Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 698608, 15 pages
http://dx.doi.org/10.1155/2014/698608

Research Article

A Systematic Methodology for Multi-Images Encryption and Decryption Based on Single Chaotic System and FPGA Embedded Implementation

Hanzhong Zheng, Simin Yu, and Xiangqian Xu

College of Automation, Guangdong University of Technology, Guangzhou 510006, China

Correspondence should be addressed to Simin Yu; siminyu@163.com

Received 2 February 2014; Accepted 18 May 2014; Published 24 June 2014

Academic Editor: Giuseppe Rega

A systematic methodology is developed for multi-images encryption and decryption and field programmable gate array (FPGA) embedded implementation by using single discrete time chaotic system. To overcome the traditional limitations that a chaotic system can only encrypt or decrypt one image, this paper initiates a new approach to design n-dimensional (n-D) discrete time chaotic controlled systems via some variables anticontrol, which can achieve multipath drive-response synchronization. To that end, the designed n-dimensional discrete time chaotic controlled systems are used for multi-images encryption and decryption. A generalized design principle and the corresponding implementation steps are also given. Based on the FPGA embedded hardware system working platform with XUP Virtex-II type, a chaotic secure communication system for three digital color images encryption and decryption by using a 7D discrete time chaotic system is designed, and the related system design and hardware implementation results are demonstrated, with the related mathematical problems analyzed.

1. Introduction

Chaos control refers to purposefully eliminating or weakening chaotic behavior of systems through control methods when the chaotic motion is harmful. Since the OGY method was proposed in 1990 [1], much effort has been devoted to the study of controlling chaos. However, not all chaotic behaviors are harmful, and recent research has shown that chaos can actually be useful under certain circumstances, such as liquid mixing, information processing, flexible systems design, and secret communications. Therefore, chaotification by means of making an originally nonchaotic dynamical system chaotic, or enhancing existing chaos, has attracted some special attention lately. In 1994, Schiff et al. proposed the idea of chaos anticontrol [2]. In 1996, Chen and Lai proposed the Chen-Lai algorithm, which uses a linear state feedback controller and a mod-operation for the whole system to make all the Lyapunov exponents of the controlled system strictly positive, thereby obtaining chaos in the sense of Li-Yorke or Devaney [3–7]. Thereafter, Wang and Chen put forward the Wang-Chen algorithm [4, 8]. The idea of the Chen-Lai and Wang-Chen algorithms is to design a linear state feedback controller, which can change the eigenvalues of the system Jacobian matrix, thereby assigning desirable Lyapunov exponents to the controlled system [4]. In addition, some methods are also developed for anticontrol of continuous-time dynamical systems [9–11].

It is well known that the distinct properties of chaos, such as positive Lyapunov exponents, ergodicity, quasirandomness, sensitively dependence on initial conditions, and system parameters, have granted chaotic dynamics as a promising alternative for the conventional cryptographic algorithms. More importantly, unlike the conventional cryptographic algorithms which are mainly based on discrete mathematics, chaos-based cryptography relied on the complex dynamics of nonlinear systems or maps which are deterministic but simple. Therefore, it can provide a fast and secure means for data protection, which is crucial for multimedia data transmission over fast communication channels, such as the broadband internet communication [12–15]. Just because of

this, in recent years, numerous efforts have been devoted to develop various chaos-based image encryptions and secure communications. For all that, to the best of our knowledge, it is the most conventional practice that a chaotic system can only encrypt or decrypt one image by means of block cipher-based or stream cipher-based chaos discrete mapping [16–26]. One may ask whether or not there is a possible way further to break such a limitation so as to encrypt and decrypt multi-images by using single chaotic system. This paper gives a positive answer to the question.

In this paper, differing from the Chen-Lai and Wang-Chen algorithms, a new approach for designing n-dimensional discrete-time chaotic systems via some state-variable anticontrol is initiated, and a generalized design principle and the corresponding implementation steps are also given. To be specific, in order to overcome the traditional limitations that a chaotic system can only encrypt or decrypt one image, a discrete time nominal system with a stable saddle-focus at the origin is firstly designed. Then, one can do similarity transformation and introduce a controller on the nominal system via some state variable anticontrol, to obtain the related controlled chaotic system, which can achieve multipath drive-response synchronization. On the basis of this, a systematic methodology can be developed here for multi-images encryption and decryption by using single discrete time chaotic system. To that end, three 160×120 BMP digital color images with 24-bit per pixel are taken as examples for implementation and application. On the transmitter side, three 32-bit chaotic stream ciphers generated by a discrete-time chaotic system are used. For every 24-bit pixel, only 8-bit pixel is encrypted each time since the Ethernet transmission protocols and agreements are taken into account. The three encrypted digital color images are transmitted through LAN with only a router by using the time division multiplexing approach. On the receiver end, through a corresponding reverse operation, three encrypted digital color images can be decrypted if synchronization is achieved. Based on the FPGA embedded hardware system working platform with FPGA chip model XUP Virtex-II, a chaotic secure communication system for three digital color images encryption and decryption by using a 7D discrete time chaotic system is designed and implemented, with experimental results demonstrated. Both theoretical analysis and experimental results confirm the feasibility of this approach. More importantly, the main reasons why the presented system works well are given by the rigorous mathematical proof both for chaos existence and rapid synchronized convergence, since both of them play a very important role in image encryption and decryption.

The rest of the paper is organized as follows. A controlled chaotic system is designed via some variable anticontrol in Section 2. A representative example is given in Section 3. Multipath drive-response synchronization based on single chaotic system is given and analyzed in Section 4. FPGA embedded implementation for three digital color images encryption and decryption is implemented and demonstrated in Section 5. The corresponding NIST test results are given in Section 6. Finally, Section 7 concludes the paper.

2. Design of Discrete Time Chaotic System via Some Variable Anticontrol

2.1. Nominal System Design. Consider n $(n \geq 4)$-dimensional discrete time linear nominal system:

$$x(k+1) = Bx(k), \tag{1}$$

where

$$x(k+1) = \begin{pmatrix} x_1(k+1) \\ x_2(k+1) \\ \vdots \\ x_n(k+1) \end{pmatrix}_{n\times 1}, \quad x(k) = \begin{pmatrix} x_1(k) \\ x_2(k) \\ \vdots \\ x_n(k) \end{pmatrix}_{n\times 1},$$
$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}_{n\times n}. \tag{2}$$

Assume that B has a generalized form of block diagonal matrix. In the following, two conditions are involved.

(1) When n is an even number, letting $m = n/2$, one gets the generalized form of B:

$$B = \begin{pmatrix} B_1 & 0 & 0 & \cdots & 0 \\ 0 & B_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & B_{m-1} & 0 \\ 0 & 0 & \cdots & 0 & B_m \end{pmatrix}_{n\times n}, \tag{3}$$

where B_m is a 2×2 block matrix, given by

$$B_m = \begin{pmatrix} \gamma_m & \omega_{m1} \\ \omega_{m2} & \gamma_m \end{pmatrix}. \tag{4}$$

According to (3) with (4), letting $\omega_{m1} \cdot \omega_{m2} < 0$, one gets the characteristic roots of B at the origin:

$$\lambda_{2m-1,2m} = \gamma_m \pm j\sqrt{|\omega_{m1} \cdot \omega_{m2}|}, \tag{5}$$

where $m = 1, 2, 3, \ldots, n/2$.

When $\gamma_i \neq \gamma_j, \omega_{i1} \cdot \omega_{i2} \neq \omega_{j1} \cdot \omega_{j2}$ $(i, j = 1, 2, \ldots, n/2;\ i \neq j)$ are satisfied, there exist n distinct eigenvalues. Particularly, when $|\lambda_{2m-1,2m}| < 1$, n characteristic roots of B are located inside the unit circle, making the nominal system asymptotically stable.

(2) When n is an odd number, letting $m = (n-1)/2$, one gets the generalized form of B:

$$B = \begin{pmatrix} B_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & B_2 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & B_{m-1} & \cdots & 0 \\ 0 & 0 & 0 & \cdots & B_m & 0 \\ -1 & -1 & -1 & \cdots & -1 & \gamma_n \end{pmatrix}_{n\times n}, \tag{6}$$

where B_m is a 2×2 block matrix, also given by (4).

Suppose $\omega_{m1} \cdot \omega_{m2} < 0$; one gets the characteristic roots of B at the origin:

$$\begin{aligned} \lambda_{2m-1,2m} &= \gamma_m \pm j\sqrt{|\omega_{m1} \cdot \omega_{m2}|}. \\ \lambda_n &= \gamma_n, \end{aligned} \tag{7}$$

where $m = (n-1)/2$.

When $\gamma_i \neq \gamma_j$, $\omega_{i1} \cdot \omega_{i2} \neq \omega_{j1} \cdot \omega_{j2}$ $(i, j = 1, 2, \ldots, n/2;\ i \neq j)$ are satisfied, there exist n distinct eigenvalues. Especially, when $|\lambda_{2m-1,2m}| < 1$ and $|\lambda_n| < 1$, n characteristic roots of B are located inside the unit circle, making the nominal system asymptotically stable.

Do similarity transformation on nominal system (1). It is noted that, except for the block diagonal matrix B_m and γ_n, the remaining elements are zeros in B. In order to effectively control the nominal system, do similarity transformation on the nominal system (1), such that

$$A = PBP^{-1}, \tag{8}$$

where P is an invertible matrix in the form of

$$P = \begin{pmatrix} 0 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 0 \end{pmatrix}_{n \times n}. \tag{9}$$

Finally, one gets the nominal system after doing similarity transformation:

$$x(k+1) = Ax(k), \tag{10}$$

where

$$A = PBP^{-1} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}_{n \times n}. \tag{11}$$

It is especially pointed that, after similarity transformation, A and B have the same characteristic polynomial and eigenvalues. That is, the nominal system (1) and the converted nominal system (10) have the same stability.

