# 基于 DNA 编码与正弦混沌映射的气象图加密技术研究

布海力切木·阿吾冬 李国东
(新疆财经大学应用数学学院 乌鲁木齐 830012)

**摘 要** 气象图片在传输过程中可能被偷、截取,导致数据外流影响国家的气象数据安全,因此传输之前加密,接收后再解密使用是安全可靠的。加密方法是首先把气象图的 R,G,B 3 层分开,降低图层间的相关性,再将 DNA 编码与正弦混沌映射相结合,对气象图各层分别进行加密。由于此方法具备并行计算的优势,大大提高了计算机的加解密速度。该算法密钥空间大、对初始值敏感、抗攻击性强、加密方法可逆,能够安全、高效地抵抗一系列攻击方法,从而保证了气象图像的安全传输使用,解决了大数据时代的传统加密和解密技术在操作图像时的困难。该方法完全可以应用于灰度或其他普通彩色图像的加密工作。但是由于气象图的拍摄量大、单位时间内需要加密的图像多,即需要在安全的基础上高速加密,因此该方法是如气象等收集大量图片资料的领域的首选,并且在军事、医学等图像保密通信领域也具有巨大的应用潜力。

**关键词** 气象图加密,DNA 编码,正弦混沌映射,并行计算,密钥空间,高效,可逆,军事,医学
**中图法分类号** TP309 **文献标识码** A

## Study on DNA Encoding & Sine Chaos-based Meteorological Image Encryption Technology

Buhalqam AWDUN LI Guo-dong
(College of Applied Mathematics, Xinjiang University of Finance and Economics, Urumqi 830012, China)

**Abstract** Meteorological images in the transmission process may be stolen and intercepted, and it leads to the data flow, which do harm to the country's meteorological data security. Thus, encryption before the transmission and decoding after receiving is a safe and reliable way. Encryption method first separates the three layers of meteorological image R, G, B to reduce the correlation between the layers. Second, it combines DNA encoding and sine chaotic mapping to encrypt the meteorological images' layers separately. This method has the advantage of parallel computation, so the speed of encryption and decryption is greatly improved. The algorithm has large key space, strong attack resistance, reversible encryption methods and it is also sensitive to initial value. Therefore, it can against a series of attacks safely and efficiently. Then, the method can meet our needs of safe meteorological image transmission. In the age of big data, this method solves the difficulties of traditional encryption and decryption technology. This method also can be applied to the encryption of gray or other common color images. However, due to the large amount of the taken meteorological images in every day, the number of images needs to be encrypted in the unit time is large. In other words, high speed encryption on the basis of security is needed. Thus this method is extremely suitable for the fields, which collect a large amount of image data, such as meteorology. And it also has great potential applications in the military, medicine and other image secure communication fields.

**Keywords** Encryption of meteorological images, DNA encoding, Sine chaotic mapping, Parallel computation, Key space, Efficient, Reversible, Military, Medicine

## 1 引言

现今网络技术迅猛发展,更多的数字图像需要被存储和通信。高技术在为生活带来方便的同时对数字图像的安全造成了严重的威胁,如气象图像被偷、被截取对国家的气象数据保密带来威胁。图像加密机制是最常见的有效方法之一。一天内拍摄的气象图像量多,并且图像本身具有庞大的数据量和高度冗余的特性,使得传统的加密和解密技术在操作图像时十分困难。这要求在研究过程中,使用的方法在保证可逆和抵抗明文攻击的前提下计算机加解密速度越快越好。加密过程普遍采用混沌理论[7]。

气象图的数据量大,用普通的彩色图像加密方案远远满

本文受国家自然科学基金(11461063),国家教育部人文社会科学基金(13YJAZH040),国家社科基金(14BTJ021),新疆维吾尔自治区普通高等学校人文社会科学重点研究基地基金(050315B03)资助。
布海力切木·阿吾冬(1989—),女,硕士,主要研究方向为数据分析与图像处理,E-mail:261728984@qq.com;李国东(1972—),男,博士,教授,硕士生导师,主要研究方向为数据分析与图像处理。

足不了气象图的快速加密、解密工作的需求。DNA 编码是计算机科学和分子生物学相结合而发展起来的新型研究领域。DNA 编码具有强大的并行计算能力。本文将混沌映射和 DNA 编码相结合对彩色气象图像进行加密，大大缩短了加密工作所耗的时间，同时加强了抗攻击性。仿真实验结果表明本文采用的方法可逆、有效、安全，并且抵抗明文攻击强。

