Journal of System Simulation

Volume 31 | Issue 5 Article 20

11-20-2019

A New Memristor Chaotic System and Its Application in Image Encryption

Shuanghui Qu
1. School of Physics, Shijiazhuang University, Shijiazhuang 050035, China; ;

Zhihong Yang
2. School of electromechanical engineering, Shijiazhuang University, Shijiazhuang 050035, China;

Xuwei Rong
2. School of electromechanical engineering, Shijiazhuang University, Shijiazhuang 050035, China;

Shuhua Wu
1. School of Physics, Shijiazhuang University, Shijiazhuang 050035, China; ;

A New Memristor Chaotic System and Its Application in Image Encryption

Abstract

Abstract: *A new memristor chaotic system is designed by the method of bringing an ion migration memristor into the Chen system equation.* The basic dynamic characteristics of the memristive system are investigated via bifurcation, Lyapunov exponent et al, which proves the validity of the new system. *The new memristor system is applied in the image encryption* to improve the security of the encryption key. *A dual encryption algorithm is used*, which makes every pixel value of plaintext influence all pixel values of ciphertext. Although there is no direct link between plaintext and ciphertext, the sensibility of ciphertext varying with plaintext can be improved. The result improves the application in message encryption based on complex system.

Keywords

ion migration memristor, chaotic system, dynamic properties, image encryption

Recommended Citation

Qu Shuanghui, Yang Zhihong, Rong Xuwei, Wu Shuhua. A New Memristor Chaotic System and Its Application in Image Encryption[J]. Journal of System Simulation, 2019, 31(5): 984-991.

第 31 卷第 5 期 系统仿真学报© Vol. 31 No. 5
2019 年 5 月 Journal of System Simulation May, 2019

一个新忆阻混沌系统及其在图像加密中的应用

屈双惠[1]，杨志宏[2]，容旭巍[2]，吴淑花[1]
(1.石家庄学院物理学院，河北 石家庄 050035；2.石家庄学院机电学院，河北 石家庄 050035)

摘要：通过引入离子迁移忆阻器对原 Chen 系统的状态方程进行了变换，构建了一个新系统，并对新系统的分岔图、李雅普诺夫指数谱等动力学特性进行了分析，结果表明新系统确实具有混沌特性。将新的忆阻混沌系统应用于图像加密技术，能够生成安全指数更高的密钥系统。采用双重扩散加密的方法，使明文与密文之间没有直接联系，将明文在各个位置像素值的影响渗透到密文的所有像素，提高了密文对明文的敏感性，促进了混沌系统在保密通信中的应用。

关键词：离子迁移忆阻器；混沌系统；动力学特性；图像加密
中图分类号：TP391.9/O415.5 文献标识码：A 文章编号：1004-731X (2019) 05-0984-08
DOI: 10.16182/j.issn1004731x.joss.17-0170

A New Memristor Chaotic System and Its Application in Image Encryption

Qu Shuanghui[1], *Yang Zhihong*[2], *Rong Xuwei*[2], *Wu Shuhua*[1]
(1. School of Physics, Shijiazhuang University, Shijiazhuang 050035, China;
2. School of electromechanical engineering, Shijiazhuang University, Shijiazhuang 050035, China)

Abstract: *A new memristor chaotic system is designed by the method of bringing an ion migration memristor into the Chen system equation.* The basic dynamic characteristics of the memristive system are investigated via bifurcation, Lyapunov exponent et al, which proves the validity of the new system. *The new memristor system is applied in the image encryption* to improve the security of the encryption key. *A dual encryption algorithm is used*, which makes every pixel value of plaintext influence all pixel values of ciphertext. Although there is no direct link between plaintext and ciphertext, the sensibility of ciphertext varying with plaintext can be improved. The result improves the application in message encryption based on complex system.

Keywords: ion migration memristor; chaotic system; dynamic properties; image encryption

引言

21 世纪以来，忆阻器是唯一被实验证明存在的、具有复制特性的新型电路元件。这种复制特性是原来存在的电阻、电容和电感这 3 种基本电路元件进行任意搭配组合都无法实现的。忆阻器是一种无源二端基本电路元件，具有非线性和非失忆性，其中的非失忆性即为记忆功能，对混沌电路、通信工程以及神经网络等工程技术的理论研究与实践开发有着深远的影响。由于忆阻器的阻值可以随着磁通或者电荷量的改变而发生变化，它的伏安特性曲线通过原点，能够产生极其丰富的非线性曲线，则将其应用于混沌系统会提高系统的复杂性以及信号的随机性，更有益于发挥混沌系统在保密通信工作中的应用价值[1-6]。

