doi:10.3969/j.issn.1672-1292.2019.01.002

异构磁控忆阻混沌电路的同步及其在彩色图像加密中的应用

吕晏旻[1],闵富红[1],彭光娅[1],张若飞[2]

(1.南京师范大学电气与自动化工程学院,江苏 南京 210023)
(2.南京环网动力设备有限公司,江苏 南京 210042)

[**摘要**] 基于 Lyapunov 稳定性理论,设计一种含有指数函数的非线性同步控制器,实现了异构磁控忆阻混沌系统之间的完全同步、比例投影同步和函数投影同步. 通过误差曲线、同步时序图及同步相图等证明同步控制器的有效性与可行性. 选择合适的密钥,实现异构忆阻系统同步在彩色图像加密中的应用,通过直方图、相关性及密钥敏感性分析验证了加密效果. 结果表明,将这种忆阻混沌同步应用到图像加密中具有很高的研究价值与工程意义.

[**关键词**] 异构忆阻系统,完全同步,投影同步,彩色图像加密
[**中图分类号**]O415.5　[**文献标志码**]A　[**文章编号**]1672-1292(2019)01-0008-11

Synchronization of Heterogeneous Magnetron Memristive Chaotic Circuits and Its Application in Color Image Encryption

Lü Yanmin[1], Min Fuhong[1], Peng Guangya[1], Zhang Ruofei[2]

(1.School of Electrical and Automation Engineering, Nanjing Normal University, Nanjing 210023, China)
(2.Nanjing Power Equipment Company, Nanjing 210042, China)

Abstract: This paper, based on Lyapunov stability theory, designs the nonlinear synchronization controller with exponential function, which is used to realize complete synchronization, proportional projective synchronization and function projective synchronization between two heterogeneous memristor-based chaotic systems. Subsequently, the validity and feasibility of the synchronization controller are proved by the error curve, the synchronous sequence diagrams and synchronous phase. Moreover, the application of the synchronization in color image encryption is fulfilled by selecting appropriate keys. Correspondingly, the effect of encryption is verified by the analysis of histogram, correlation and key sensitivity. Finally, it is found that the application of the synchronization of memristive systems in image encryption is meaningful and valuable through memerical results.

Key words: heterogeneous memristive system, complete synchronization, projective synchronization, color image encryption

近年来,随着忆阻器模型的物理实现及忆阻混沌系统动力学分析与研究的广泛展开,忆阻混沌系统的同步控制研究在国内外掀起热潮[1-4]. 目前多数文献的同步研究范围还仅限于同构忆阻混沌系统. 文献[5]利用脉冲控制法,设计基于三次光滑磁控双忆阻模型的蔡氏混沌系统耦合同步控制器. 文献[6]依据 Lyapunov 稳定性理论,设计非线性主动控制器,实现一种忆阻混沌系统的改进投影同步. 文献[7]针对多忆阻混沌系统实现组合同步. 随着同构系统同步研究的不断发展,异构系统的混沌同步也成为近几年研究的新热点. 文献[8-9]弥补性地提出了广义混沌同步控制器,并将其应用在异构混沌系统之中. 学者们对异构忆阻混沌系统的同步也进行了初步探索. 文献[10]基于滑模控制器,实现了两个异构忆阻系统之间的同步. 文献[11]将提出的主动反推控制技术应用到两个异构忆阻混沌系统之间,完成了两个系统之

收稿日期:2018-04-28.
基金项目:国家自然科学基金(61871230).
通讯联系人:闵富红,博士,教授,研究方向:非线性电路系统. E-mail:minfuhong@ njnu.edu.cn

间的多种同步. 然而,目前针对异构忆阻混沌系统同步控制的研究仍然较少,异构忆阻混沌系统具有更加复杂且丰富的动力学行为,其同步的实现将为之后一系列应用奠定基础,有一定研究价值.

随着混沌同步理论研究的深入,其在保密通信中的应用也成为一个重要研究方向. 用混沌同步来加密信息将很难被破译,具有很高的保密度,且使用范围广,不仅可用于静态加密场合,也可处理实时信号[12]. 文献[13]实现了两个同构系统的错位投影同步,并将其应用到灰色图像加密之中. 文献[14]设计了一个同步混沌系统,将其应用范围拓展到彩色图像加密. 文献[15]重点研究同步系统的加密算法,基于混沌系统对初值及参数的敏感度,以此验证混沌同步加密拥有更大的密钥空间、更强的抗破译能力. 而关于忆阻系统同步在保密通信中的应用研究还较少见. 由于忆阻器的自身特性,其同步后的加密序列较传统混沌同步系统具有更高的初值敏感性、更强的类随机和连续宽带功率谱特性[16-17]. 因此,若将忆阻混沌系统的同步运用到彩色图像加密中,其密钥空间增大,抗破译能力也会相应提高.

本文基于 Lyapunov 稳定性原理,针对两个结构不同但维数相同的磁控忆阻混沌电路,设计含有指数项的非线性同步控制器. 该控制器结构简单,可实现有源磁控 Lorenz-like 忆阻混沌系统与 Chua-like 忆阻混沌系统之间的完全同步、正反比例投影同步和函数投影同步. 异构系统之间多种同步的实现,可为后续其在保密通信中的应用打下基础. 随后,通过分析两个忆阻系统的混沌序列,选取到合适的密钥,将忆阻混沌系统的同步应用到彩色图像加密中. 将彩色图像分为三色进行处理,针对每一种颜色设计一个初值,即对应 8 个密钥,通过直方图、相关性分析及密钥敏感性等验证加密效果. 数值仿真结果表明,将此异构系统同步应用到图像加密中,在扩大密钥空间的同时,也增强了图像信息的破译难度,拥有一定可行性.