2.2. Controlled Chaotic System Design via Some Variable Anticontrol. According to (10), by selecting $x_m(k), x_{m+1}(k), \ldots, x_n(k)$ from $x(k)$ as l feedback control variables, one can design a uniformly bounded controller:

$$\begin{aligned} g(\sigma x, \varepsilon) &= \begin{pmatrix} g_1(\sigma_1 x_m, \varepsilon_1) \\ g_2(\sigma_2 x_{m+1}, \varepsilon_2) \\ \vdots \\ g_l(\sigma_l x_n, \varepsilon_l) \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{n \times 1} \\ &= \begin{pmatrix} \operatorname{mod}(\sigma_1 x_m, \varepsilon_1) \\ \operatorname{mod}(\sigma_2 x_{m+1}, \varepsilon_2) \\ \vdots \\ \operatorname{mod}(\sigma_l x_n, \varepsilon_l) \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{n \times 1}, \end{aligned} \tag{12}$$

where $g(\sigma x, \varepsilon)$ is a uniformly bounded nonlinear function, such as periodic or modular functions. Here, select $g(\sigma x, \varepsilon)$ as a modular function $\operatorname{mod}(\cdot)$. In addition, parameters $\sigma = [\sigma_1, \sigma_2, \ldots, \sigma_l, 0, \ldots, 0]$ are controller gain and $\varepsilon = [\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_l, 0, \ldots, 0]$ are controller supremum. l is the number of feedback control variables $x_m(k), x_{m+1}(k), \ldots, x_n(k)$. m is the subscript value of the first feedback control variable $x_m(k)$.

From (10)–(12), one obtains the controlled system, given by

$$x(k+1) = Ax(k) + g(\sigma x(k), \varepsilon). \tag{13}$$

The corresponding component form of (13) is given by

$$\begin{aligned} x_1(k+1) &= a_{11}x_1(k) + \cdots + a_{1m-1}x_{m-1}(k) + a_{1m}x_m(k) \\ &\quad + \cdots + a_{1n}x_n(k) + g_1(\sigma_1 x_m(k), \varepsilon_1) \\ &\vdots \\ x_l(k+1) &= a_{l1}x_1(k) + \cdots + a_{lm-1}x_{m-1}(k) + a_{lm}x_m(k) \\ &\quad + \cdots + a_{ln}x_n(k) + g_l(\sigma_l x_n(k), \varepsilon_l) \\ &\vdots \\ x_m(k+1) &= a_{m1}x_1(k) + \cdots + a_{mm-1}x_{m-1}(k) \\ &\quad + a_{mm}x_m(k) + \cdots + a_{mn}x_n(k) \\ &\vdots \end{aligned}$$

$$x_n(k+1) = a_{n1}x_1(k) + \cdots + a_{nm-1}x_{m-1}(k) + a_{nm}x_m(k) + \cdots + a_{mn}x_n(k). \tag{14}$$

Theorem 1. *Consider the controlled system* (14). *If the following two conditions are satisfied, then the controlled system* (14) *is chaotic.*

(i) *n characteristic roots of A are located inside the unit circle, making the corresponding nominal system* (10) *asymptotically stable.*

(ii) *The controller* (12) *is uniformly bounded. By selecting parameters σ and ε, the controlled system matrix A_C of system* (14) *has at least one characteristic root located outside the unit circle, where A_C is given by*

$$A_C = \begin{pmatrix} a_{11} & \cdots & a_{1,m-1} & a_{1,m} + \dfrac{\partial g_1(\sigma_1 x_m, \varepsilon_1)}{\partial x_m} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{l,1} & \cdots & a_{l,m-1} & a_{l,m} & \cdots & a_{l,m} + \dfrac{\partial g_l(\sigma_l x_n, \varepsilon_l)}{\partial x_n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,m-1} & a_{m,m} & \cdots & a_{m,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m-1} & a_{n,m} & \cdots & a_{n,n} \end{pmatrix}. \tag{15}$$

Proof. In the many features of chaos, two basic characteristics, namely, being globally bounded while having a positive Lyapunov exponent, are widely used as criteria for chaos [4]. Consider the solution of (14):

$$x(k) = A^k x_0 + \sum_{j=0}^{k-1} A^{k-j-1} g(\sigma x(j), \varepsilon). \tag{16}$$

It follows from conditions (i) and (ii) that, since $\|A\| < 1$ and $\sup_{0\le k<\infty}\|g(\sigma x, \varepsilon)\| \le \varepsilon_j < \infty$, one has

$$\begin{aligned} \sup_{0\le k<\infty}\|x(k)\| &\le \sup_{0\le k<\infty}\|A\|^k \cdot \|x_0\| + \sup_{0\le k<\infty}\sum_{j=0}^{k-1}\|A\|^{k-j-1}\cdot\varepsilon_j \\ &\le \sup_{0\le k<\infty}\|x_0\| + \sup_{0\le k<\infty}\varepsilon_j \cdot \sum_{j=0}^{k-1}\|A\|^{k-j-1}, \end{aligned} \tag{17}$$

where $\sum_{j=0}^{k-1}\|A\|^{k-j-1} = \|A\|^0 + \|A\|^1 + \|A\|^2 + \cdots + \|A\|^{k-1}$ is a geometric series with common ratio $\|A\|$. Hence, one gets

$$\sum_{j=0}^{k-1}\|A\|^{k-j-1} = \frac{\|A\|^0 - \|A\|\cdot\|A\|^{k-1}}{1-\|A\|} = \frac{1-\|A\|^k}{1-\|A\|}. \tag{18}$$

Substituting (18) into (17), one gets

$$\begin{aligned} \sup_{0\le k<\infty}\|x(k)\| &\le \sup_{0\le k<\infty}\|x_0\| + \sup_{0\le k<\infty}\varepsilon_j \cdot \frac{1-\|A\|^k}{1-\|A\|} \\ &\le \sup_{0\le k<\infty}\|x_0\| + \sup_{0\le k<\infty}\frac{\varepsilon_j}{1-\|A\|} < \infty. \end{aligned} \tag{19}$$

Therefore, $x(k)$ is globally bounded.

According to the Lyapunov exponent formula for discrete-time chaotic systems,

$$\begin{aligned} \lambda_i(x_0) &= \lim_{m\to\infty}\lambda_{mi}(x_0) \\ &= \lim_{m\to\infty}\frac{1}{2m}\ln\left[\mu_i\left(T_m^T\ T_m\right)\right] \quad (i = 1, 2, \ldots, n), \end{aligned} \tag{20}$$

where $i = 1, 2, \ldots, n$. When A_C has at least one characteristic root located outside the unit circle, system (14) generates at least one positive Lyapunov exponent.

Therefore, the controlled system (14) is chaotic since it is globally bounded and has at least one positive Lyapunov exponent. □

3. A Typical Example

Consider a 7D nominal matrix B in the form of

$$B = \begin{pmatrix} \gamma_1 & \omega_{11} & 0 & 0 & 0 & 0 & 0 \\ \omega_{12} & \gamma_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \gamma_2 & \omega_{21} & 0 & 0 & 0 \\ 0 & 0 & \omega_{22} & \gamma_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \gamma_3 & \omega_{31} & 0 \\ 0 & 0 & 0 & 0 & \omega_{32} & \gamma_3 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & \gamma_7 \end{pmatrix}_{7\times 7}, \tag{21}$$

where $\gamma_1 = 0.31$, $\omega_{11} = \omega_{12} = 0.23$, $\gamma_2 = 0.13$, $\omega_{21} = \omega_{22} = 0.21$, $\gamma_3 = -0.17$, $\omega_{31} = \omega_{32} = 0.33$, and $\gamma_7 = -0.19$.

Suppose that the similarity transformation is

$$P = \begin{pmatrix} 0 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 0 \end{pmatrix}_{7\times 7}. \tag{22}$$

According to $A = PBP^{-1}$, one gets the converted nominal matrix, given by

$$A = \begin{pmatrix} 0.1983 & -0.3417 & 0.0483 & -0.3717 & 0.4683 & -0.1917 & -0.8417 \\ -0.2650 & -0.1850 & 0.1250 & -0.2950 & 0.5450 & -0.1150 & -0.7650 \\ -0.0783 & -0.5383 & 0.2117 & -0.1283 & 0.5017 & -0.1583 & -0.8083 \\ -0.0083 & -0.4683 & -0.0583 & -0.1383 & 0.5717 & -0.0883 & -0.7383 \\ -0.0483 & -0.5083 & 0.1117 & -0.3083 & 0.3617 & 0.2017 & -0.7783 \\ 0.0617 & -0.3983 & 0.2217 & -0.1983 & 0.3117 & -0.1883 & -0.6683 \\ 0.0100 & -0.4500 & 0.1700 & -0.2500 & 0.5900 & -0.0700 & 0.0900 \end{pmatrix}_{7\times 7}. \tag{23}$$

By selecting three feedback state variables as $x_5(k)$, $x_6(k)$, and $x_7(k)$, the controller is obtained by

$$g(\sigma x, \varepsilon) = \begin{pmatrix} g_1(\sigma_1 x_5, \varepsilon_1) \\ g_2(\sigma_2 x_6, \varepsilon_2) \\ g_3(\sigma_3 x_7, \varepsilon_3) \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}_{7\times 1} = \begin{pmatrix} \operatorname{mod}(\sigma_1 x_5, \varepsilon_1) \\ \operatorname{mod}(\sigma_2 x_6, \varepsilon_2) \\ \operatorname{mod}(\sigma_3 x_7, \varepsilon_3) \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}_{7\times 1}, \tag{24}$$

