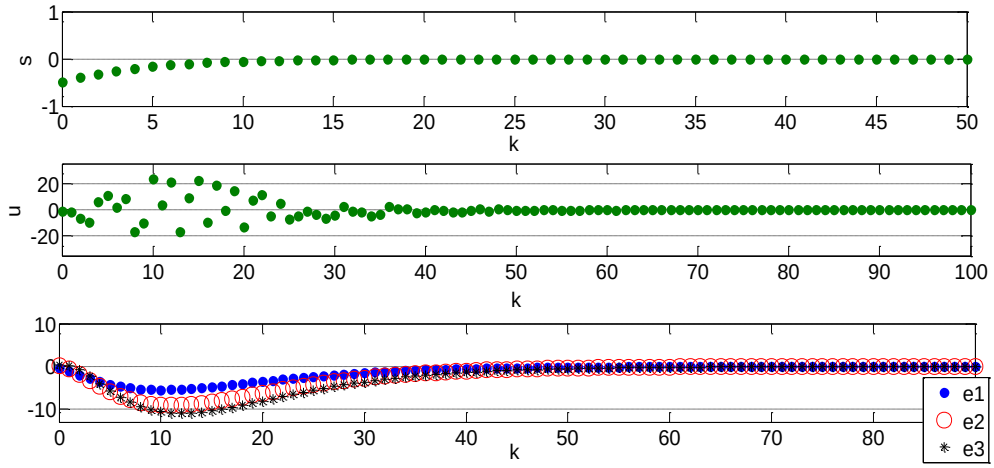

Figure 5. Responses of the switching surface, control input and synchronization error.

3. Design of High-Security USB Flash Drive Based on Chaos Authentication

In this paper, we aim to construct a high-security USB flash drive via chaos synchronization and authentication. We use an ARM-based microcontroller as the hardware-based encryption engine. To focus on promoting the convenience and system security, we use the most popular smart phone to perform authentication with the hardware-based encryption engine. Moreover, not only do we solve the disadvantages in the traditional encrypted flash drives but also provide more secure encryption protection.

3.1. Design of High-Security USB Flash Drive

The structure of the high-security USB flash drives are shown in Figure 6. In addition to the original flash memory and USB flash memory controller, we introduce an ARM-based microcontroller, power management unit and a Bluetooth module (nRF51822) for performing data transmission, chaos synchronization and authentication with the smart phone.

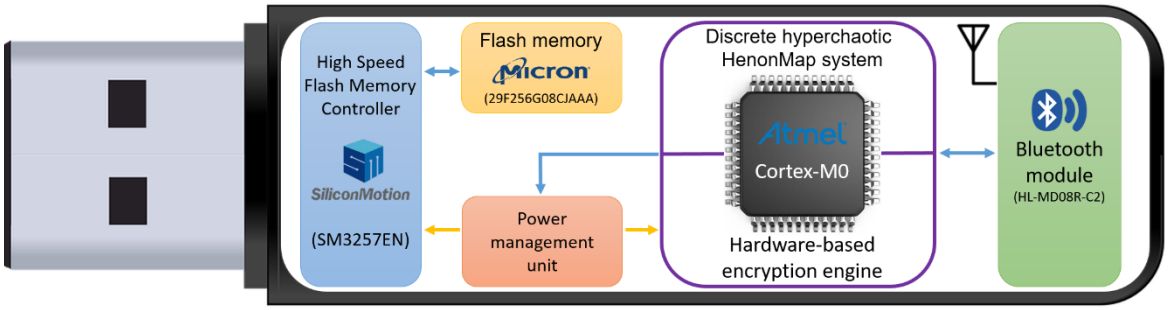

Figure 6. High-security USB flash drive architecture.

We built discrete slave and master hyperchaotic systems in the microcontroller and user's smartphone, respectively. The synchronization controller is implemented at ARM-based microcontroller side to achieve synchronization between the master and slave chaotic systems. Before confirming the user's identity and synchronization, the microcontroller disables the USB flash memory controller such that the computer cannot detect the existence of USB flash drive and cannot access the data. After completing chaos synchronization and authentication, ARM-based microcontroller will enable USB flash memory controller and allow the computer to read or write the data in high-security USB flash drive.