1 同步控制器的设计

设两个结构不同的 n 维动力学系统:$\dot{x}_i(i=1,2,3,\cdots,n)=f_i(x_1,x_2,x_3,\cdots x_n)$ 为驱动系统,$\dot{y}_i(i=1,2,3,\cdots,n)=g_i(y_1,y_2,y_3,\cdots,y_n)+u_i$ 为响应系统,其中,x_i 为驱动系统的状态变量,y_i 为响应系统的状态变量,u_i 为所设计的同步控制器,则驱动系统如式(1)所示:

$$\begin{aligned}
\dot{x}_1&=f_1(x_1,x_2,x_3,\cdots,x_n),\\
\dot{x}_2&=f_2(x_1,x_2,x_3,\cdots,x_n),\\
\dot{x}_3&=f_3(x_1,x_2,x_3,\cdots,x_n),\\
&\vdots\\
\dot{x}_n&=f_n(x_1,x_2,x_3,\cdots,x_n).
\end{aligned}\tag{1}$$

响应系统如式(2)所示:

$$\begin{aligned}
\dot{y}_1&=g_1(y_1,y_2,y_3,\cdots,y_n)+u_1,\\
\dot{y}_2&=g_2(y_1,y_2,y_3,\cdots,y_n)+u_2,\\
\dot{y}_3&=g_3(y_1,y_2,y_3,\cdots,y_n)+u_3,\\
&\vdots\\
\dot{y}_n&=g_n(y_1,y_2,y_3,\cdots,y_n)+u_n.
\end{aligned}\tag{2}$$

定义驱动系统和响应系统之间的同步误差为 $e_i=y_i-\alpha x_i, i=1,2,\cdots,n$. α 为设定的比例系数或比例函数,当 $\alpha=1$ 时,驱动系统与响应系统实现完全同步;当 $\alpha\in\mathbf{R}^n\cap\alpha\neq1\cap a\neq0$ 时,驱动系统与响应系统成不同比例投影同步;当 α 为关于时间 t 的函数时,驱动系统与响应系统成函数投影同步. 若要实现驱动系统与响应系统同步,则驱动系统和响应系统要满足如下关系式:

$$\lim_{t\to\infty}\|\boldsymbol{e}_i\|=\lim_{t\to\infty}\|y_i-\alpha x_i\|=0.\tag{3}$$

此时,即可将两个不同系统的同步控制问题转化为对同步误差的控制问题. 因此,可得误差系统动力学方程为:

$$\begin{aligned}
&\dot{e}_1=g_1(y_1,y_2,y_3,\cdots,y_n)-\dot{\alpha}x_1-\alpha f_1(x_1,x_2,x_3,\cdots,x_n)+u_1,\\
&\dot{e}_2=g_2(y_1,y_2,y_3,\cdots,y_n)-\dot{\alpha}x_2-\alpha f_2(x_1,x_2,x_3,\cdots,x_n)+u_2,\\
&\dot{e}_3=g_3(y_1,y_2,y_3,\cdots,y_n)-\dot{\alpha}x_3-\alpha f_3(x_1,x_2,x_3,\cdots,x_n)+u_3,\\
&\qquad\vdots\\
&\dot{e}_n=g_n(y_1,y_2,y_3,\cdots,y_n)-\dot{\alpha}x_n-\alpha f_n(x_1,x_2,x_3,\cdots,x_n)+u_n.
\end{aligned}\tag{4}$$

根据 Lyapunov 渐进稳定性定理,设计正定二次型函数 $\boldsymbol{V}=\frac{1}{2}\boldsymbol{e}^{\mathrm{T}}\boldsymbol{e}$ 作 Lyapunov 函数,若有 $\dot{\boldsymbol{V}}=\dot{\boldsymbol{e}}^{\mathrm{T}}\boldsymbol{e}$,只要 $\dot{\boldsymbol{V}}$ 半负定,则系统(4)是大范围渐进稳定的,因而两个系统同步控制问题又可间接转化为对控制规律及控制参数的选择问题. 以下将以实现两个特定忆阻混沌系统之间的同步为例,对实现异构忆阻混沌系统的同步进行具体说明.

2　异构忆阻混沌系统的同步控制

令文献[18]中提出的 Chua-like 系统为驱动系统,设为忆阻混沌系统Ⅰ. 此系统为基于经典 Chua 电路构建的有源磁控忆阻混沌系统,其数学模型为:

$$\begin{cases}
\dot{x}_1=\alpha_1(z_1-W(w_1)x_1),\\
\dot{y}_1=\beta_1y_1-z_1,\\
\dot{z}_1=y_1-x_1-\xi_1z_1,\\
\dot{w}_1=x_1.
\end{cases}\tag{5}$$

式中,$W(w_1)=a+3bw_1^2$,即三次有源磁控忆阻器的数学模型,w_1 为忆阻器的磁通量,a 和 b 为决定忆阻器特征的忆阻参数;α、β 和 ξ 为决定系统运动状态的系统参数. 选择电路参数为 $a=-0.4$,$b=0.8$,$\alpha_1=4$,$\beta_1=0.7$,$\xi_1=0.1$.

令文献[19]中的 Lorenz-like 系统为响应系统,设为忆阻混沌系统Ⅱ. 此系统为基于经典 Lorenz 系统构建的有源磁控忆阻混沌系统,其数学模型为:

$$\begin{cases}
\dot{x}_2=36y_2z_2-\alpha_2x_2-z_2W(w_2)+u_1,\\
\dot{y}_2=\xi_2y_2-\beta_2x_2z_2+u_2,\\
\dot{z}_2=8x_2y_2-\gamma_2z_2+u_3,\\
\dot{w}_2=x_2+u_4.
\end{cases}\tag{6}$$

式中,$W(w_2)=a+3bw_2^2$;u_1、u_2、u_3 和 u_4 为所设计的同步控制器. 选择电路参数 $a=-0.5$,$b=0.8$,$\alpha_2=15$,$\beta_2=8$,$\xi_2=1.68$,$\gamma_2=15.15$.

定义同步误差为:

$$\begin{cases}
e_1=x_2-\alpha x_1,\\
e_2=y_2-\alpha y_1,\\
e_3=z_2-\alpha z_1,\\
e_4=w_2-\alpha w_1.
\end{cases}\tag{7}$$

根据式(4)可得如下误差系统动力学方程:

$$\begin{cases}
\dot{e}_1=36y_2z_2-\alpha_2x_2-z_2W(w_2)-\dot{\alpha}x_1-\alpha(\alpha_1(z_1-W(w_1)x_1))+u_1,\\
\dot{e}_2=\xi_2y_2-\beta_2x_2z_2-\dot{\alpha}y_1-\alpha(\beta_1y_1-z_1)+u_2,\\
\dot{e}_3=8x_2y_2-\gamma_2z_2-\dot{\alpha}z_1-\alpha(y_1-x_1-\xi_1z_1)+u_3,\\
\dot{e}_4=x_2-\dot{\alpha}w_1-\alpha x_1+u_4.
\end{cases}\tag{8}$$