对数据量大而且相邻数据相关性较强的图像、

收稿日期：2017-04-20 修回日期：2017-07-21；
基金项目：河北省自然科学基金(F2013106079)，石家庄学院科研平台建设成果(XJPT002)；
作者简介：屈双惠(1978-)，女，河北石家庄，硕士，副教授，研究方向为非线性系统；杨志宏(1978-)，男，河北玉田，硕士，讲师，研究方向为图像加密。

视频等多媒体数据而言，混沌密钥在加密实时性方面有着更强的优势，所以混沌图像加密方法的研究越来越受到人们的关注。原有的图像加密算法，大都是由像素位置置乱和像素值加密 2 个步骤构成。这种算法中的密钥与明文基本无关，导致无法抵御选择明文攻击，另外这种算法中的置乱过程和像素值加密过程彼此独立，使得置乱过程形同虚设，只会延长加密时间，降低工作效率[7]。

本文将离子迁移忆阻器的磁通变量引入到混沌系统构造了一个新的系统，通过数值仿真详尽分析了新系统的基本动力学特性，验证了新系统的混沌特性。相对一般的整数阶混沌系统，忆阻混沌系统由于引入了离子迁移忆阻器的磁通变量，具有参数更多、结构更复杂、更难以预测的非线性行为，将其运用到图像保密工作中更有益于提高混沌密钥系统的安全性。所设计的加密方案采用双重加密形式，把第一次加密的结果运用到第二次加密中，将明文在各位置像素值的影响渗透到了最终密文的所有像素中，使得密文与明文、密钥之间具有复杂的非线性关系，更有利于抵御选择明文攻击。

1 忆阻混沌系统

本文在已有的三维 Chen 系统基础上引入离子迁移忆阻器的磁通变量，构建出一个新的三维忆阻混沌系统。

已有的三维 Chen 系统的数学模型为

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=(c-a)x+cy-xz\\ \dot{z}=-bz+xy\end{cases} \tag{1}$$

式中：a，b，c 是常数。当参数 a=35，b=3，c=28 时，系统(1)处于混沌状态。

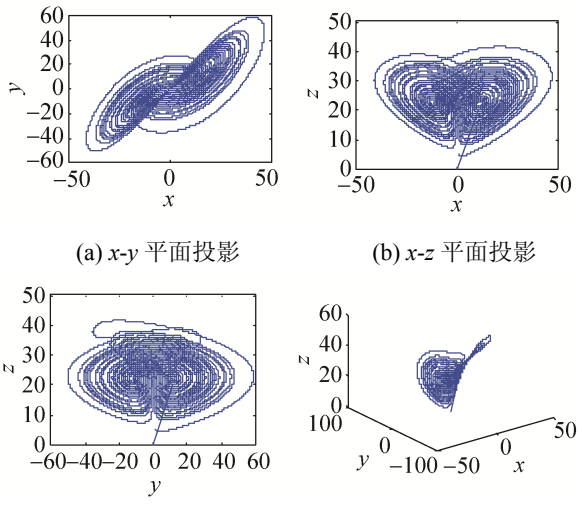
引入离子迁移忆阻器的磁通变量对三维 Chen 系统的状态方程进行变换，得到一个新的三维忆阻混沌系统，其状态方程如下：

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=(c-a)x+dy-xz\\ \dot{z}=-bz-10^5 f(-|x|)\end{cases} \tag{2}$$

式中：a，b，c，d 为系统参数；x，y，z 为系统的 3 个状态变量；$f(x)$满足离子迁移磁控忆阻器的磁通和电荷之间的关系，其表达式如下：

$$f(x)=\begin{cases}(x-c_3)/R_{\text{off}}, & x<c_1\\ \dfrac{\sqrt{2kx+M^2(0)}-M(0)}{k}, & c_1\leqslant x<c_2\\ (x-c_4)/R_{\text{on}}, & x\geqslant c_2\end{cases} \tag{3}$$