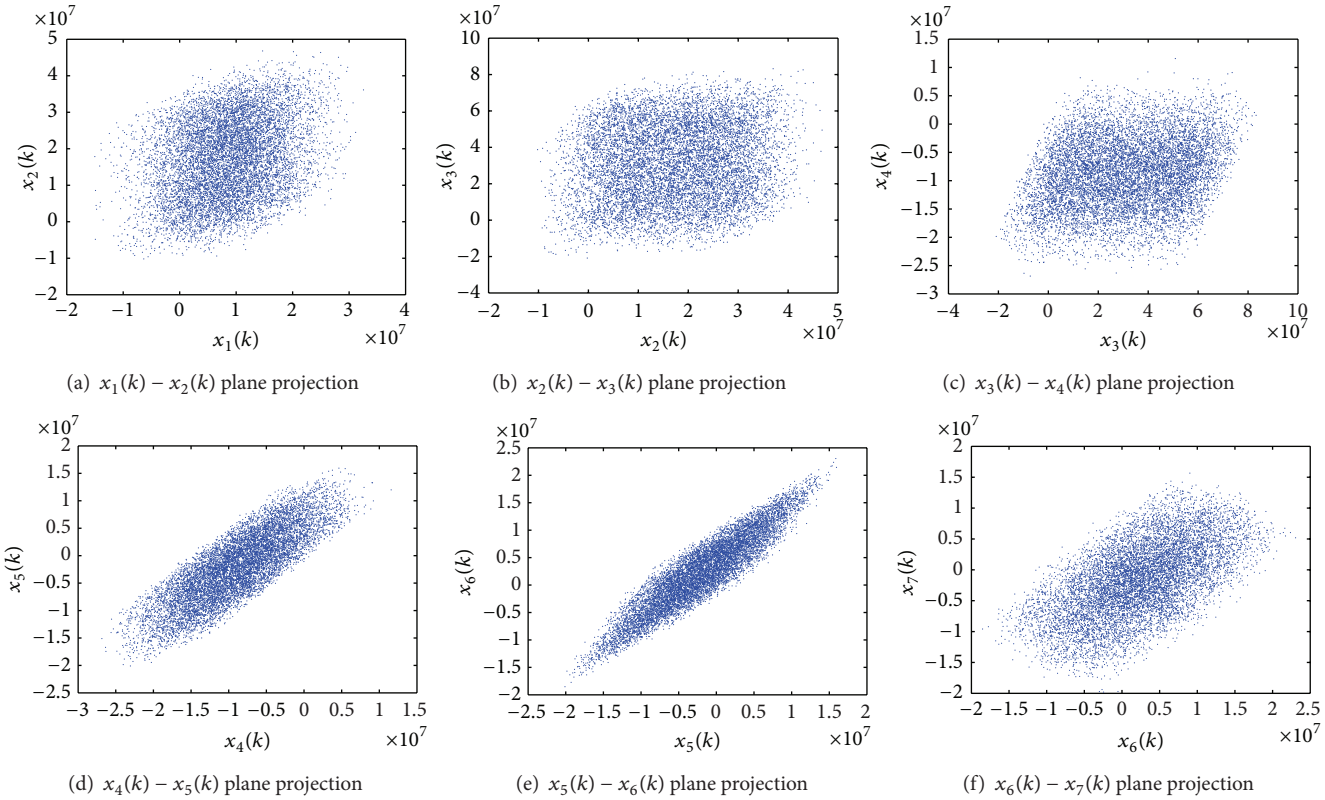
where parameters $\varepsilon_1 = 1.6\times 10^7$, $\sigma_1 = 2.3\times 10^7$, $\varepsilon_2 = 3.3\times 10^7$, and $\sigma_2 = 4.2\times 10^7$, $\varepsilon_3 = 6.7\times 10^7$, $\sigma_3 = 5.0\times 10^7$.

According to (23) with (24), one gets the controlled system, given by

$$\begin{pmatrix} x_1(k+1) \\ x_2(k+1) \\ x_3(k+1) \\ x_4(k+1) \\ x_5(k+1) \\ x_6(k+1) \\ x_7(k+1) \end{pmatrix} = \begin{pmatrix} 0.1983 & -0.3417 & 0.0483 & -0.3717 & 0.4683 & -0.1917 & -0.8417 \\ -0.2650 & -0.1850 & 0.1250 & -0.2950 & 0.5450 & -0.1150 & -0.7650 \\ -0.0783 & -0.5383 & 0.2117 & -0.1283 & 0.5017 & -0.1583 & -0.8083 \\ -0.0083 & -0.4683 & -0.0583 & -0.1383 & 0.5717 & -0.0883 & -0.7383 \\ -0.0483 & -0.5083 & 0.1117 & -0.3083 & 0.3617 & 0.2017 & -0.7783 \\ 0.0617 & -0.3983 & 0.2217 & -0.1983 & 0.3117 & -0.1883 & -0.6683 \\ 0.0100 & -0.4500 & 0.1700 & -0.2500 & 0.5900 & -0.0700 & 0.0900 \end{pmatrix} \times \begin{pmatrix} x_1(k) \\ x_2(k) \\ x_3(k) \\ x_4(k) \\ x_5(k) \\ x_6(k) \\ x_7(k) \end{pmatrix} + \begin{pmatrix} \operatorname{mod}(\sigma_1 x_5(k), \varepsilon_1) \\ \operatorname{mod}(\sigma_2 x_6(k), \varepsilon_2) \\ \operatorname{mod}(\sigma_3 x_7(k), \varepsilon_3) \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \tag{25}$$

where A_C is in the form of

$$A_C = \begin{pmatrix} 0.1983 & -0.3417 & 0.0483 & -0.3717 & 0.4683 + \varepsilon_1\sigma_1 & -0.1917 & -0.8417 \\ -0.2650 & -0.1850 & 0.1250 & -0.2950 & 0.5450 & -0.1150 + \varepsilon_2\sigma_2 & -0.7650 \\ -0.0783 & -0.5383 & 0.2117 & -0.1283 & 0.5017 & -0.1583 & -0.8083 + \varepsilon_3\sigma_3 \\ -0.0083 & -0.4683 & -0.0583 & -0.1383 & 0.5717 & -0.0883 & -0.7383 \\ -0.0483 & -0.5083 & 0.1117 & -0.3083 & 0.3617 & 0.2017 & -0.7783 \\ 0.0617 & -0.3983 & 0.2217 & -0.1983 & 0.3117 & -0.1883 & -0.6683 \\ 0.0100 & -0.4500 & 0.1700 & -0.2500 & 0.5900 & -0.0700 & 0.0900 \end{pmatrix}. \tag{26}$$



(a) $x_1(k) - x_2(k)$ plane projection (b) $x_2(k) - x_3(k)$ plane projection (c) $x_3(k) - x_4(k)$ plane projection

(d) $x_4(k) - x_5(k)$ plane projection (e) $x_5(k) - x_6(k)$ plane projection (f) $x_6(k) - x_7(k)$ plane projection

Figure 1: A 7D chaotic attractor.

By calculating, one gets the seven eigenvalues of B and A as follows:

$$\begin{aligned} \lambda_1 &= -0.1900, \\ \lambda_{2,3} &= 0.3100 \pm j0.2300, \\ \lambda_{4,5} &= 0.1300 \pm j0.2100, \\ \lambda_{6,7} &= -0.1700 \pm j0.3300. \end{aligned} \tag{27}$$

Therefore, all the characteristic roots of B and A are located inside the unit circle.

Similarly, one gets seven eigenvalues of A_C as follows:

$$\begin{aligned} \lambda_1 &= -4.3, \\ \lambda_{2,3} &= 1.4208 \times 10^7 \pm j1.4213 \times 10^7, \\ \lambda_{4,5} &= -1.4208 \times 10^7 \pm j1.4213 \times 10^7, \\ \lambda_{6,7} &= 2.2 \pm j3.7. \end{aligned} \tag{28}$$

Hence, in the controlled system (25), seven eigenvalues of A_C are located outside the unit circle.

According to Theorem 1, the controlled system (25) is chaotic, with a chaotic attractor as shown in Figure 1.

4. Principle of Multipath Drive-Response Synchronization via Single Chaotic System

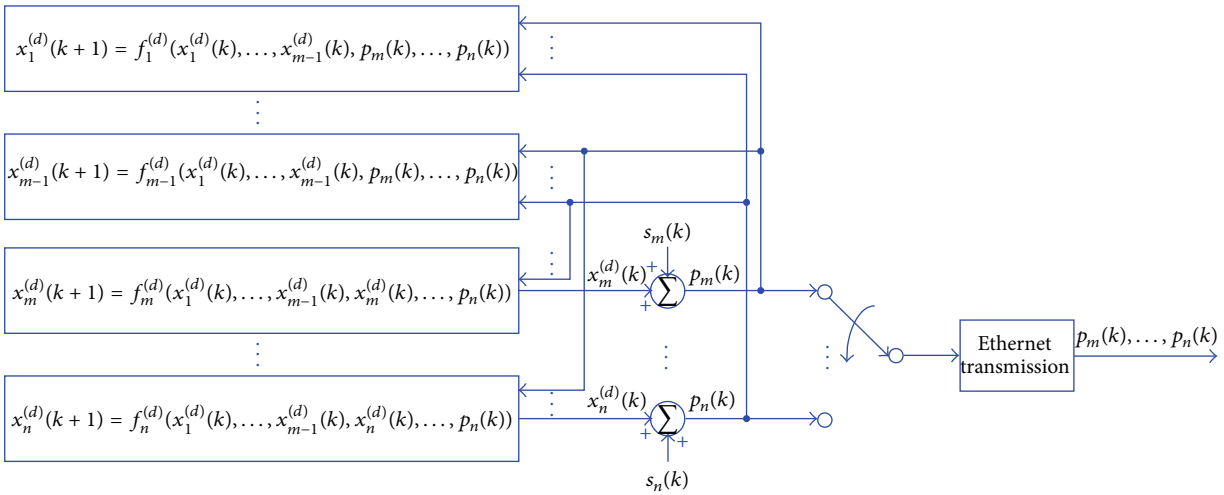
In this section, the principle of multipath drive-response synchronization based on single chaotic system is investigated.