式中,α 是设定的比例系数或比例函数. 选择如下非线性反馈控制函数:

$$\begin{cases}\dot{u}_1=\dot{\alpha}x_2/\alpha+\alpha(\alpha_1(z_1-W(w_1)x_1))-36y_2z_2+\alpha_2x_2+z_2W(w_2)-k_1^{|\mathrm{sign}(e_1)|}e_1,\\ \dot{u}_2=\dot{\alpha}y_2/\alpha+\alpha(\beta_1y_1-z_1)-\xi_2y_2+\beta_2x_2z_2-k_2^{|\mathrm{sign}(e_2)|}e_2,\\ \dot{u}_3=\dot{\alpha}z_2/\alpha+\alpha(y_1-x_1-\xi_1z_1)-8x_2y_2+\gamma_2z_2-k_3^{|\mathrm{sign}(e_3)|}e_3,\\ \dot{u}_4=\dot{\alpha}w_2/\alpha+\alpha x_1-x_2-k_4^{|\mathrm{sign}(e_4)|}e_4.\end{cases}\tag{9}$$

将式(9)代入式(8),得到如下误差方程:

$$\begin{cases}\dot{e}_1=\dot{\alpha}e_1/\alpha-k_1^{|\mathrm{sign}(e_1)|}e_1,\\ \dot{e}_2=\dot{\alpha}e_2/\alpha-k_2^{|\mathrm{sign}(e_2)|}e_2,\\ \dot{e}_3=\dot{\alpha}e_3/\alpha-k_3^{|\mathrm{sign}(e_3)|}e_3,\\ \dot{e}_4=\dot{\alpha}e_4/\alpha-k_4^{|\mathrm{sign}(e_4)|}e_4.\end{cases}\tag{10}$$

此时,分析驱动系统与响应系统的同步问题,可转化为分析误差系统(8)的稳定性问题.

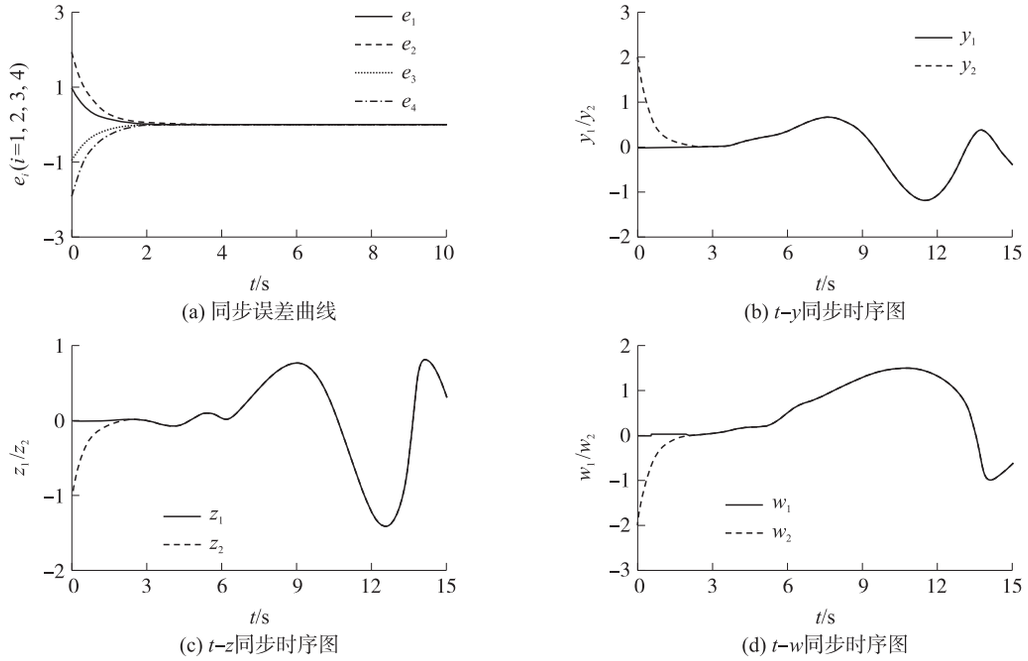
构造 Lyapunov 函数为 $\boldsymbol{V}=\frac{1}{2}\boldsymbol{e}^{\mathrm{T}}\boldsymbol{e}$,对关于时间 t 进行求导,可得:

$$\dot{\boldsymbol{V}}=\dot{\boldsymbol{e}}^{\mathrm{T}}\boldsymbol{e}=e_1\dot{e}_1+e_2\dot{e}_2+e_3\dot{e}_3+e_4\dot{e}_4=\dot{\alpha}e_1^2/\alpha-k_1^{|\mathrm{sign}(e_1)|}e_1^2+\dot{\alpha}e_2^2/\alpha-k_2^{|\mathrm{sign}(e_2)|}e_2^2+\dot{\alpha}e_3^2/\alpha-k_3^{|\mathrm{sign}(e_3)|}e_3^2+\dot{\alpha}e_4^2/\alpha-k_4^{|\mathrm{sign}(e_4)|}e_4^2=$$
$$(\dot{\alpha}/\alpha-k_1^{|\mathrm{sign}(e_1)|})e_1^2+(\dot{\alpha}/\alpha-k_2^{|\mathrm{sign}(e_2)|})e_2^2+(\dot{\alpha}/\alpha-k_3^{|\mathrm{sign}(e_3)|})e_3^2+(\dot{\alpha}/\alpha-k_4^{|\mathrm{sign}(e_4)|})e_4^2.\tag{11}$$

由此可知,当满足 $\dot{\alpha}/\alpha-k_i^{|\mathrm{sign}(e_i)|}<0(i=1,2,3,4)$ 时,一定有 $\dot{\boldsymbol{V}}$ 半负定,则可实现驱动系统与响应系统同步. 当 $\alpha\in\mathbf{R}$ 时,只需满足 $-k_i^{|\mathrm{sign}(e_i)|}<0(i=1,2,3,4)$,即 $k_i>0(i=1,2,3,4)$,驱动系统与响应系统即可实现完全同步($\alpha=1$)或不同比例投影同步($\alpha\in\mathbf{R}^n\cap\alpha\neq1\cap a\neq0$). 当 α 是关于时间 t 的函数时,关于 α 的选择和 $k_i(i=1,2,3,4)$ 的取值有多种组合,满足 $\dot{\alpha}/\alpha-k_i^{|\mathrm{sign}(e_i)|}<0(i=1,2,3,4)$ 时,即可实现驱动系统与响应系统之间的函数投影同步.