3.2. Realization of Chaos Authentication

As mentioned above, after the slave chaos system established in the high-security USB flash drive, it synchronized with the master system in the smartphone; the same random signal can be simultaneously obtained in both the USB flash drive and the smartphone. In order to improve security and avoid being cracked, we designed a non-linear encryption and decryption function. Using a random number generated in the discrete master chaotic system in the user's smartphone to encrypt a specified user password, and then send the encrypted password to the USB flash drive via the Bluetooth module. The high-security USB flash drive will receive the encrypted signal and is able to decrypt it due to the synchronization. The above non-linear encryption and decryption function design is given as follows:

$$E(x,p,t) = x_1^2 + \left(1 + x_2^2\right) p\hat{p} = D(y,E,t) = \left(E(x,p,t) - y_1^2\right) / \left(1 + y_2^2\right) \tag{15}$$

where $E(x,p,t)$ is a non-linear encryption function, $D(y,E,t)$ is a non-linear decryption function, p is the key (default built, not user-defined), $\hat{p}$ is the recovered key, x is the random state of master chaotic system in the smartphone, y is the random state of slave chaotic system built in USB flash drive. The complete authentication mechanism is shown in Figure 7.

3.3. High-Security USB Flash Drive Operation

High-security USB flash drive operation is very simply described as below:

Step 1: Plug high-security USB flash drive into the USB port of your computer.
Step 2: Open the APP installed on the user's smartphone for user authentication.
Step 3: When passing chaos authentication as shown in Figure 7, the user can begin to access the data in the high-security USB flash drive.

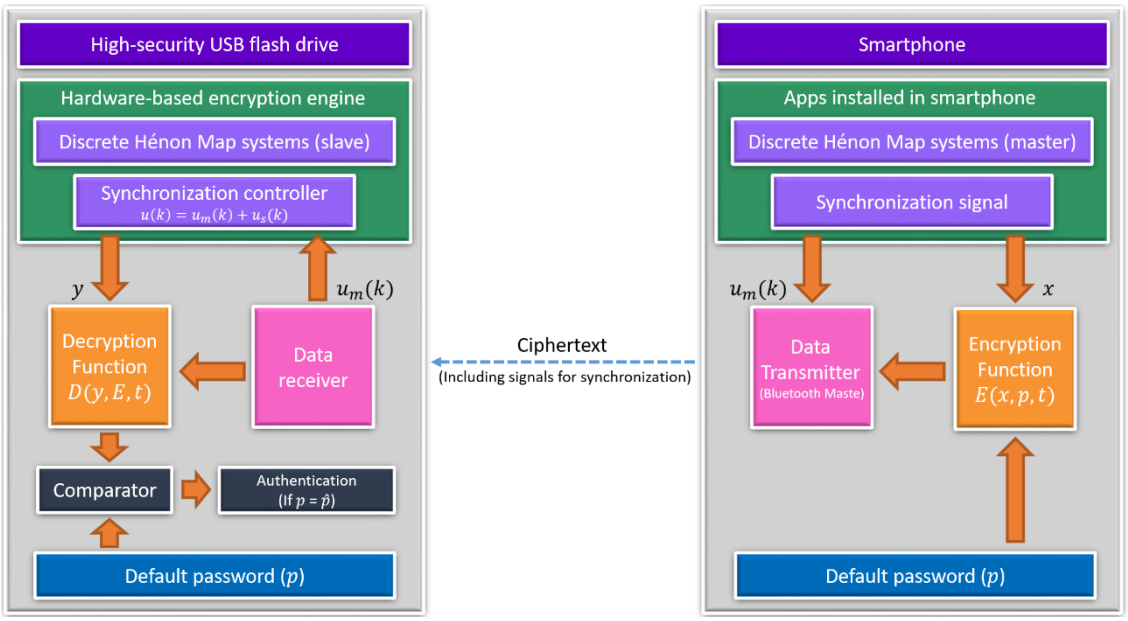

Figure 7. The authentication mechanism between USB flash drive and user's smartphone.