4.1. Multipath Drive-Response Synchronization via Single Chaotic System. A diagram for multipath drive-response synchronization via single chaotic system is shown in Figure 2, and its fundamental working principles are described as follows.

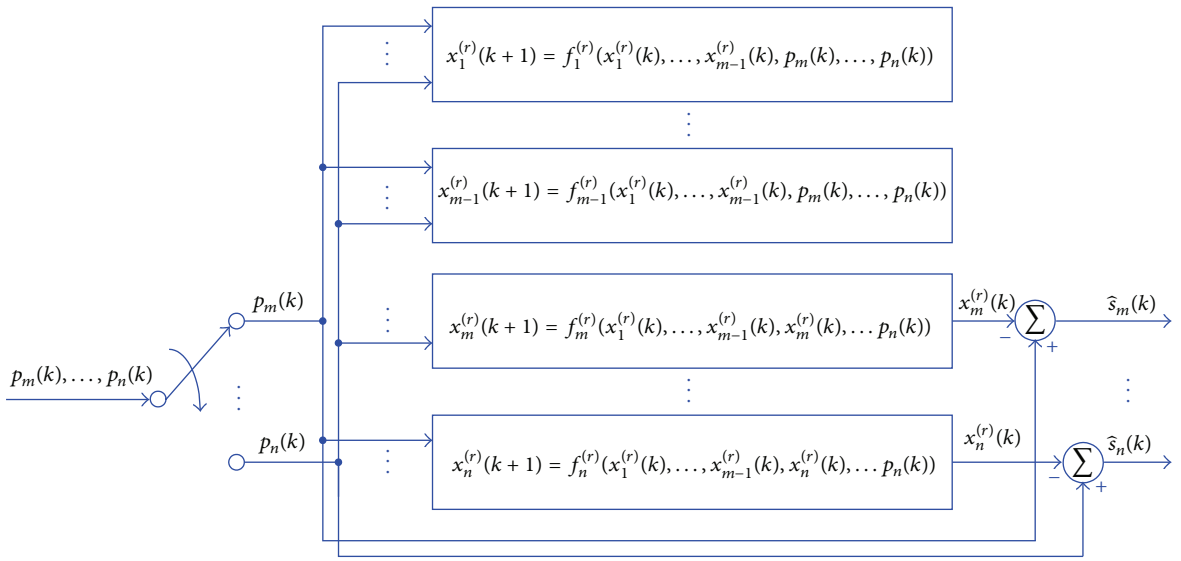
(i) The l state variables $x_m^{(d)}(k), \ldots, x_n^{(d)}(k)$ generated by the drive system are used for chaotic encryption sequences, which encrypt pixels $s_m(k), \ldots, s_n(k)$ of l images. Therefore, one can obtain the l encrypted signals $p_m(k) = x_m^{(d)}(k) + s_m(k), \ldots, \ p_n(k) = x_n^{(d)}(k) + s_n(k)$.

(ii) The l encrypted signals $p_m(k) = x_m^{(d)}(k) + s_m(k), \ldots, p_n(k) = x_n^{(d)}(k) + s_n(k)$ are feedback to the drive system. The related feedback principle is that, except for jth equation, the drive system state variables $x_j^{(d)}(k)$ of the remaining $n-1$ equations are replaced by $p_j(k)$, where $j = m, \ldots, n$.

(iii) The l encrypted signals $p_m(k) = x_m^{(d)}(k) + s_m(k), \ldots, p_n(k) = x_n^{(d)}(k) + s_n(k)$ are transmitted through Ethernet by using the time division multiplexing



(a) The drive system



(b) The response system

FIGURE 2: A diagram for multipath drive-response synchronization via single chaotic system.

approach, which are used for driving the response system. The related drive principle is that, except for jth equation, the response system state variables $x_j^{(r)}(k)$ of the remaining $n-1$ equations are replaced by $p_j(k)$, where $j = m, \ldots, n$.

On the transmitter side, according to (14) and Figure 2, the drive system is obtained by

$$\begin{aligned} x_1^{(d)}(k+1) &= a_{11}^{(d)} x_1^{(d)}(k) + \cdots + a_{1m-1}^{(d)} x_{m-1}^{(d)}(k) \\ &\quad + a_{1m}^{(d)} p_m(k) + \cdots + a_{1n}^{(d)} p_n(k) \\ &\quad + g_1^{(d)}\left(\sigma_1^{(d)} p_m(k), \varepsilon_1^{(d)}\right) \\ &\triangleq f_1^{(d)}\left(x_1^{(d)}(k), \ldots, x_{m-1}^{(d)}(k), p_m(k), \ldots, p_n(k)\right) \\ &\vdots \\ x_l^{(d)}(k+1) &= a_{l1}^{(d)} x_1^{(d)}(k) + \cdots + a_{lm-1}^{(d)} x_{m-1}^{(d)}(k) \\ &\quad + a_{lm}^{(d)} p_m(k) + \cdots + a_{ln}^{(d)} p_n(k) \\ &\quad + g_l^{(d)}\left(\sigma_l^{(d)} p_n(k), \varepsilon_l^{(d)}\right) \\ &\triangleq f_l^{(d)}\left(x_1^{(d)}(k), \ldots, x_{m-1}^{(d)}(k), p_m(k), \ldots, p_n(k)\right) \\ &\vdots \\ x_m^{(d)}(k+1) &= a_{m1}^{(d)} x_1^{(d)}(k) + \cdots + a_{mm-1}^{(d)} x_{m-1}^{(d)}(k) \\ &\quad + a_{mm}^{(d)} x_m^{(d)}(k) + a_{mm+1}^{(d)} p_{m+1}(k) \\ &\quad + \cdots + a_{mn}^{(d)} p_n(k) \\ &\triangleq f_m^{(d)}\left(x_1^{(d)}(k), \ldots, x_{m-1}^{(d)}(k), x_m^{(d)}(k), p_{m+1}(k), \ldots, p_n(k)\right) \\ &\vdots \end{aligned}$$

$$\begin{aligned} x_n^{(d)}(k+1) &= a_{n1}^{(d)} x_1^{(d)}(k) + \cdots + a_{nm-1}^{(d)} x_{m-1}^{(d)}(k) \\ &\quad + a_{nm}^{(d)} p_m(k) + \cdots + a_{nm-1}^{(d)} p_{n-1}(k) \\ &\quad + a_{nn}^{(d)} x_n^{(d)}(k) \\ &\triangleq f_n^{(d)}\left(x_1^{(d)}(k), \ldots, x_{m-1}^{(d)}(k), p_m(k), \ldots, \right. \\ &\qquad \left. p_{n-1}(k), x_n^{(d)}(k)\right). \end{aligned} \tag{29}$$

Similarly, at the receiver end, the response system is described by

$$\begin{aligned} &x_1^{(r)}(k+1) \\ &\quad = a_{11}^{(r)} x_1^{(r)}(k) + \cdots + a_{1m-1}^{(r)} x_{m-1}^{(r)}(k) + a_{1m}^{(r)} p_m(k) \\ &\qquad + \cdots + a_{1n}^{(r)} p_n(k) + g_1^{(r)}\left(\sigma_1^{(r)} p_m(k), \varepsilon_1^{(r)}\right) \\ &\quad \triangleq f_1^{(r)}\left(x_1^{(r)}(k), \ldots, x_{m-1}^{(r)}(k), p_m(k), \ldots, p_n(k)\right) \\ &\qquad \vdots \\ &x_l^{(r)}(k+1) \\ &\quad = a_{l1}^{(r)} x_1^{(r)}(k) + \cdots + a_{lm-1}^{(r)} x_{m-1}^{(r)}(k) + a_{lm}^{(r)} p_m(k) \\ &\qquad + \cdots + a_{ln}^{(r)} p_n(k) + g_l^{(r)}\left(\sigma_l^{(r)} p_n(k), \varepsilon_l^{(r)}\right) \\ &\quad \triangleq f_l^{(r)}\left(x_1^{(r)}(k), \ldots, x_{m-1}^{(r)}(k), p_m(k), \ldots, p_n(k)\right) \\ &\qquad \vdots \\ &x_m^{(r)}(k+1) \\ &\quad = a_{m1}^{(r)} x_1^{(r)}(k) + \cdots + a_{mm-1}^{(r)} x_{m-1}^{(r)}(k) + a_{mm}^{(r)} x_m^{(r)}(k) \\ &\qquad + a_{mm+1}^{(r)} p_{m+1}(k) + \cdots + a_{mn}^{(r)} p_n(k) \\ &\quad \triangleq f_m^{(r)}\left(x_1^{(r)}(k), \ldots, x_{m-1}^{(r)}(k), x_m^{(r)}(k), \right. \\ &\qquad \left. p_{m+1}(k), \ldots, p_n(k)\right) \\ &\qquad \vdots \\ &x_n^{(r)}(k+1) \\ &\quad = a_{n1}^{(r)} x_1^{(r)}(k) + \cdots + a_{nm-1}^{(r)} x_{m-1}^{(r)}(k) + a_{nm}^{(r)} p_m(k) \\ &\qquad + \cdots + a_{nn-1}^{(r)} p_{n-1}(k) + a_{nn}^{(d)} x_n^{(d)}(k) \\ &\quad \triangleq f_n^{(r)}\left(x_1^{(r)}(k), \ldots, x_{m-1}^{(r)}(k), p_m(k), \ldots, \right. \\ &\qquad \left. p_{n-1}(k), x_n^{(r)}(k)\right). \end{aligned} \tag{30}$$

4.2. Relationship of n, l, and m. In (29) and (30), n is the number of dimensions of the chaotic system, l is the number of feedback control variables $x_m(k), x_{m+1}(k), \ldots, x_n(k)$, and it is also the number of encrypted and decrypted images. m is the subscript value of the first feedback control variable $x_m(k)$. In order to weigh both the number of encrypted images and the safety performance, l is determined by

$$l = (n - m) + 1 = \text{round}\left(\frac{n}{2}\right). \tag{31}$$

According to (31), when l is determined, one can obtain the subscript value m of the first feedback control variable $x_m(k)$, given by

$$m = n + 1 - l. \tag{32}$$

Obviously, inequality $l \leq m - 1$ holds.