2.1 异构忆阻混沌系统的完全同步

如上分析,当 $\alpha=1$ 时,只需满足 $k_i>0(i=1,2,3,4)$,驱动系统与响应系统即可实现完全同步. 为了体现该同步器的优越性,随机取 $k_1=k_2=k_3=k_4=2$,并随机设置有源磁控忆阻混沌系统Ⅰ和忆阻混沌系统Ⅱ的初始条件为$(x_{1o1},y_{1o1},z_{1o1},w_{1o1},x_{2o2},y_{2o2},z_{2o2},w_{2o2})=(0.01,0,0,0,1,2,-1,-2)$. 同步误差曲线如图 1(a)所示,可以看出,两个不同的忆阻混沌系统大约在 $t=2.5$ s 时达到完全同步. 同步时序图如图 1(b)、(c)、(d)所示,状态变量的时序图均呈现出驱动系统和响应系统在 $t=2.5$ s 左右达到完全同步.



(a) 同步误差曲线　(b) t–y同步时序图

(c) t–z同步时序图　(d) t–w同步时序图

图 1　完全同步仿真图($\alpha=1$)

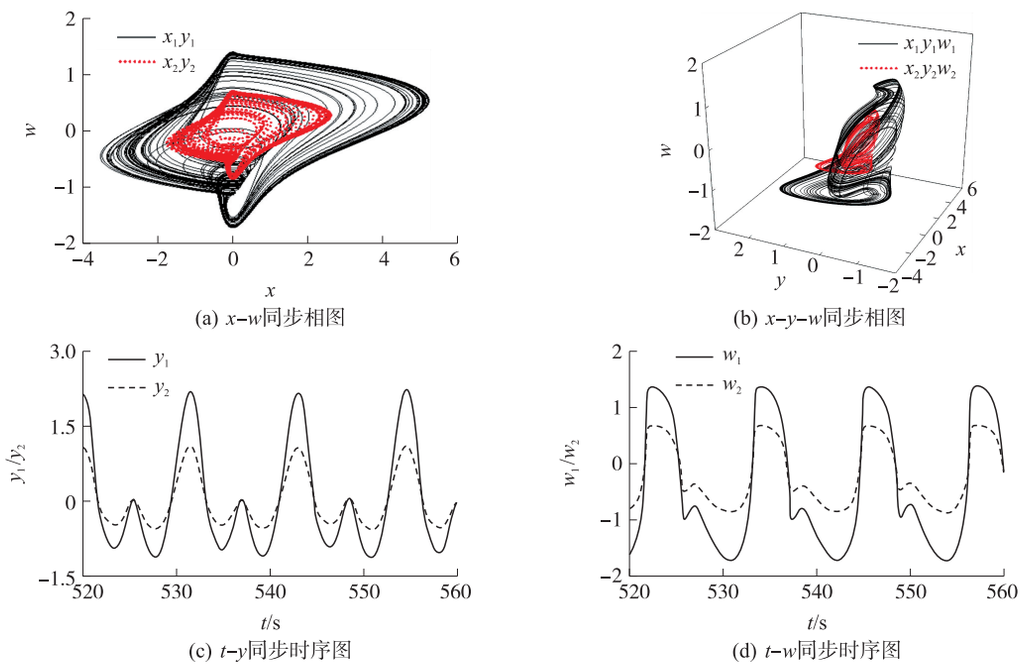
Fig. 1　The diagram of full synchronization($\alpha=1$)

2.2　异构忆阻混沌系统的不同比例投影同步

当 $\alpha\in\mathbf{R}^n\cap\alpha\neq1\cap a\neq0$ 时,实现两个不同忆阻混沌系统的不同比例投影同步,同样只需满足 $k_i>0(i=1,2,3,4)$,驱动系统与响应系统即可实现比例投影同步. 根据 $k_i>0(i=1,2,3,4)$ 这个条件,$k_i(i=1,2,3,4)$ 的值可以随机再取一组数据,如:$k_1=1,k_2=2,k_3=3,k_4=4$,并同样随机设置忆阻混沌系统Ⅰ和忆阻混沌系统Ⅱ的初始条件为 $(x_{1o2},y_{1o2},z_{1o2},w_{1o2},x_{2o2},y_{2o2},z_{2o2},w_{2o2})=(-1,1,2,-1,0.01,0,0,0)$.

2.2.1　$\alpha=0.5$ 时的比例投影同步

当 $\alpha=0.5$ 时,意味着响应系统中各个状态变量的数值均是由驱动系统相应变量的相应数值缩小两倍所得. 同步相图如图 2(a)、(b)所示,图中黑色线条描绘驱动系统产生的吸引子,灰色为响应系统产生的吸引子. 可以清楚地观察到,响应系统与驱动系统的投影同步比例为 0.5,满足同步控制器的设计要求. 以两个状态变量的时序图加以说明,如图 2(c)、(d)所示,亦能清楚地观察到响应系统中各个状态变量的数值是驱动系统相应变量数值的 0.5 倍,满足 0.5 倍投影同步比例的要求.



(a) x–w同步相图　(b) x–y–w同步相图

(c) t–y同步时序图　(d) t–w同步时序图

图 2　正比例投影同步仿真图($\alpha=0.5$)

Fig. 2　The diagram of positive proportional projection synchronization($\alpha=0.5$)