式中各参数的值为 $c_1=[R_{\text{off}}^2-M^2(0)]/2k$，$c_2=[R_{\text{on}}^2-M^2(0)]/2k$，$c_3=[(R_{\text{off}}-M(0))^2]/2k$，$c_4=[(R_{\text{on}}-M(0)^2]/2k$，$k=[(R_{\text{on}}-R_{\text{off}})u_v R_{\text{on}}]/D^2$。式中：$x$ 为忆阻器的输入磁通；D 为薄膜总长度；$M(0)$为忆阻器的初始值；R_{on}，R_{off}分别表示忆阻器的极限值，若 $W(t)$表示含氧空缺的 TiO_{2-x}层随时间变化时的厚度，则 R_{on}是当 $W(t)$=0 时的值，R_{off}是当 $W(t)$=D 时的值；u_v表示氧空缺的平均移动量[5-6]。忆阻器的初始状态 D=10 nm，$M(0)$=16 kΩ，R_{on}=100 Ω，R_{off}=20 kΩ，u_v=10^{14}m^{2}s^{-1}V^{-1}。通过数值计算发现，当选取系统参数 a=10，b=2.5，c=30，d=2 时，系统处于混沌状态，如图 1 所示。



(a) x-y 平面投影　(b) x-z 平面投影

(c) y-z 平面投影　(d) x-y-z 空间投影

图 1　忆阻系统的混沌吸引子

Fig. 1　Chaotic attractors of the memristor chaotic system

Lyapunov 指数(LE)可以定量的表征系统的运动特性，形象的描述系统相邻轨线间彼此排斥和吸引的程度，因此利用 LE 谱可以清晰地观察到系统

DOI: 10.16182/j.issn1004731x.joss.17-0170

第 31 卷第 5 期 系统仿真学报 Vol. 31 No. 5
2019 年 5 月 Journal of System Simulation May, 2019

运动状态随参数变化时的情况。对于三维系统，当 $LE_1=0$，$LE_3<LE_2<0$ 时对应于周期运动；而当系统处于混沌状态时 $LE_1>0$。图 2 给出了在 a=[4,12]时，该忆阻混沌系统的 LE 指数随着系统参数 a 发生变化时的图线。观察变化曲线可以看出，当 a=[4,5.8]时，新系统的 LE 指数中只有一个指数 $LE_1=0$，其它两个 LE 指数都是小于 0 的，表明此区间对应于周期运动；而在 a>5.8 的区间可以观察到 $LE_1>0$，表明此区间对应于混沌运动[8]。

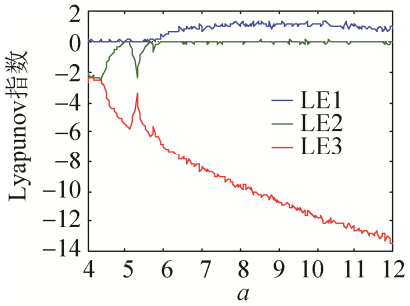


图 2 参数 a 变化时的 Lyapunov 指数谱
Fig. 2 Lyapunov exponential spectrum of parameter a

图 3 给出了忆阻系统的状态变量 x 随着系统参数 a 发生变化时的分岔图，将其与图 2 的 LE 曲线谱进行对比分析可以发现，两者随参数 a 的变化情况完全相符，当 a=[4,5.8]时，系统为周期运动；而在其他区域系统处于混沌状态。图 4 为 y=0 时忆阻混沌系统的 Poincaré 截面图，观察图像可以看到，在 Poincaré 截面图上有许多成片的密集型点，也表明新系统具有混沌特性。

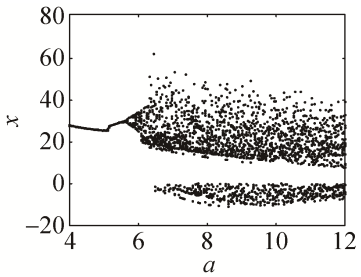


图 3 x 变量随参数 a 变化时的分岔图
Fig. 3 Bifurcation diagram of parameter a versus variable x

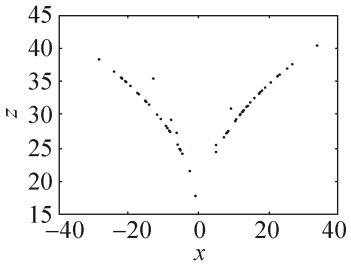


图 4 y = 0 时的 Poincaré 映射图
Fig. 4 Poincaré map on x-z plane(y=0)