4.3. Analysis of Multipath Drive-Response Chaotic Synchronization

Theorem 2. *Consider the drive system* (29) *and the response system* (30). *If the following two conditions are satisfied, then the response system can synchronize the drive system.*

(i) *The parameters of* (29) *and* (30) *exactly match.*

(ii) *Eigenvalue roots of nominal matrix B and A satisfy* $|\lambda_{2m-1,2m}| = |\gamma_m \pm j\sqrt{|\omega_{m1} \cdot \omega_{m2}|}| < 1$ *and* $|\lambda_n| = |\gamma_n| < 1$.

Proof. According to (29), (30), and condition (i) from Theorem 2, one gets the error system, given by

$$\begin{aligned} \Delta x_1(k+1) &= a_{11}\Delta x_1(k) + a_{12}\Delta x_2(k) \\ &\quad + \cdots + a_{1m-1}\Delta x_{m-1}(k), \\ \Delta x_2(k+1) &= a_{21}\Delta x_1(k) + a_{22}\Delta x_2(k) \\ &\quad + \cdots + a_{2m-1}\Delta x_{m-1}(k), \\ &\vdots \\ \Delta x_{m-1}(k+1) &= a_{m-11}\Delta x_1(k) + a_{m-12}\Delta x_2(k) \\ &\quad + \cdots + a_{m-1m-1}\Delta x_{m-1}(k), \\ \Delta x_m(k+1) &= a_{m1}\Delta x_1(k) + a_{m2}\Delta x_2(k) \\ &\quad + \cdots + a_{mm-1}\Delta x_{m-1}(k) + a_{mm}\Delta x_m(k), \\ \Delta x_{m+1}(k+1) &= a_{m+11}\Delta x_1(k) + a_{m+12}\Delta x_2(k) \\ &\quad + \cdots + a_{m+1m-1}\Delta x_{m-1}(k) \\ &\quad + a_{m+1m+1}\Delta x_{m+1}(k), \\ &\vdots \\ \Delta x_n(k+1) &= a_{n1}\Delta x_1(k) + a_{n2}\Delta x_2(k) \\ &\quad + \cdots + a_{nm-1}\Delta x_{m-1}(k) + a_{nn}\Delta x_n(k), \end{aligned} \tag{33}$$

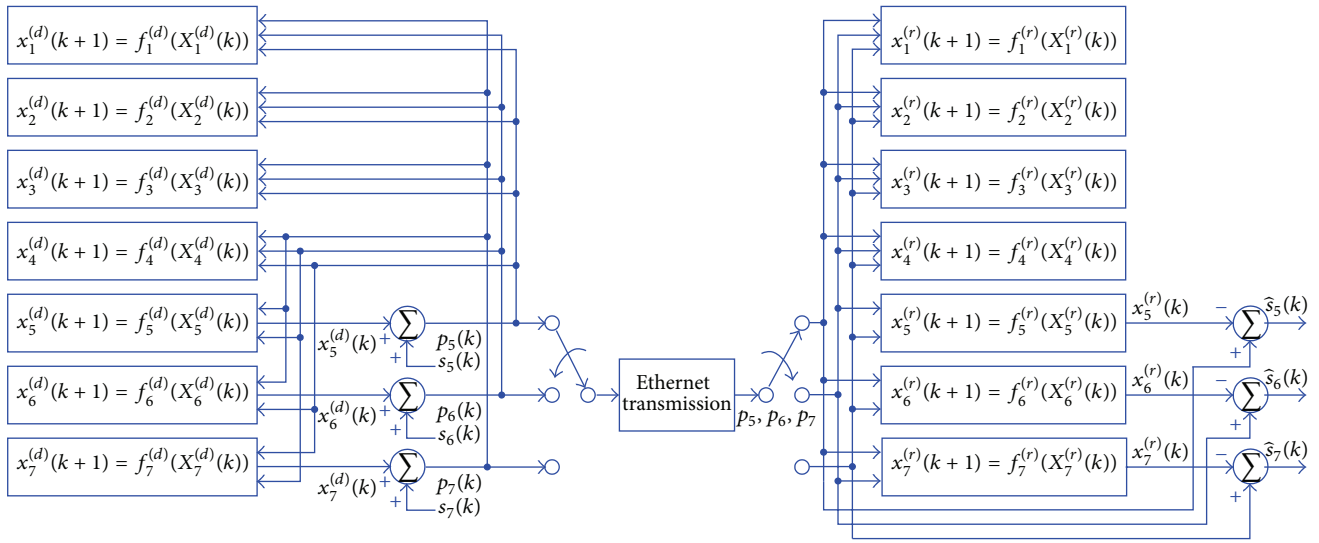


Figure 3: A diagram for 7D three-path drive-response synchronization system.

where $a_{ij}^{(d)} = a_{ij}^{(r)} = a_{ij}$ with $1 \le i, j \le n$, $\varepsilon_j^{(d)} = \varepsilon_j^{(r)}$, $\sigma_j^{(d)} = \sigma_j^{(r)}$ with $1 \le j \le l$, and $\Delta x_j(k+1) = \Delta x_j^{(d)}(k+1) - \Delta x_j^{(r)}(k+1)$ and $\Delta x_j(k) = \Delta x_j^{(d)}(k) - \Delta x_j^{(r)}(k)$ with $1 \le j \le n$.

From (33), one gets

$$\begin{pmatrix} \Delta x_1(k) \\ \Delta x_2(k) \\ \vdots \\ \Delta x_{m-1}(k) \end{pmatrix} = \left(\left[a_{ij} \right]_{m-1\times m-1} \right)^k \begin{pmatrix} \Delta x_1(0) \\ \Delta x_2(0) \\ \vdots \\ \Delta x_{m-1}(0) \end{pmatrix}. \quad (34)$$

By taking norm on both sides of (34), one has

$$\left\| \begin{pmatrix} \Delta x_1(k) \\ \Delta x_2(k) \\ \vdots \\ \Delta x_{m-1}(k) \end{pmatrix} \right\| = \left\| \left(\left[a_{ij} \right]_{m-1\times m-1} \right)^k \begin{pmatrix} \Delta x_1(0) \\ \Delta x_2(0) \\ \vdots \\ \Delta x_{m-1}(0) \end{pmatrix} \right\| \le \left\| \left[a_{ij} \right]_{m-1\times m-1} \right\|^k \cdot \left\| \begin{pmatrix} \Delta x_1(0) \\ \Delta x_2(0) \\ \vdots \\ \Delta x_{m-1}(0) \end{pmatrix} \right\|. \quad (35)$$

From condition (ii) of Theorem 2, one has $\| [a_{ij}]_{m-1\times m-1} \| < 1$. Hence, the error system (35) is asymptotically stable. Therefore,

$$\lim_{k\to\infty} \left\| \Delta x_i(k) \right\| = \lim_{k\to\infty} \left\| x_i^{(d)}(k) - x_i^{(r)}(k) \right\| = 0, \quad (36)$$

where $i = 1, 2, \ldots, m-1$.

Furthermore, from condition (ii) of Theorem 2, $|a_{jj}| < 1$ $(j = m, m+1, \ldots, n)$ hold, such that

$$\begin{aligned} &\lim_{k\to\infty} \Delta x_j(k+1) \\ &= \lim_{k\to\infty} \left[a_{j1}\Delta x_1(k) + a_{j2}\Delta x_2(k) + \cdots + a_{jm-1}\Delta x_{m-1}(k) \right] \\ &\quad + \lim_{k\to\infty} a_{jj}\Delta x_j(k). \end{aligned} \quad (37)$$

Substituting (36) into (37), one has

$$\begin{aligned} \lim_{k\to\infty} \Delta x_j(k+1) &= \lim_{k\to\infty} a_{jj}\Delta x_j(k) \longrightarrow \lim_{k\to\infty} \Delta x_j(k) \\ &= \lim_{k\to\infty} \left| a_{jj} \right|^k \Delta x_j(0) = 0, \end{aligned} \quad (38)$$

where $j = m, m+1, \ldots, n$.

By combining (36) with (38), one has

$$\lim_{k\to\infty} \left\| \Delta x_i(k) \right\| = \lim_{k\to\infty} \left\| x_i^{(d)}(k) - x_i^{(r)}(k) \right\| = 0, \quad (39)$$

where $i = 1, 2, \ldots, n$.

From (39), it is concluded that the drive system (29) and the response system (30) can synchronize. Nevertheless, it should be noted that, in practical situations, only a few iterative steps are needed for synchronization. □

4.4. A 7D Three-Path Drive-Response Synchronization System. According to Figure 2 and (29)-(30), let $n = 7$. From (31)-(32), one gets $l = \text{round}(n/2) = 3$ and $m = n + 1 - l = 5$. A diagram for 7D three-path drive-response synchronization system is shown in Figure 3.