2.2.2　$\alpha=-2$ 时的比例投影同步

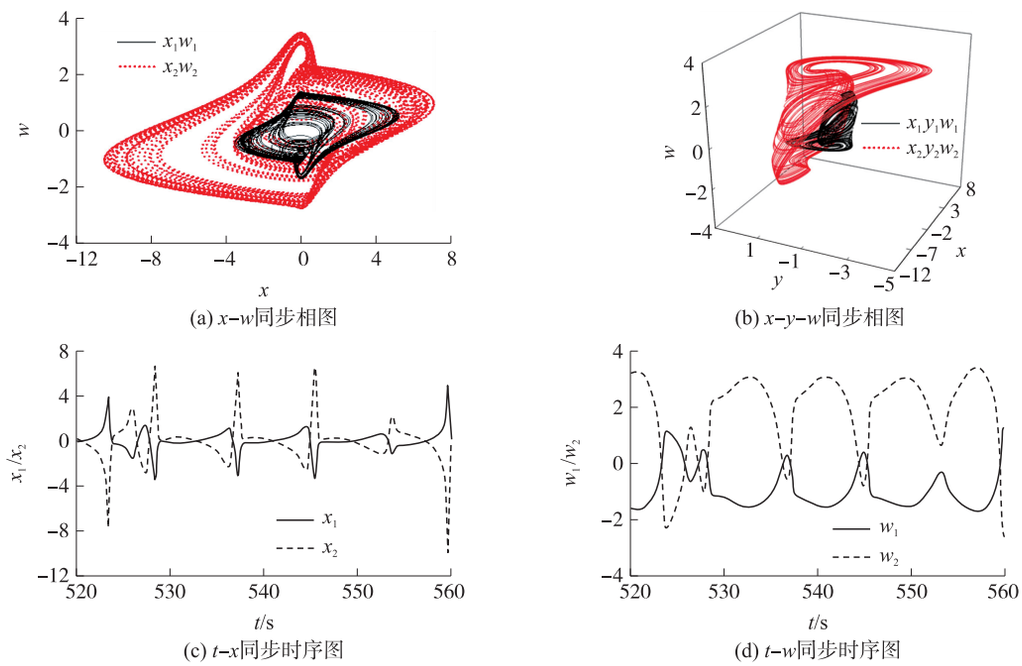
当 $\alpha=-2$ 时,意味着响应系统中各个状态变量的数值均是由驱动系统相应变量的相应数值扩大两倍并取相反数所得. 同步相图如图 3(a)、(b)所示,图中黑色区域为驱动系统产生的吸引子,灰色区域为响应系统产生的吸引子. 可以清楚地观察到,响应系统与驱动系统的投影同步比例为−2,满足同步控制器的设计要求. 列举两个状态变量的时序图如图 3(c)、(d)所示,从时序图亦能清楚地观察到响应系统中各个状态变量的数值是驱动系统相应变量数值的−2 倍,满足−2 倍投影同步比例的要求.

2.3　异构忆阻混沌系统的函数投影同步

当 α 是关于时间 t 的函数时,满足 $\dot{\alpha}/\alpha-k_i^{|\mathrm{sign}(e_i)|}<0(i=1,2,3,4)$,即可实现系统(5)与系统(6)间的函数投影同步. 关于 α 的选择和 $k_i(i=1,2,3,4)$ 的取值有多种组合,随机取 $\alpha=-1+0.5\sin t$ 和 $k_1=k_2=k_3=k_4=2$,则可得到 $\dot{\alpha}=0.5\cos t,-k_i^{|\mathrm{sign}(e_i)|}(i=1,2,3,4)\in\{-1,-2\}$,即满足 $\dot{\alpha}/\alpha-k_i^{|\mathrm{sign}(e_i)|}<0(i=1,2,3,4)$,此时函数投影同步控制方法进一步得到验证.

为了与不同比例投影同步形成对比,驱动和响应系统的初始值同样设置为 $(x_{1o2},y_{1o2},z_{1o2},w_{1o2},x_{2o2},y_{2o2},z_{2o2},w_{2o2})=(-1,1,2,-1,0.01,0,0,0)$. 同步相图如图 4(a)和(b)所示,图中黑色代表驱动系统的吸引子,灰色代表响应系统的吸引子. 可以看出,该状态下的同步状态不同于上述的正、反比例投影同步,而是由关于时间 t 的函数决定,也满足此时控制器的控制要求. 同时,从时序图也可验证这一现象,如图 4(c)

和(d)所示,变量之间的变化遵循一定规律但又不单单是比例或方向上的变化,同样证实了此时的同步状态是由时间函数 t 决定的.

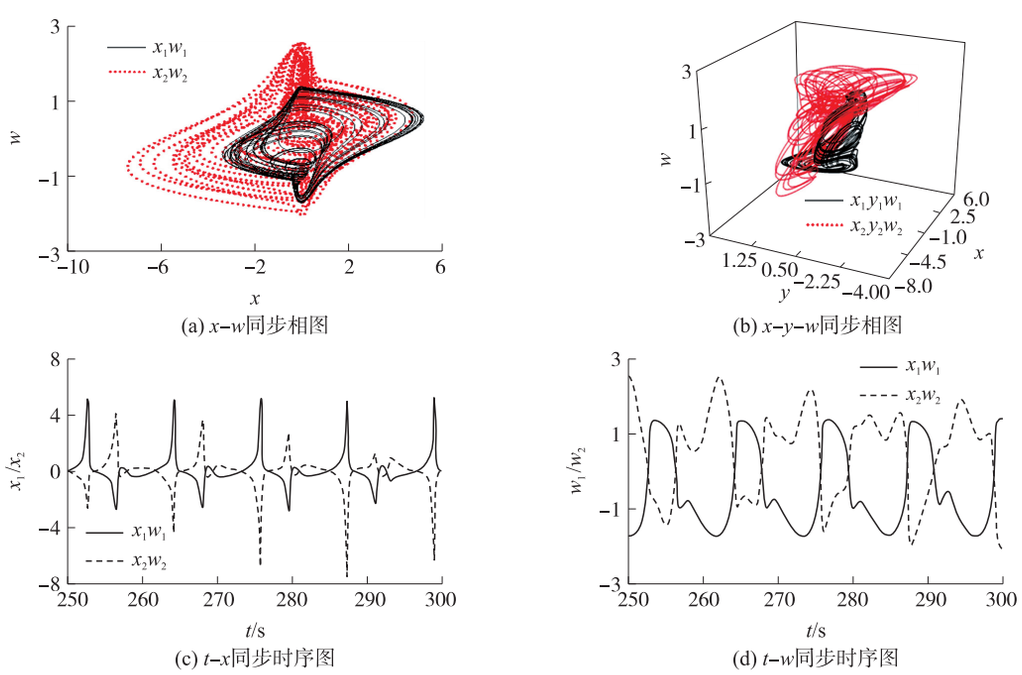


(a) x–w同步相图　(b) x–y–w同步相图

(c) t–x同步时序图　(d) t–w同步时序图

图 3　反比例投影同步仿真图($\alpha=-2$)

Fig. 3　The diagram of back projection synchronization($\alpha=-2$)



(a) x–w同步相图　(b) x–y–w同步相图

(c) t–x同步时序图　(d) t–w同步时序图

图 4　函数投影同步仿真图

Fig. 4　The diagram of functional projection synchronization

3　在彩色图像加密中的应用

混沌信号具有高度随机、不可预测及高度复杂等特性,故其在保密通信中具有良好的应用前景. 基于上文讨论,本节将混沌同步应用于彩色图像加密之中,在实现驱动系统与响应系统的完全同步的条件下,则可解调出有用信号.