2 图像加密

本文为忆阻混沌系统设计的加密算法如图 5 所示。

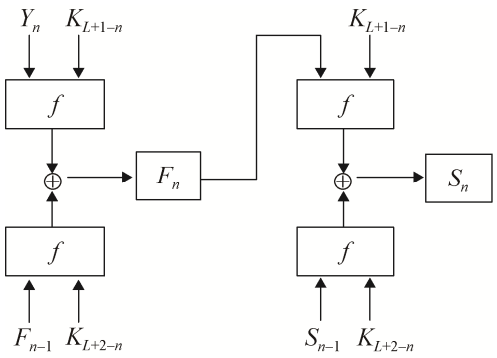


图 5 图像加密算法框架图
Fig. 5 Frame diagram of the image encryption algorithm

图 5 中 n 的取值范围是{1, 2,…, L}。图中用 $\boldsymbol{K}$={K_1, K_2,..., K_{L+1}}表示由忆阻混沌系统生成的混沌密钥序列，加密时反向应用；原明文图像的像素值序列用 $\boldsymbol{Y}$={Y_1, Y_2, ..., Y_L}表示；第一重替代加密后会得到一个中间密文像素值序列，用 $\boldsymbol{F}$={F_1, F_2, ..., F_L}表示；图 5 中，当 n=1 时，$F_{n-1}=F_0$，表示加密明文图像第 1 个像素时所引入的参数，可设为第一重加密的初始密钥，$F_0 \in [0,255]$；之后，对中间密文像素值序列进行第二重加密，可以得到最终的密文像素值序列，用 $\boldsymbol{S}$={S_1, S_2,..., S_L}表示；当 n=1 时，$S_{n-1}=S_0$，表示加密中间密文第 1 个像素时引入的参数，可设为第二重加密的初始密钥；函数 f 是一个非线性运算函数。其中，明文图像的像素总和 $L=M\times N$，M，N 分别为明文图像的像素行数和列数。整个加密过程具有两大优势：一是采

用双重加密形式，将第一重加密得到的运算结果运用到第二重加密过程中，将明文在各个位置像素值的影响渗透到最终密文的所有像素中，提高密文对明文的敏感性；二是密文与明文、密钥之间具有复杂的非线性关系，更有利于抵御选择明文攻击。

2.1 混沌密钥序列

先由系统(2)迭代产生一个忆阻混沌系统的实数序列 $\boldsymbol{T}$，之后进行改造，得到忆阻混沌密钥序列 $\boldsymbol{K}$，运用于图像加密。具体步骤如下：

第 1 步　去除由新忆阻混沌系统(2)迭代生成的实数数据中的前 n_0 项预迭代数据，存放于初始化的空序列 $\boldsymbol{T}$ 中，去除预迭代数据可以消除暂态运行带来的不稳定因素。

第 2 步　新忆阻混沌系统(2)迭代一次生成一组实数数据{x，y，z}，设计一个与 x、y、z 相关的变量 r，令 r=mod(floor(|x+y+z|)，3)。当 r=0 时，将{x，z，y}加入序列 $\boldsymbol{T}$，则 $\boldsymbol{T}$={$\boldsymbol{T}$，x，z，y}；当 r=1 时，将{y，x，z}加入序列 $\boldsymbol{T}$，则 $\boldsymbol{T}$={$\boldsymbol{T}$，y，x，z}；当 r=2 时，将{z，y，x}加入序列 $\boldsymbol{T}$，则 $\boldsymbol{T}$={$\boldsymbol{T}$，z，y，x}。

第 3 步　重复执行上一步操作(floor(L/3)+1)次，将能获得一个长度为 L'(L+1≤L'≤L+3)的原始忆阻混沌实数序列 $\boldsymbol{T}$。

第 4 步　按照下述计算公式对实数序列 $\boldsymbol{T}$ 进行改造，得到忆阻混沌密钥序列 $\boldsymbol{K}$。

$$K(i)=\mathrm{mod}(\mathrm{floor}(|T_i|-\mathrm{floor}(|T_i|))\times 10^{14},256)$$
$$i=1,2\ldots\ldots,L'\ (L+1\leqslant L'\leqslant L+3) \tag{4}$$

计算结果显示，$K(i)\in[1,255]$，取前面 L+1 个数据构成密钥序列 $\boldsymbol{K}$。

2.2 基于双重扩散的加密和解密操作

把前面获得的忆阻混沌密钥序列 $\boldsymbol{K}$ 运用到双重加密算法中，将明文的影响渗透到整个密文中。用{$Y(i)$|i=1, 2,…, L}表示需要加密的原明文图像的像素序列；用{$F(i)$|i=1, 2, …, L}表示经过第一重加密后得到的中间密文图像的像素序列；用{$S(i)$|i=1, 2, …, L}表示经过两重加密后得到的最终密文图像的像素序列。

以下为第一重加密公式：

$$\mathrm{temp}_1=\mathrm{mod}(Y(i)+K(L+1-i),256),$$
$$\mathrm{temp}_2=\mathrm{mod}(F(i-1)+K(L+2-i),256),$$
$$F(i)=\mathrm{temp}_1\oplus\mathrm{temp}_2,\quad i=1,2,3,\ldots\ldots,L \tag{5}$$