From Figure 3, the 7D drive system is obtained by

$$\begin{aligned}
x_1^{(d)}(k+1) &= f_1^{(d)}\left(X_1^{(d)}(k)\right) = a_{11}^{(d)}x_1^{(d)}(k) + a_{12}^{(d)}x_2^{(d)}(k) \\
&\quad + a_{13}^{(d)}x_3^{(d)}(k) + a_{14}^{(d)}x_4^{(d)}(k) \\
&\quad + a_{15}^{(d)}p_5(k) + a_{16}^{(d)}p_6(k) + a_{17}^{(d)}p_7(k) \\
&\quad + g_1^{(d)}\left(\sigma_1^{(d)}p_5(k), \varepsilon_1^{(d)}\right), \\
x_2^{(d)}(k+1) &= f_2^{(d)}\left(X_2^{(d)}(k)\right) = a_{21}^{(d)}x_1^{(d)}(k) + a_{22}^{(d)}x_2^{(d)}(k) \\
&\quad + a_{23}^{(d)}x_3^{(d)}(k) + a_{24}^{(d)}x_4^{(d)}(k) \\
&\quad + a_{25}^{(d)}p_5(k) + a_{26}^{(d)}p_6(k) + a_{27}^{(d)}p_7(k) \\
&\quad + g_2^{(d)}\left(\sigma_2^{(d)}p_6(k), \varepsilon_2^{(d)}\right), \\
x_3^{(d)}(k+1) &= f_3^{(d)}\left(X_3^{(d)}(k)\right) = a_{31}^{(d)}x_1^{(d)}(k) + a_{32}^{(d)}x_2^{(d)}(k) \\
&\quad + a_{33}^{(d)}x_3^{(d)}(k) + a_{34}^{(d)}x_4^{(d)}(k) \\
&\quad + a_{35}^{(d)}p_5(k) + a_{36}^{(d)}p_6(k) + a_{37}^{(d)}p_7(k) \\
&\quad + g_3^{(d)}\left(\sigma_3^{(d)}p_7(k), \varepsilon_3^{(d)}\right), \\
x_4^{(d)}(k+1) &= f_4^{(d)}\left(X_4^{(d)}(k)\right) = a_{41}^{(d)}x_1^{(d)}(k) + a_{42}^{(d)}x_2^{(d)}(k) \\
&\quad + a_{43}^{(d)}x_3^{(d)}(k) + a_{44}^{(d)}x_4^{(d)}(k) + a_{45}^{(d)}p_5(k) \\
&\quad + a_{46}^{(d)}p_6(k) + a_{47}^{(d)}p_7(k), \\
x_5^{(d)}(k+1) &= f_5^{(d)}\left(X_5^{(d)}(k)\right) = a_{51}^{(d)}x_1^{(d)}(k) + a_{52}^{(d)}x_2^{(d)}(k) \\
&\quad + a_{53}^{(d)}x_3^{(d)}(k) + a_{54}^{(d)}x_4^{(d)}(k) + a_{55}^{(d)}x_5^{(d)}(k) \\
&\quad + a_{56}^{(d)}p_6(k) + a_{57}^{(d)}p_7(k), \\
x_6^{(d)}(k+1) &= f_6^{(d)}\left(X_6^{(d)}(k)\right) = a_{61}^{(d)}x_1^{(d)}(k) + a_{62}^{(d)}x_2^{(d)}(k) \\
&\quad + a_{63}^{(d)}x_3^{(d)}(k) + a_{64}^{(d)}x_4^{(d)}(k) + a_{65}^{(d)}p_5(k) \\
&\quad + a_{66}^{(d)}x_6^{(d)}(k) + a_{67}^{(d)}p_7(k), \\
x_7^{(d)}(k+1) &= f_7^{(d)}\left(X_7^{(d)}(k)\right) = a_{71}^{(d)}x_1^{(d)}(k) + a_{72}^{(d)}x_2^{(d)}(k) \\
&\quad + a_{73}^{(d)}x_3^{(d)}(k) + a_{74}^{(d)}x_4^{(d)}(k) + a_{75}^{(d)}p_5(k) \\
&\quad + a_{76}^{(d)}p_6(k) + a_{77}^{(d)}x_7^{(d)}(k).
\end{aligned} \tag{40}$$

Similarly, the response system is described by

$$\begin{aligned}
x_1^{(r)}(k+1) &= f_1^{(r)}\left(X_1^{(r)}(k)\right) = a_{11}^{(r)}x_1^{(r)}(k) + a_{12}^{(r)}x_2^{(r)}(k) \\
&\quad + a_{13}^{(r)}x_3^{(r)}(k) + a_{14}^{(r)}x_4^{(r)}(k) + a_{15}^{(r)}p_5(k) \\
&\quad + a_{16}^{(r)}p_6(k) + a_{17}^{(r)}p_7(k) \\
&\quad + g_1^{(r)}\left(\sigma_1^{(r)}p_5(k), \varepsilon_1^{(r)}\right), \\
x_2^{(r)}(k+1) &= f_2^{(r)}\left(X_2^{(r)}(k)\right) = a_{21}^{(r)}x_1^{(r)}(k) + a_{22}^{(r)}x_2^{(r)}(k) \\
&\quad + a_{23}^{(r)}x_3^{(r)}(k) + a_{24}^{(r)}x_4^{(r)}(k) + a_{25}^{(r)}p_5(k) \\
&\quad + a_{26}^{(r)}p_6(k) + a_{27}^{(r)}p_7(k) \\
&\quad + g_2^{(r)}\left(\sigma_2^{(r)}p_6(k), \varepsilon_2^{(r)}\right), \\
x_3^{(r)}(k+1) &= f_3^{(r)}\left(X_3^{(r)}(k)\right) = a_{31}^{(r)}x_1^{(r)}(k) + a_{32}^{(r)}x_2^{(r)}(k) \\
&\quad + a_{33}^{(r)}x_3^{(r)}(k) + a_{34}^{(r)}x_4^{(r)}(k) + a_{35}^{(r)}p_5(k) \\
&\quad + a_{36}^{(r)}p_6(k) + a_{37}^{(r)}p_7(k) \\
&\quad + g_3^{(r)}\left(\sigma_3^{(r)}p_7(k), \varepsilon_3^{(r)}\right), \\
x_4^{(r)}(k+1) &= f_4^{(r)}\left(X_4^{(r)}(k)\right) = a_{41}^{(r)}x_1^{(r)}(k) + a_{42}^{(r)}x_2^{(r)}(k) \\
&\quad + a_{43}^{(r)}x_3^{(r)}(k) + a_{44}^{(r)}x_4^{(r)}(k) \\
&\quad + a_{45}^{(r)}p_5(k) + a_{46}^{(r)}p_6(k) + a_{47}^{(r)}p_7(k), \\
x_5^{(r)}(k+1) &= f_5^{(r)}\left(X_5^{(r)}(k)\right) = a_{51}^{(r)}x_1^{(r)}(k) + a_{52}^{(r)}x_2^{(r)}(k) \\
&\quad + a_{53}^{(r)}x_3^{(r)}(k) + a_{54}^{(r)}x_4^{(r)}(k) + a_{55}^{(r)}x_5^{(r)}(k) \\
&\quad + a_{56}^{(r)}p_6(k) + a_{57}^{(r)}p_7(k), \\
x_6^{(r)}(k+1) &= f_6^{(r)}\left(X_6^{(r)}(k)\right) = a_{61}^{(r)}x_1^{(r)}(k) + a_{62}^{(r)}x_2^{(r)}(k) \\
&\quad + a_{63}^{(r)}x_3^{(r)}(k) + a_{64}^{(r)}x_4^{(r)}(k) + a_{65}^{(r)}p_5(k) \\
&\quad + a_{66}^{(r)}x_6^{(r)}(k) + a_{67}^{(r)}p_7(k), \\
x_7^{(r)}(k+1) &= f_7^{(r)}\left(X_7^{(r)}(k)\right) = a_{71}^{(r)}x_1^{(r)}(k) + a_{72}^{(r)}x_2^{(r)}(k) \\
&\quad + a_{73}^{(r)}x_3^{(r)}(k) + a_{74}^{(r)}x_4^{(r)}(k) + a_{75}^{(r)}p_5(k) \\
&\quad + a_{76}^{(r)}p_6(k) + a_{77}^{(r)}x_7^{(r)}(k),
\end{aligned} \tag{41}$$

where the controller $g(\sigma x, \varepsilon) = \mathrm{mod}(\sigma x, \varepsilon)$ is determined by (24), parameters $a_{ij}^{(d)} = a_{ij}^{(r)} = a_{ij}$ $(1 \le i, j \le 7)$ are given by (23), and $\varepsilon_i^{(d)} = \varepsilon_i^{(r)}$, $\sigma_i^{(d)} = \sigma_i^{(r)}$ $(1 \le i \le 3)$ are

$$\begin{aligned}
&\varepsilon_1^{(d)} = \varepsilon_1^{(r)} = \varepsilon_1 = 1.6 \times 10^7, \quad && \sigma_1^{(d)} = \sigma_1^{(r)} = \sigma_1 = 2.3 \times 10^7, \\
&\varepsilon_2^{(d)} = \varepsilon_2^{(r)} = \varepsilon_2 = 3.3 \times 10^7, \quad && \sigma_2^{(d)} = \sigma_2^{(r)} = \sigma_2 = 4.2 \times 10^7, \\
&\varepsilon_3^{(d)} = \varepsilon_3^{(r)} = \varepsilon_3 = 6.7 \times 10^7, \quad && \sigma_3^{(d)} = \sigma_3^{(r)} = \sigma_3 = 5.0 \times 10^7.
\end{aligned} \tag{42}$$

According to (40) and (41), if all parameters exactly match, the synchronization simulation results are shown in Figure 4, from which one can see that the synchronization can be achieved only about 10 iterative steps needed. The

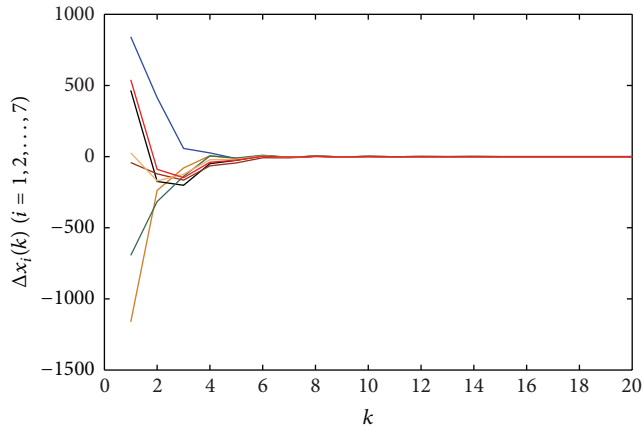


Figure 4: The synchronization simulation results.