4. Conclusions and Future Work

This paper has recommended a novel design of high-security USB flash drives with proposed authentication based on chaos synchronization. By using the discrete sliding mode control, a simple and successful DSMC controller has been introduced for synchronizing two chaotic systems. Moreover, the synchronization scheme and the non-linear encryption and decryption function design have been applied to construct a high-security USB flash drive. The simulation and experimental results verify that the methods are correct and the drawbacks of poor performance and inconvenience in the traditional encrypted USB flash drives are all removed. In the future, we will continuously study the improvement for chaos authentication by combining the well-known cryptosystems with the synchronized dynamic keys in this paper. Furthermore, the security analysis and the effectiveness of resistance to attacks will also be studied to ensure the security of USB flash drives.

Author Contributions: All authors contributed to the paper. P.-Y.W. wrote the manuscript with the supervision from T.-L.L. and J.-J.Y., P.-C.C., Y.-C.L. and L.-K.W. are responsible for the hardware design of the high-security USB flash drives.

Funding: This work was financially supported by the Ministry of Science and Technology, Taiwan, under grant MOST-105-2221-E-006-103-MY2 and MOST-106-2221-E-366-001.

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

References

1. Hietala, J.D. *Hardware versus Software A Usability Comparison of Software-Based Encryption with Seagate Secure™ Hardware-Based Encryption*; Seagate: Cupertino, CA, USA, 2008; pp. 6–7.
2. Lin, J.S.; Huang, C.F.; Liao, T.L.; Yan, J.J. Design and implementation of digital secure communication based on synchronized chaotic systems. *Digit. Signal Process.* **2010**, *20*, 229–237. [CrossRef]
3. Ye, G.; Huang, X. A feedback chaotic image encryption scheme based on both bit-level and pixel-level. *J. Vib. Control* **2015**, *22*, 1171–1180. [CrossRef]
4. Zhang, J.; Zhang, Y. An image encryption algorithm based on balanced pixel and chaotic map. *Math. Probl. Eng.* **2014**, *2014*, 216048. [CrossRef]
5. Hua, Z.; Zhou, Y.; Pun, C.M.; Chen, C.P. 2D Sine Logistic modulation map for image encryption. *Inf. Sci.* **2015**, *297*, 80–94. [CrossRef]
6. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]

7. Njah, A.N. Tracking control and synchronization of the new hyperchaotic Liu system via backstepping techniques. *Nonlinear Dyn.* **2010**, *61*, 1–9. [CrossRef]
8. Yu, Y.; Li, H.X. Adaptive hybrid projective synchronization of uncertain chaotic systems based on backstepping design. *Nonlinear Anal. Real World Appl.* **2011**, *12*, 388–393. [CrossRef]
9. Kuo, C.L. Design of a fuzzy sliding-mode synchronization controller for two different chaos systems. *Comput. Math. Appl.* **2011**, *61*, 2090–2095. [CrossRef]
10. Yau, H.T.; Kuo, C.L.; Yan, J.J. Fuzzy sliding mode control for a class of chaos synchronization with uncertainties. *Int. J. Nonlinear Sci. Numer. Simul.* **2006**, *7*, 333–338. [CrossRef]
11. Cheng, D.L.; Huang, C.F.; Cheng, S.Y.; Yan, J.J. Synchronization of optical chaos in vertical-cavity surface-emitting lasers via optimal PI controller. *Expert Syst. Appl.* **2009**, *36*, 6854–6858. [CrossRef]
12. Pai, M.C. Global synchronization of uncertain chaotic systems via discrete-time sliding mode control. *Appl. Math. Comput.* **2014**, *228*, 663–671. [CrossRef]
13. Young, K.D.; Utkin, V.K.; Ozguner, U. A control engineer's guide to sliding mode control. *IEEE Trans. Autom. Control Syst. Technol.* **1999**, *7*, 328–342. [CrossRef]
14. Yan, M.; Shi, Y. Robust discrete-time sliding mode control for uncertain systems with time-varying state delay. *IET Control Theory Appl.* **2008**, *2*, 662–674. [CrossRef]
15. Miller, D.A. A discrete generalized hyperchaotic Henon map circuit. In Proceedings of the 44th IEEE 2001 Midwest Symposium on Circuits and Systems (MWSCAS) 2001, Dayton, OH, USA, 14–17 August 2001.