由运算公式可知，在第一重扩散加密中，原明文图像在各个位置像素的加密结果都会直接影响后一个像素的加密。

以下为第二重加密公式：

$$\mathrm{temp}_1=\mathrm{mod}(F(i)+K(L+1-i),256),$$
$$\mathrm{temp}_2=\mathrm{mod}(S(i-1)+K(L+2-i),256),$$
$$S(i)=\mathrm{temp}_1\oplus\mathrm{temp}_2,\quad i=1,2,3,\ldots\ldots,L \tag{6}$$

其中，当 i=1 时，对应的 $S(i-1)=S_0=F_L$，即把第一重扩散加密的最后一个因素作为第二重扩散加密的初始密钥，从而把原明文在各个位置像素值的影响渗透到最终密文的所有像素。

执行完上述操作后加密过程完成。由此可以看出，在第二重加密过程中最终的密文 $S(i)$与原始的明文 $Y(i)$之间已没有直接的联系，无法利用第二重加密公式反推出 $K(i)$；另外，在每一重加密过程中，密文与明文之间既有“异或”运算，又有非线性“取模”运算，攻击者要想通过选择特殊的明文来破解忆阻混沌密钥序列 $\boldsymbol{K}$ 是很难的，因此本加密方法能够有效抵御选择明文攻击。

与双重加密相对应，解密过程需要进行双重解密。正向应用混沌密钥序列 $\boldsymbol{K}$。双重解密都需要从最后一个像素开始，逐渐循环至第 1 个像素点。用矩阵 $\boldsymbol{Y}'$来表示第一重解密图像，用矩阵 $\boldsymbol{Y}''$来表示第二重解密图像，像素值分别设置为{$\boldsymbol{Y}'(i)$|i=1，2，…，L}、{$\boldsymbol{Y}''(i)$|i=1，2，…，L}。

第一重解密操作是针对第二重加密操作进行，其运算公式为：

$$\mathrm{temp}_1=S(i)\oplus\mathrm{mod}(S(i-1)+K(L+2-i),256)$$
$$Y'(i)=\mathrm{mod}(\mathrm{temp}_1+256-K(L+1-i),256),$$
$$i=L,L-1,\ldots\ldots,2,1 \tag{7}$$

第一重解密工作完成后，得到的解密图像应当

第 31 卷第 5 期 系统仿真学报 Vol. 31 No. 5
2019 年 5 月 Journal of System Simulation May, 2019

与第一重加密后得到的中间密文一致，即 $\boldsymbol{Y}'=\boldsymbol{F}$。所以当 i=1 时，$\boldsymbol{S}(i-1)=\boldsymbol{S}(0)=\boldsymbol{Y}'(L)$。

第二重解密操作是针对第一重加密操作进行，其运算公式为：

$$\begin{aligned}&\text{temp}_2 = Y'(i) \oplus \text{mod}(Y'(i-1) + K(L+2-i), 256)\\&Y''(i) = \text{mod}(\text{temp}_2 + 256 - K(L+1-i), 256),\\&i = L, L-1, \ldots\ldots, 2, 1\end{aligned} \tag{8}$$

其中，当 i=1 时，$\boldsymbol{Y}'(i-1)=\boldsymbol{Y}'(0)=\boldsymbol{F}_0$。

执行完上述操作后解密过程完成，可以获得双重解密后的解密图像 $\boldsymbol{Y}''$。保证解密过程中所用的初始密钥，所有参数值与加密过程中的完全一样，则可获得与原始图像一模一样的解密图像，即 $\boldsymbol{Y}''=\boldsymbol{Y}$。