Figure 5: FPGA embedded hardware system working platform.

receiver can decrypt three-path encrypted signals through synchronization, given by

$$\begin{aligned}
\widehat{s}_5(k) &= \left[s_5(k) + x_5^{(d)}(k)\right] - x_5^{(r)}(k) = s_5(k), \\
\widehat{s}_6(k) &= \left[s_6(k) + x_6^{(d)}(k)\right] - x_6^{(r)}(k) = s_6(k), \\
\widehat{s}_7(k) &= \left[s_7(k) + x_7^{(d)}(k)\right] - x_7^{(r)}(k) = s_7(k).
\end{aligned} \tag{43}$$

5. FPGA Embedded Implementation for Three Images Encryption and Decryption

In this section, a chaotic secure communication system for three digital color images encryption and decryption by using a 7D discrete time chaotic system is designed, based on FPGA embedded hardware system working platform with XUP Virtex-II type. The corresponding system design and hardware implementation results are then demonstrated. Furthermore, parameters safety performance test results are also given.

5.1. Hardware and Software Systems Design. FPGA embedded hardware system working platform with XUP Virtex-II type consists of three parts: an encrypter, a decryptor, and the Ethernet, as shown in Figure 5. Hardware design result of FPGA embedded system on chip is shown in Figure 6, which consists of twelve parts: (1) two processor cores (ppc405_0 and ppc405_1); (2) a processor local bus (PLB); (3) an on-chip peripheral bus (OPB); (4) a PLB to OPB bridge (plb2opb); (5) a DDR synchronous dynamic random access memory mounted on PLB (plb_ddr); (6) an OPB to device control register bus bridge (opb2dcr); (7) a joint test action group (JTAG); (8) a clock IP (clk_IP); (9) a controller mounted on OPB (opb_controller); (10) a block RAM mounted on PLB (plb_bram); (11) a video graphics array frame buffer (VGA frame buffer); (12) 57 input and output pins (Pin). Software system design consists of four parts: encryption algorithms, decryption algorithms, udp protocol, and six images display simultaneously, with their design flowcharts as shown in Figures 7, 8, 9, and 10, respectively.

In our hardware experiments, three 160 × 120 BMP digital color images with 24-bit per pixel are taken as typical examples. On the transmitter side, three 32-bit chaotic stream ciphers $x_5^{(d)}(k)$, $x_6^{(d)}(k)$, and $x_7^{(d)}(k)$ generated by 7D discrete-time chaotic system (29) are used for encrypting three 24-bit

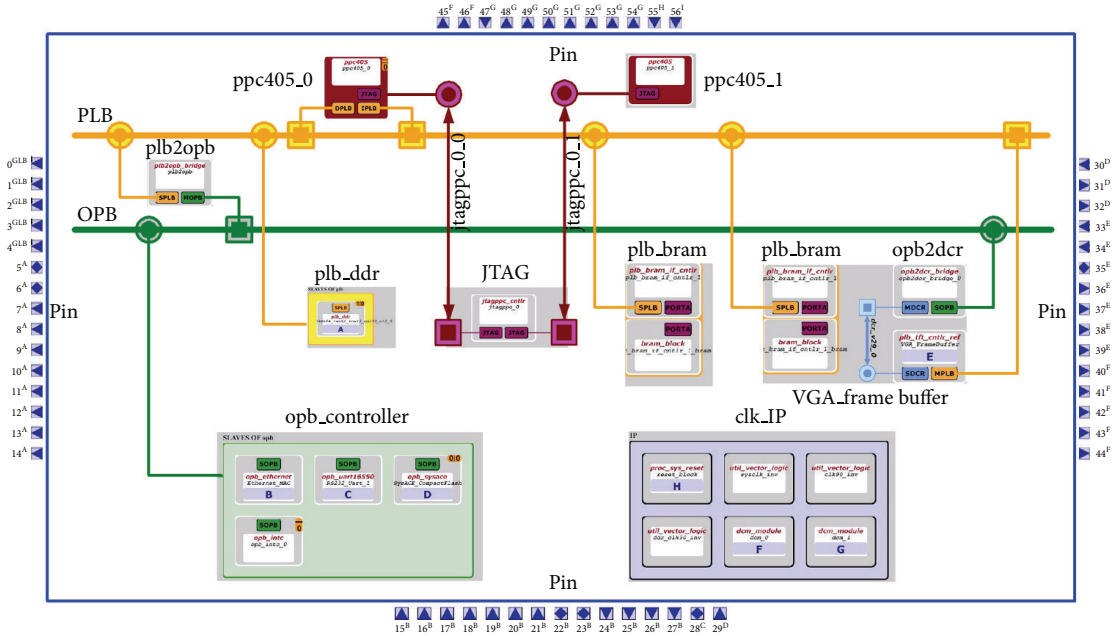


Figure 6: Hardware design results for FPGA embedded system on chip.

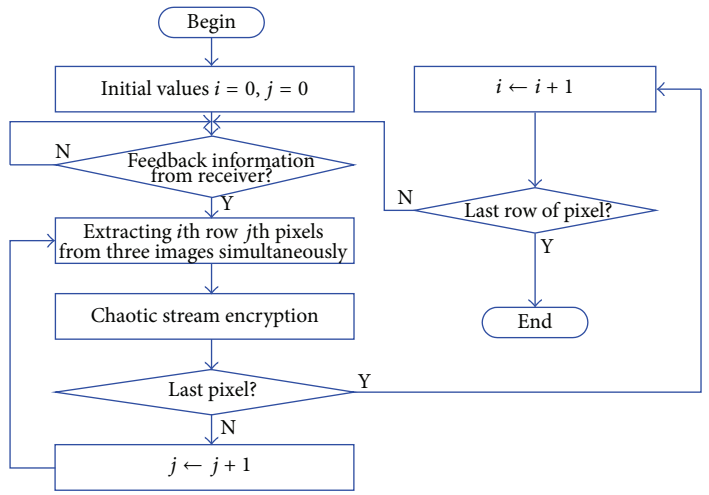


Figure 7: The flowchart for encryption.

pixels $s_5(k)$, $s_6(k)$, and $s_7(k)$ of the corresponding three digital color images simultaneously. For every 24-bit pixel, only 8-bit pixel is encrypted each time since the Ethernet transmission protocols and agreements are taken into account. Therefore, encrypting three 160 × 120 BMP digital color images with 24-bit per pixel needs to iterate 160 × 120 × 3 times. The three encrypted digital color images are transmitted through Ethernet by using the time division multiplexing approach. At the receiver end, three 32-bit chaotic stream ciphers $x_5^{(r)}(k)$, $x_6^{(r)}(k)$, and $x_7^{(r)}(k)$ generated by 7D discrete-time chaotic system (30) are used for the corresponding decrypting operation. When chaotic synchronization between the drive system (29) and the response system (30) is achieved, three encrypted digital color images can be decrypted.

5.2. Hardware Implementation Results. FPGA embedded hardware implementation results are shown in Figures 11, 12, 13, and 14. Among 7D chaotic attractors which are in agreement with simulation results given by Figures 1(a)–1(f), three original and encrypted images on the transmitter side (from top to bottom), three received encrypted and decrypted images at the receiver end (from top to bottom) are shown in Figures 11–13, all generated by FPGA. When all the parameters match exactly, the receiver can decrypt three original digital color images through synchronization, as shown in Figure 13. But the receiver cannot decrypt three original digital color images if the mismatched error of one parameter between the sender and the receiver reaches magnitude of 10^{-2}, even though other parameters match exactly, as shown in Figure 14.

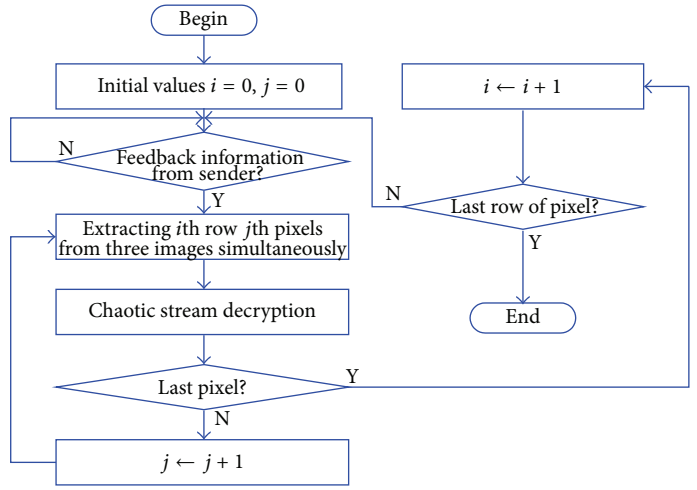


Figure 8: The flowchart for decryption.