加密与解密框图如图 5 所示,忆阻混沌系统 Ⅰ 和 Ⅱ 在同步控制下实现完全同步,进而产生混沌同步控

制信号. 将经算法处理的离散序列作为密钥,原始图像和密钥在加密算法的作用下进行加密变换,生成加密图像,完成加密过程. 解密过程则相当于一个逆过程,解密密钥为混沌同步控制信号产生的混沌序列,加密后的图像和密钥经过解密变换生成解密图像,完成解密. 最后,对比原始图像和解密后的图像,验证加密算法的可靠性.

本加密算法将同步系统的初始状态,即 8 个状态变量作为加密算法的密钥. 同时,将彩色图像分为 R、G、B 三色进行处理,针对每个颜色设置一个初始条件,一种颜色对应 8 个密钥,则 3 种颜色对应 24 个密钥,从而密钥空间大大增大,加密的抗破译能力增强.

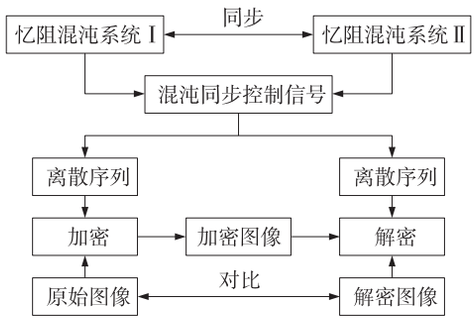
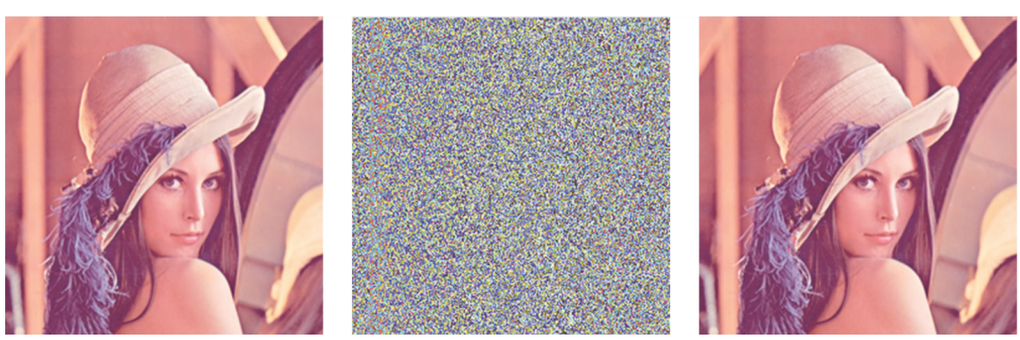


图 5　加密与解密框图

Fig. 5　The diagram of encryption and decryption

结合忆阻混沌系统的多稳态特性,为确保按混沌序列进行加密,将 RGB 的密钥设置为 $k_R=(0.01,0,0,0,0.1,0.1,0,0)$,$k_G=(0.01,0,0,-1.4,0.1,0.1,0.1,0.1)$,$k_B=(0.01,0,0,0.15,0.2,0.2,0.2,0.2)$. 从密钥设置可见,选择同步系统混沌态的序列作为密钥进行加密,驱动系统的密钥确保是混沌态即可,响应系统对应的密钥完全随机,进一步增加了破译的难度. 选取如图 6(a)所示的经典“Lean”彩色图像作为加密测试图像,图像大小为 256×256,加密和解密后的图像分别如图 6(b)、(c)所示. 加密和解密效果图显示,此算法具有较好的可行性与有效性.



(a) 原图　　(b) 加密效果图　　(c) 解密效果图

图 6　图像加密与解密效果图

Fig. 6　The effect map of image encryption and decryption

加密的安全性主要依赖于密钥的安全性,而密钥的安全性则与密钥空间的大小、密文对密钥的敏感性、密文的抗攻击能力等有关. 通常,加密后的图像越“模糊”表示加密的安全性越高. 以下将从直方图、相关性和密钥敏感性等 3 方面来分析加密效果.

3.1　直方图分析

直方图反映了图像的统计特征,每张图像均有特定的直方图,能够衡量图像加密算法的扰乱性.

直方图可以直观地反映图像的统计特征和加密前后图像发生的变化. 原始图像 R、G、B 3 个分量的直方图如图 7(a)、(b)、(c)所示,(d)、(e)和(f)分别为这 3 个分量加密后的直方图. 根据加密前后直方图的对比可见,原始图像的像素分布很不均匀,加密后的直方图不再具有原始图像的统计特征,明文图像的统计特征已扩散到加密图像中,像素分布很均匀,表明此算法加密效果良好,能较好地抵御统计分析的攻击.

3.2　相关性分析

相关性分析同属于统计分析法,主要用于探讨加密算法的扩散性. 一般情况下,原图像相邻像素的相关性很高,而加密后图像的冗余度被分散于密文中,相关性降低,不再具有原始图像的统计特征. 相邻像素相关性既可通过图形直接观察,也可以通过以下公式进行计算:

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i, \tag{12}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)]^2, \tag{13}$$

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)][y_i-E(y)], \tag{14}$$

$$\rho_{x,y}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{15}$$

式中，x 和 y 分别为相邻的两个像素值；$E(x)$ 为像素期望值；$D(x)$ 为像素方差；$\mathrm{cov}(x,y)$ 为像素协方差；$\rho_{x,y}$ 为图像相邻两个像素的相关系数.