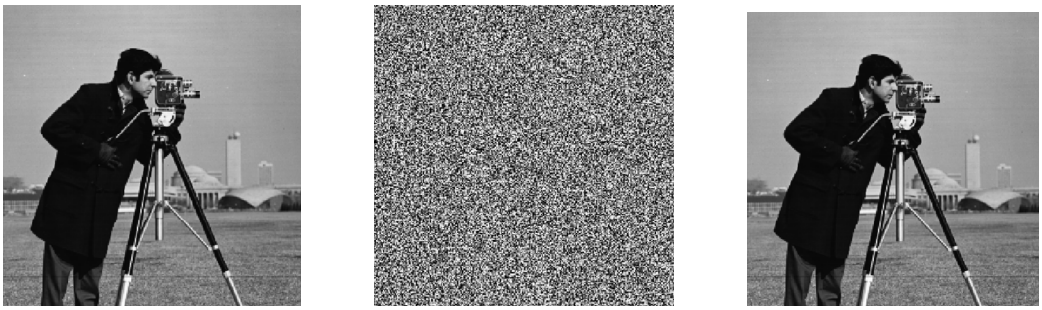
2.3 实验仿真与性能分析

本文实验中使用的是 256×256 的 cameraman 图像，在 Matlab7.5.0 下进行仿真。忆阻系统(2)的参数取值为 a=10，b=2.5，c=30，d=2，忆阻器的初始状态设为 D=10 nm，$M(0)$=16 kΩ，R_{ON}=100 Ω，R_{OFF}=20 kΩ，$u_v=10^{14}\text{m}^2\text{s}^1\text{V}^1$，则系统(2)处于混沌状态。取系统初值为 x_0=1，y_0=1，z_0=1；迭代过程的时间步长为 0.0001；取 F_0=80，n_0=800。

2.3.1 抗统计攻击的性能分析

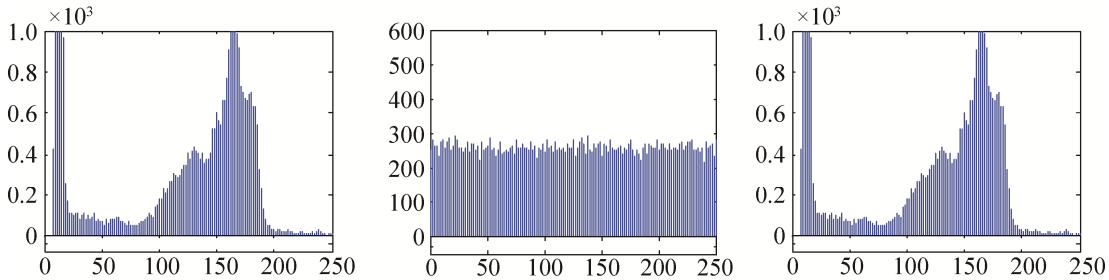
对 Cameraman 图像进行 2.2 的双重加密和解密操作，运行效果如图 6 所示，可以看到，解密图像与原始图像 Cameraman 完全一样。

图 7 为图像直方图：(a)对应原始明文图像；(b)对应最终密文图像；(c)对应双重解密后的图像。可以看出，原始的 cameraman 图像和解密图像的直方图完全一致，表现为各处像素值分布不均匀；而最终密文图像的像素值表现为各处分布较均匀，这说明最终密文图像的像素值呈现出概率均等取各种可能值的趋势。所以，本加密操作能够抵御基于统计分析的解密方法的攻击[9-12]。



(a) 原始图像 (b) 加密图像 (c) 解密图像

图 6 图像加密效果
Fig. 6 Image encryption effect



(a) 原始图像 (b) 加密图像 (c) 解密图像

图 7 图像灰度直方图
Fig. 7 Image gray value histogram

2.3.2 相关性分析

数字图像的各像素之间的相关性很大，尤其是相邻像素之间，同一行、同一列或者对角线上的相邻两个像素之间的相关系数均高于 0.9。图像加密的主要目标就是要破坏相邻像素之间的这种相关性，从而增强图像的加密效果，提高其安全性。相关系数 τ 的计算公式如下：

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

$$D(x)=\frac{1}{n}\sum_{i=1}^{n}(x_i-E(x))^2\ ,$$

$$\mathrm{cov}(x,y)=\frac{1}{n}\sum_{i=1}^{n}(x_i-E(x))(y_i-E(y))\ ,$$

$$\tau=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)\cdot D(y)}} \tag{9}$$