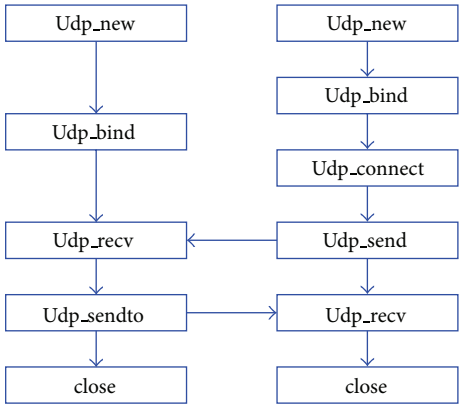


Figure 9: The flowchart for udp protocol.

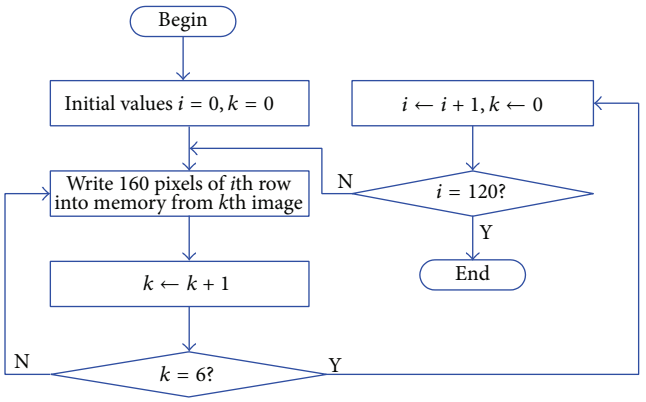


Figure 10: The flowchart for displaying six images simultaneously.

Figure 11: 7D chaotic attractors.

Figure 12: Three original and encrypted images on the transmitter side (from top to bottom).

6. NIST Safety Performance Test Results

In our NIST safety performance test for three images encryption and decryption systems (40) with (41), 10 sequences ($s = 10$) of 1,000,0000 bits are generated and tested. If the P value of any test is smaller than 0.0001, the sequences are considered to be not good enough and the generator is unsuitable. Table 1 shows P value of sequences $x_5(k)$, $x_6(k)$, and $x_7(k)$ based on discrete chaotic iterations using scheme. If there are at least two statistical values in a test, this test is marked with an asterisk and the average value is computed to characterize the statistics. We can see in Table 1 that the sequences have successfully passed the NIST statistical test suite.

Table 1: NIST test results of sequences $x_5(k)$, $x_6(k)$, and $x_7(k)$.

Statistical test	P value of $x_5(k)$	P value of $x_6(k)$	P value of $x_7(k)$
Frequency	0.616305	0.595549	0.798139
Block frequency ($m = 128$)	0.834308	0.181557	0.699313
Cumulative sums	0.462694	0.597927	0.099022
Runs	0.042808	0.153763	0.494392
Long runs of ones	0.090936	0.534146	0.534146
Rank	0.289667	0.366918	0.554420
Spectral DFT	0.108791	0.637119	0.867692
Nonoverlapping templates ($m = 9$)	0.383827	0.455937	0.514124
Overlapping templates ($m = 9$)	0.236810	0.699313	0.013569
Universal	0.334538	0.455937	0.637119
Approximate entropy ($m = 10$)	0.616305	0.275709	0.350485
Random excursions	0.3211526	0.236810	0.455937
Random excursions variant	0.299251	0.419021	0.236810
Linear complexity ($M = 500$)	0.494392	0.275709	0.739918
Serial ($m = 16$)	0.652483	0.398909	0.441177
Success	15/15	15/15	15/15

Figure 13: Three received encrypted and decrypted images at the receiver end (from top to bottom).

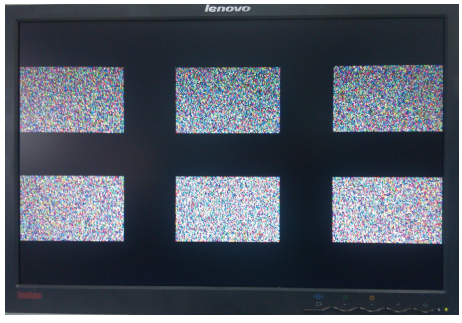


Figure 14: Three images cannot be decrypted if one parameter mismatches.

7. Conclusions

In order to break the traditional limitations that a chaotic system can only encrypt or decrypt one image, this paper has developed a systematic methodology for multi-images encryption and decryption by using single discrete time chaotic system. A generalized design principle and the corresponding implementation steps are also given. Based on the FPGA embedded hardware system working platform with XUP Virtex-II type, a chaotic secure communication system for three digital color images encryption and decryption by using a 7D discrete time chaotic system is designed and implemented, with hardware experiments and NIST safety performance tests demonstrated. Both theoretical analysis and experimental results confirm the feasibility of this approach.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 61172023 and by the Specialized Research Foundation of Doctoral Subjects of Chinese Education Ministry under Grant 20114420110003.

References

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

[2] S. J. Schiff, K. Jerger, D. H. Duong, T. Chang, M. L. Spano, and W. L. Ditto, "Controlling chaos in the brain," *Nature*, vol. 370, no. 6491, pp. 615–620, 1994.

[3] G. Chen and D. Lai, "Feedback control of Lyapunov exponents for discrete-time dynamical systems," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 6, no. 7, pp. 1341–1349, 1996.

[4] X. F. Wang and G. Chen, *Chaotification of Dynamical Systems-Theory, Method and Applications*, Shanghai Jiaotong University Press, Shanghai, China, 2006 (Chinese).

[5] G. Chen and D. Lai, "Feedback anticontrol of discrete chaos," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 8, no. 7, pp. 1585–1590, 1998.

[6] D. Lai and G. Chen, "Chaotification of discrete-time dynamical systems: an extension of the Chen-Lai algorithm," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 15, no. 1, pp. 109–117, 2005.

[7] C. Li and G. Chen, "On the Marotto-Li-Chen theorem and its application to chaotification of multi-dimensional discrete dynamical systems," *Chaos, Solitons & Fractals*, vol. 18, no. 4, pp. 807–817, 2003.

[8] X. F. Wang and G. Chen, "On feedback anticontrol of discrete chaos," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 9, no. 7, pp. 1435–1441, 1999.

[9] S. M. Yu, J. Lü, and G. Chen, *Anticontrol of Dynamical Systems and Its Applications*, Science Press, Beijing, China, 2013 (Chinese).

[10] S. Yu and G. Chen, "Anti-control of continuous-time dynamical systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 6, pp. 2617–2627, 2012.

[11] S. M. Yu and G. R. Chen, "Chaotifying continuous-time nonlinear autonomous systems," *International Journal of Bifurcation and Chaos*, vol. 17, pp. 2617–2627, 2012.

[12] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[13] G. Jakimoski and L. Kocarev, "Chaos and cryptography: block encryption ciphers based on chaotic maps," *IEEE Transactions on Circuits and Systems. I: Fundamental Theory and Applications*, vol. 48, no. 2, pp. 163–169, 2001.

[14] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 8, no. 6, pp. 1259–1284, 1998.

[15] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos, Solitons & Fractals*, vol. 32, no. 4, pp. 1518–1529, 2007.

[16] K. D. Rao and C. Gangadhar, "Discrete wavelet transform and modified chaotic key-based algorithm for image encryption and its VLSI realization," *IETE Journal of Research*, vol. 58, no. 2, pp. 114–120, 2012.

[17] H. Khanzadi, M. Eshghi, and S. E. Borujeni, "Design and FPGA implementation of a pseudo random bit generator using chaotic maps," *IETE Journal of Research*, vol. 59, pp. 63–73, 2013.

[18] M. S. Azzaz, C. Tanougast, S. Sadoudi, A. Bouridane, and A. Dandache, "FPGA implementation of new real-time image encryption based switching chaotic systems," in *Proceedings of the IET Irish Signals and Systems Conference (ISSC '09)*, pp. 1–6, 2009.

[19] M. S. Azzaz, C. Tanougast, S. Sadoudi, R. Fellah, and A. Dandache, "A new auto-switched chaotic system and its FPGA implementation," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 7, pp. 1792–1804, 2013.

[20] H.-C. Chen and J.-C. Yen, "A new cryptography system and its VLSI realization," *Journal of Systems Architecture*, vol. 49, no. 7–9, pp. 355–367, 2003.

[21] R. Mitter and M. Sridevi Sathya Priya, "A non linear equation based cryptosystem for image encryption and decryption," in *Proceedings of the International Conference on Computing, Electronics and Electrical Technologies (ICCEET '12)*, pp. 533–537, Kumaracoil, India, March 2012.

[22] K. D. Rao and C. Gangadhar, "Finite field DWT and MCKBA for image encryption and its VLSI realization," in *Proceedings of the 8th International Conference on Information, Communications and Signal Processing (ICICS '11)*, pp. 1–5, Singapore, December 2011.

[23] J. Giesl, L. Behal, and K. Vlcek, "Hardware solution of chaos based image encryption," in *Proceedings of the IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS '09)*, pp. 198–201, Liberec, Czech Republic, April 2009.

[24] M. S. Azzaz, C. Tanougast, S. Sadoudi, A. Dandache, and F. Monteiro, "Real-time image encryption based chaotic synchronized embedded cryptosystems," in *Proceedings of the 8th IEEE International NEWCAS Conference (NEWCAS '10)*, pp. 61–64, Montreal, Canada, June 2010.

[25] K. D. Rao and C. Gangadhar, "VLSI realization of a secure cryptosystem for image encryption and decryption," in *Proceedings of the International Conference on Communications and Signal Processing (ICCSP '11)*, pp. 543–547, Kozhikode, India, February 2011.

[26] J. C. Yen and J. I. Guo, "Efficient hierarchical chaotic image encryption algorithm and its VLSI realization," *IEE Proceedings-Vision, Image and Signal Processing*, vol. 147, pp. 167–175, 2000.