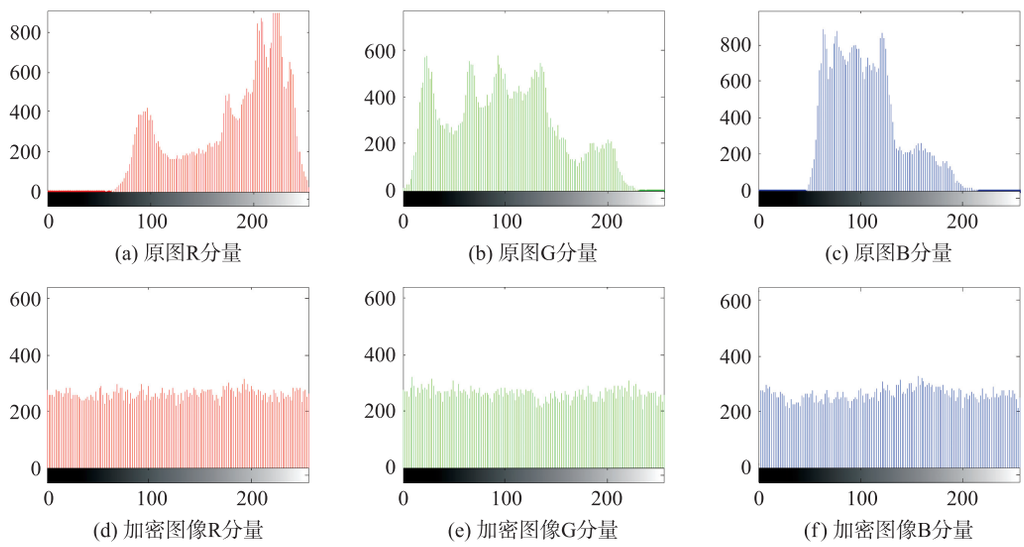


图 7　直方图

Fig. 7　Histogram

图 8(a)、(b)、(c)分别描述了原始图像 R、G、B 3 个分量的相关性，(d)、(e)和(f)为加密后图像相邻像素之间的相关性. 可以看出，原始图像的相邻像素相关性很大，而加密图像相邻像素之间几乎无相关性. 根据式(12)、(13)、(14)、(15)分别计算出原始图像在水平、垂直和对角 3 个方向的相关系数，如表 1 所示. 可见，原始图像的 R、G、B 3 个分量在 3 个方向上的相关系数均接近于 1，相邻像素之间的相关性较强，而解密图像相应的系数均小很多，说明加密图像中的像素相关性已大大减弱.

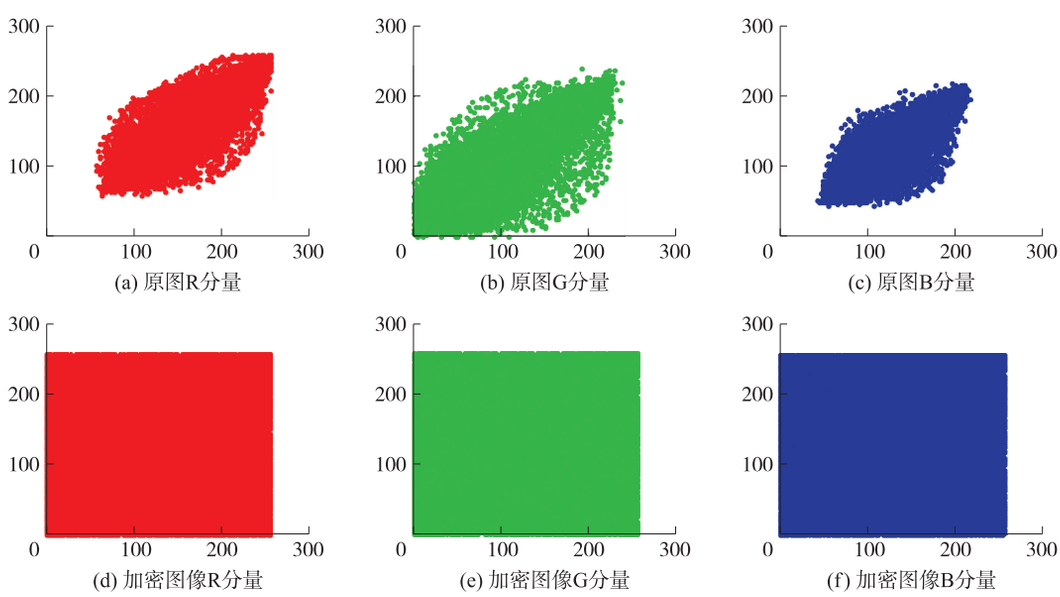


图 8　相邻像素相关性

Fig. 8　Adjacent pixel correlation

表 1　原始图像与加密图像的相关系数

Table 1　The correlation coefficient between original image and encrypted image

方向	原始图像			加密图像		
	R 分量	G 分量	B 分量	R 分量	G 分量	B 分量
水平	0.957 1	0.945 7	0.929 1	0.080 2	0.102 3	0.097 0
垂直	0.962 4	0.948 1	0.933 6	0.001 3	−0.015 8	0.019 6
对角	0.924 8	0.895 3	0.851 2	0.171 0	0.166 0	0.097 2

3.3　密钥敏感性分析

一个好的图像加密系统应能敏锐地觉察到加密密钥的微小改变,且在可实现加密的范围内,密钥空间越大越好.

安全的加密算法应具有高度的密钥敏感性,使用正确密钥解密时可恢复出原始图像. 考虑到密钥的敏感性问题,当只有 R 分量密钥的第一项出现 10^{-15} 的微小扰动,即 $k_R=(0.01+10^{-15},0,0,0,0.1,0.1,0,0)$,而其他密钥不变时,对应的解密图像如图 9(a)所示. 同理,当只有 G 分量密钥的第一项出现 10^{-15} 的扰动,即 $k_G=(0.01+10^{-15},0,0,-1.4,0.1,0.1,0.1,0.1)$,而其他密钥不变时,对应的解密图像如图 9(b)所示. 当 $k_B=(0.01+10^{-15},0,0,0.15,0.2,0.2,0.2,0.2)$,即只有 B 分量密钥的第一项出现 10^{-15} 的微小扰动,而其他密钥不变时,对应的解密图像如图 9(c)所示. 当 R、G、B 3 个分量的第一项均出现 10^{-15} 的扰动时,即同时满足上述 3 种情况,解密图像如图 9(d)所示.

从图 9 的对比可见,图 9(a)、(b)、(c)虽然能够恢复原始图像的部分信息,但仍然失去了原图的部分特征,不能完全解密. 图 9(d)完全看不出原始图像的任何信息,密钥只要存在微小误差,就不能完成图像的正确解密,说明本彩色图像加密算法具有高度的密钥敏感性.