式中：x，y 分别表示图像中相邻两个像素点的像素值；n 表示所取像素点所成的对数。

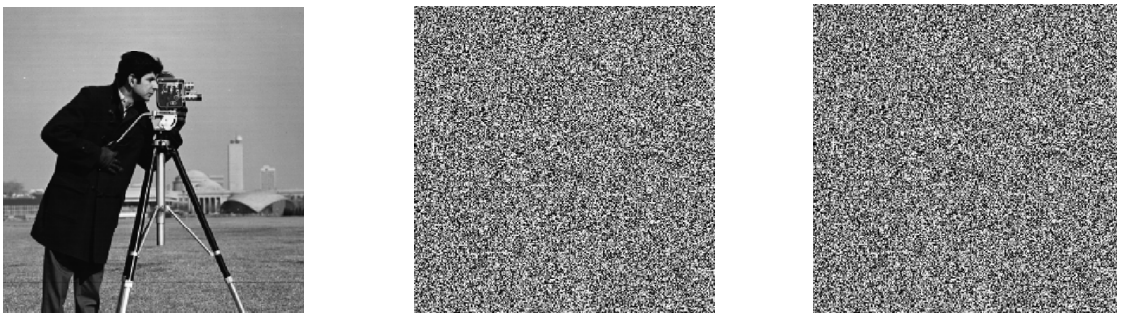
分别在水平、垂直和对角线 3 个方向上对原明文图像和密文图像的相邻像素进行分析，将所得结果列于表 1 的第 2 列和第 3 列。从表 1 中显示的结果可知，原始图像相邻像素的相关性很大，各方向的相关系数 τ 均大于 0.9；而加密图像相邻像素的之间的相关性明显被破坏，其相关系数 τ 趋近于 0，原始图像的统计相关性已经被扩散到了随机的密文中。表 1 中的第 4 列数据是基于 Chen 系统运用本文算法加密 cameraman 图像之后所得密文像素的相应结果。由此可见，将离子迁移忆阻器的磁通变量引入到 Chen 系统所得到的新型三维忆阻混沌系统更为复杂，能够更好的破坏相邻像素的相关性，使得密文有更好的随机分布特性。

表 1 相邻像素相关系数
Tab. 1 Relativity factor of adjacent pixel

方向	明文	密文	密文[Chen]
水平	0.959 9	0.000 497	–0.003 4
垂直	0.933 4	–0.004 0	–0.006 0
对角	0.908 7	–0.001 8	0.006 3

2.3.3 密钥敏感性分析

由于本文设计的忆阻混沌系统对初始值的选取极度敏感，所以本双重加密方案对密钥的敏感性极强，只要密钥稍有变动，就不可能恢复到加密前的图像信息。两个解密密钥具有微小的差别，则解密效果会有很大的差别。首先，取忆阻混沌系统(2)的初始值为$\{x_0, y_0, z_0\}=\{1, 1, 1\}$，生成第一组密钥序列 $\boldsymbol{K}_1$，对 cameraman 图像进行双重加密；之后，取忆阻混沌系统(2)的初始值为$\{x_0, y_0, z_0\}=\{1+10^{-10}, 1, 1\}$，生成第二组密钥序列 $\boldsymbol{K}_2$，对加密后的 cameraman 图像进行双重解密。图 8(c)给出了 x_0 误差为 10^{-10} 时的解密图像，误差解密获得的结果与原始图像完全不一样。



(a) 原始图像 (b) 加密图像 (c) x_0 误差为 10^{-10} 的解密图像

图 8 密钥敏感性测试结果
Fig. 8 Sensibility test of encryption key

第 31 卷第 5 期 系统仿真学报 Vol. 31 No. 5
2019 年 5 月 Journal of System Simulation May, 2019

2.3.4 密钥空间分析

密钥空间的大小是衡量一种加密方案抗攻击能力的重要指标，如果密钥空间太小，则加密方案容易受到穷举攻击，导致其安全性不高。本文设计的加密方案中采用三维忆阻混沌系统的 3 个状态变量的初始值作为原始密钥，每个数据用 16 位十进制数字的实数表示；所以，密钥空间至少为 $10^{16}\times10^{16}\times10^{16}=10^{48}$。这个空间已经很大，如果将 a，b，c，d，D，$M(0)$，R_{on}，R_{off}，u_v，F_0 和 n_0 等参考值都考虑进去，密钥空间更大，足够抵抗任意类型的暴力攻击。

2.3.5 执行效率分析

实验的操作平台是 Intel core(TM) i3-350M 2.27GHz CPU，1.92GB 内存和 320GB 硬盘容量的 PC 机硬件环境以及 Windows XP，Matlab7.5.0 编译器的软件环境；最终密钥和像素采用无符号整数表示。用本文设计的方案对一幅 256×256 的 8 位灰度图像进行加密操作的时间大约是 6.930 3 s。在同样的计算机系统环境下对相同的原始图像进行文献[7]中的加密操作时间大约是 9.584 5 s。由此可见，本文设计的双重加密速度要快于文献[7]的算法。文献[7]中的算法包括行、列置乱和一轮像素替代加密操作，其中的置乱操作需要另外生成置乱密钥序列，导致其算法操作时间增加。