(a) R分量误差为10^{-15}时的解密图　(b) G分量误差为10^{-15}时的解密图

(c) B分量误差为10^{-15}时的解密图　(d) RGB误差为10^{-15}时的解密图

图 9　解密效果图

Fig. 9　The effect map of decryption

4 结语

本文主要从同步的角度对忆阻混沌系统进行控制分析,通过误差曲线、时序图、同步平面相图和三维同步相图等观测同步效果,并将异构忆阻混沌系统同步产生的混沌序列运用到彩色图像加密之中. 首先基于稳定性理论,根据异构系统的微分方程设计含有指数项的非线性同步控制器,从而实现两个不同忆阻混沌系统的完全同步、正反比例同步及函数投影同步. 之后,考虑到异构忆阻混沌系统同步后可提供更大且更为复杂的密钥空间,故将异构同步忆阻混沌系统的混沌序列运用到彩色图像加密中,彩色图像分为R、G、B 3 个分量进行对比分析,实验表明其加密效果显著且密钥敏感性高. 该应用增加了密钥空间,提高了信息破译的难度,有更高的理论价值与工程意义.

[参考文献](References)

[1] YANG X,CAO J,QIU J. Pth moment exponential stochastic synchronization of coupled memristor-based neural networks with mixed delays via delayed impulsive control[J]. Neural networks the official journal of the international neural network society,2015,65(C):80-91.

[2] 梁义,王兴元. 结点含时滞的具有零和非零时滞耦合的复杂网络混沌同步[J]. 物理学报,2013,62(1):018901 0-018901 6.
LIANG Y,WANG X Y. Chaotic synchronization in complex networks with delay nodes by non-delay and delay couplings[J]. Acta Phys Sin,2013,62(1):018901 0-018901 6.(in Chinese)

[3] 郑光超,刘崇新,王琰. 一种具有隐藏吸引子的分数阶混沌系统的动力学分析及有限时间同步[J]. 物理学报,2018(5):050502 1-050502 8.
ZHENG G C,LIU C X,WANG Y. Dynamic analysis and finite time synchronization of a fractional-order chaotic system with hidden attractors[J]. Acta Phys Sin,2018(5):050502 1-050502 8.(in Chinese)

[4] 张玮玮,陈定元,吴然超,等. 一类基于忆阻器分数阶时滞神经网络的修正投影同步[J]. 应用数学和力学,2018,39(2):239-248.
ZHANG W W,CHEN D Y,WU R C,et al. Modified-projective-synchronization of memristor-based fractional-order delayed neural networks[J]. Applied mathematics and mechanics,2018,39(2):239-248.(in Chinese)

[5] YANG S J,LI C D,HUANG T W. Synchronization of coupled memristive chaotic circuits via state dependent impulsive control[J]. Nonlinear dynamics,2017,88(1):115-129.

[6] WANG S,WANG X,ZHOU Y. A memristor-based complex Lorenz system and its modified projective synchronization[J]. Entropy,2015,17(11):7628-7644.

[7] ZHANG B,DENG F Q. Double-compound synchronization of six memristor-based Lorenz systems[J]. Nonlinear dynamics,2014,77(4):1519-1530.

[8] 桑金玉,王娇,岳立娟. 异构二维延迟系统的广义混沌同步[J]. 物理学报,2010,59(11):7618-7622.
SANG J Y,WANG J,YUE L J. Synchronization of chaos for two-dimensional time-delayed chaotic systems with different structures[J]. Acta Phys Sin,2010,59(11):7618-7622.(in Chinese)

[9] 张小红,周勇飞. 异构超混沌广义同步系统构造及其电路仿真[J]. 计算机工程与科学,2014,36(3):551-557.
ZHANG X H,ZHOU Y F. Generalized synchronization system construction of heterogeneous hyperchaotic and its circuit simulation[J]. Computer engineering and science,2014,36(3):551-557.(in Chinese)

[10] WEN S,ZENG Z,HUANG T,et al. Fuzzy modeling and synchronization of different memristor-based chaotic circuits[J]. Physics letters A,2013,377(34/36):2016-2021.

[11] RAKKIYAPPAN R,SIVASAMY R,LI X D. Synchronization of identical and nonidentical memristor-based chaotic systems via active backstepping control technique[J]. Circuits,systems,and signal processing,2015,34(3):763-778.

[12] 于娜. 混沌同步技术在保密通信中的研究与应用[D]. 哈尔滨:黑龙江大学,2007.
YU N. Research and application of chaotic synchronization technology in secure communication[D]. Harbin:Heilongjiang University,2007.(in Chinese)

[13] 闵富红,王恩荣. 超混沌 Qi 系统的错位投影同步及其在保密通信中的应用[J]. 物理学报,2010,59(11):7657-7662.
MIN F H,WANG E R. Dislocated projective synchronization of Qi hyper-chaotic system and its application to secure commu-

nication[J]. Acta Phys Sin,2010,59(11):7657-7662.(in Chinese)

[14] 韩凤英. 基于混沌同步的高效数字图像加密方案[J]. 琼州学院学报,2014,21(5):30-33.
HAN F Y. High performance digital image encryption scheme based on chaotic synchronization[J]. Journal of Qiongzhou university,2014,21(5):30-33.(in Chinese)

[15] 陈宁,贺小滨,桂卫华,等. 基于混沌离散序列的图像加密算法研究[J]. 上海交通大学学报,2017,51(10):1273-1280.
CHEN N,HE X B,GUI W H,et al. Research on image encryption system based on chaotic discrete sequence[J]. Journal of Shanghai jiaotong university,2017,51(10):1273-1280.(in Chinese)

[16] 徐君燕,卜建荣,黄芳. 异结构混沌同步系统图像加密方法的研究[J]. 机械科学与技术,2013,32(6):899-903.
XU J Y,BU J R,HUANG F. Study on digital image encryption method based on different structure chaos synchronization system[J]. Mechanical science and technology for aerospace engineering,2013,32(6):899-903.(in Chinese)

[17] 吴洁宁,王丽丹,段书凯. 基于忆阻器的时滞混沌系统及伪随机序列发生器[J]. 物理学报,2017,66(3):240-250.
WU J N,WANG L D,DUAN S K. A memristor-based time-delay chaotic systems and pseudo-random sequence generator[J]. Acta Phys Sin,2017,66(3):240-250.(in Chinese)

[18] PENG G,MIN F. Multistability analysis,circuit implementations and application in image encryption of a novel memristive chaotic circuit[J]. Nonlinear dynamics,2017,90(3):1607-1625.

[19] PENG G,MIN F. Circuit implementation,synchronization of multistability,and image encryption of a four-wing memristive chaotic system[J/OL]. Journal of electrical and computer engineering,2018[2018-04-28]. https://doi.org/10.1155/2018/8649294.

[责任编辑:严海琳]