3 结论

本文引入离子迁移忆阻器的磁通变量对三维 Chen 系统的状态方程进行变换，得到一个新的三维忆阻混沌系统，通过对新系统的相图、分岔图等基本特性进行分析，证实了新混沌系统的存在性。利用忆阻混沌系统设计了对图像的双重加密方案，将明文在各位置像素值的影响渗透到密文的所有像素，使得密文与明文、密钥之间在整个加密过程中保持了复杂的非线性关系，这样可以能够有效抵御选择明文攻击，有益于混沌系统在保密通信中的应用。

参考文献：

[1] 方颖, 徐炳吉. 一种基于荷控忆阻器的混沌电路[J]. 计算机科学, 2014, 41(11): 447-450.
Fang Ying, Xu Bingji. Charge-controlled Memristor-based Chaotic Circuit[J]. Computer Science, 2014, 41(11): 447-450.

[2] 杨芳艳, 冷家丽, 李清都. 基于 Chua 电路的四维超混沌忆阻电路[J]. 物理学报, 2014, 63(8): 080502.
Yang Fangyan, Leng Jiali, Li Qingdu. The 4-dimensional hyperchaotic memristive circuit based on Chua's circuit[J]. Acta Physica Sinica, 2014, 63(8): 080502.

[3] 宋德华, 吕梦菲, 任翔, 等. 忆阻电路的基本性质及其应用[J]. 物理学报, 2012, 61(11): 118101.
Song Dehua, Lü Mengfei, Ren Xiang, et al. Basic properties and applications of the memristor circuit[J]. Acta Physica Sinica, 2012, 61(11): 118101.

[4] 谭志平, 杨红姣, 刘奇能, 等. 最简荷控型忆阻器混沌电路的设计及实现[J]. 计算物理, 2015, 32(4): 496-504.
Tan Zhiping, Yang Hongjiao, Liu Qineng, et al. Analysis and Implementation of a Simplest Charge-controlled Memristor Chaotic Circuit[J]. Chinese Journal of Computational Physics, 2015, 32(4): 496-504.

[5] 阮静雅, 孙克辉, 牟俊. 基于忆阻器反馈的 Lorenz 超混沌系统及其电路实现[J]. 物理学报, 2016, 65(19): 190502.
Ruan Jingya, Sun Kehui, Mou Jun. Memristor-based Lorenz hyper-chaotic system and its circuit implementation[J]. Acta Physica Sinica, 2016, 65(19): 190502.

[6] 闵富红, 王珠林, 王恩荣, 等. 新型忆阻器混沌电路及其在图像加密中的应用[J]. 电子与信息学报, 2016, 38(10): 2681-2688.
Min Fuhong, Wang Zhulin, Wang Enrong, et al. New Memristor Chaotic Circuit and Its Application to Image Encryption[J]. Journal of Electronics & Information Technology, 2016, 38(10): 2681-2688.

[7] 王静, 蒋国平. 一种超混沌图像加密算法的安全性分析及其改进[J]. 物理学报, 2011, 60(6): 060503.
Wang Jing, Jiang Guoping. Cryptanalysis of a hyper-chaotic image encryption algorithm and its improved version[J]. Acta Physica Sinica, 2011, 60(6): 060503.

[8] 张晓丹, 李志萍, 张丽丽. 一类基于奇异值分解的 Lyapunov 指数计算方法[J]. 北京科技大学学报, 2005, 27(3): 371-374.
Zhang Xiaodan, Li Zhiping, Zhang Lili. A Method Based on Singular Value Decomposition for Computation of

Lyapunov exponent [J]. Journal of University of Science and Technology Beijing, 2005, 27(3): 371-374.

[9] Azzaz M S, Tanougast C, Sadoudi S, et al. Robust chaotic key stream generator for real-time images encryption[J]. Journal of Real-Time Image Processing(S1861-8200), 2013, 8(3): 297-306.

[10] 张小红, 廖琳玉, 俞梁华. 新型忆阻细胞神经网络的建模及电路仿真[J]. 系统仿真学报, 2016, 28(8): 1715-1731.
Zhang Xiaohong, Liao Linyu, Yu Lianghua. Novel Modeling of Memristive Cellular Neural Network and Its Circuit Simulation[J]. Journal of System Simulation, 2016, 28(8): 1715-1731.

[11] Deng X H, Zhu C X. Image encryption algorithms based on chaos through dual scrambling of pixel position and bit[J]. Journal on Communications (S2374-4367), 2014, 35(3): 216-223.

[12] Wang Y, Wong K W, Liao X, et al. A new chaos-based fast image encryption algorithm[J]. Applied Soft Computing (S1568-4946), 2011, 11(1): 514-522.