## 2 基本理论

### 2.1 混沌映射

解决图像安全问题的方法都是基于混沌的理论。因为混沌信号是一种伪随机信号，由确定性方程产生，一旦给定系统参数和初始值，便可精确地再生出混沌信号。真随机信号虽然能保证“一次一密”的绝对安全性，但它不能再生，从而不能达到真正解密的目的；而混沌信号在基本能保证伪随机特性的前提下对系统参数和初始值非常敏感，难以分析、重构和预测。由于混沌系统的高度复杂性，大多数研究采用数值法，即相图法、Lyapunov（李雅普诺夫）指数法[5,6,8]和功率谱方法等。常用的混沌系统有切比雪夫映射、正弦映射、立方映射、Logistic 映射[9]和 Lorenz 映射、埃农（Henon）映射、帐篷映射、Kent（肯特）映射等。本文使用的混沌映射是正弦混沌映射。为了更有说服力，首先简单地证明正弦映射是混沌映射，证明过程如下。

正弦映射方程为：

$$\begin{cases} f_{(x)}=\mu\sin(\beta x_i-\theta) \\ x(i+1)=f(x) \end{cases} \tag{1}$$

其中，$\mu,\beta,\theta$ 为参数。

Lyapunov（李雅普诺夫）指数方程为：

$$\lambda=\lim_{n\to\infty}\lambda_n(x_0)=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n=1}\ln\left|\frac{\mathrm{d}f(x_n,\mu)}{\mathrm{d}x}\right| \tag{2}$$

则正弦映射的 Lyapunov 指数方程为：

$$\lambda=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln|f'(\mu,x_i)|=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln|\mu\beta\cos(\beta x_i-\theta)| \tag{3}$$

图 1 为正弦映射分岔和 Lyapunov 指数与系数的关系图。正的 Lyapunov 指数表示相邻轨迹按照指数迅速分离，运动局部不稳定，并且对初始值敏感，轨迹在有界区间内多次折叠，从而导致混沌；负的 Lyapunov 指数表示相体积收缩，轨迹局部稳定，并且对初始值不敏感，$\lambda=0$ 为临界状态。因此，$\lambda>0$可作为系统混沌行为的一个判据。由图 1 可以看出使 $\lambda>0$ 的值较多，正弦映射属于超混沌系统。

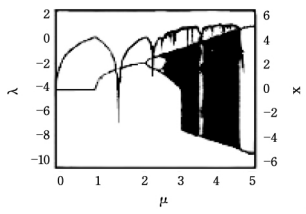



图 1 正弦映射分岔和 Lyapunov 指数与系数的关系图

### 2.2 DNA 编码

DNA 包含 A（腺嘌呤）、T（胸腺嘧啶）、C（胞嘧啶）、G（鸟嘌呤）4 种碱基。其中 A 和 T 是互补的一对，C 和 G 是互补的一对。在二进制中 0 和 1 是互补的一对，所以 00 与 11 是互补的一对，01 与 10 也是互补的一对。利用互补性质的相似性和唯一性，把二进制和 DNA 联系在一起。像素值的范围为 1－255，把每一个像素值用一个 8 位二进制表示，用一个碱基代替二进制数的相邻两位，碱基与两位二进制总共有 $C_4^1C_2^1=8$ 种配对方式，配对方式如表 1 所列。每个像素值可以用一个长度为 4 的 DNA 序列来表示，进而对图像进行 DNA 编码。

表 1 DNA 碱基与二进制数的配对方式

| | 方式 1 | 方式 2 | 方式 3 | 方式 4 | 方式 5 | 方式 6 | 方式 7 | 方式 8 |
|---|---|---|---|---|---|---|---|---|
| A | 00 | 00 | 11 | 11 | 10 | 10 | 01 | 01 |
| T | 11 | 11 | 00 | 00 | 01 | 01 | 10 | 10 |
| C | 10 | 01 | 10 | 01 | 10 | 01 | 10 | 01 |
| G | 01 | 10 | 01 | 10 | 01 | 10 | 01 | 10 |

本文采用的配对方式是 $A=00,T=11,C=01,G=10$，例如，像素值 125 是用十进制来表示的，把它换算成二进制等于 01111011（需满足每个像素值的二进制值都为 8 位，若换算得到的二进制数不足 8 位可在前补零）。通过上述的 DNA 编码规则得到的编码为 CTGT。

DNA 加法、减法和互补规则如下。

（1）加法：因为 00＋00＝00，00＋01＝01，00＋10＝10，00＋11＝11，01＋01＝10，01＋10＝11，01＋11＝100，10＋10＝100，10＋11＝101，11＋11＝110，所以本文中 $A+A=A$，$A+C=C$，$A+G=G$，$A+T=T$，$C+C=G$，$C+G=T$，$C+T=A$，$G+G=A$，$G+T=C$，$T+T=G$。由于二进制满足加法交换律，因此 DNA 加法也满足加法交换律。

（2）减法：由（1）可以得到相应的 DNA 减法，例如 $T-G=C$ 等。

（3）互补规则：A 的补为 T，T 的补为 A，G 的补为 C，C 的补为 G。

## 3 算法步骤

由于利用单一的混沌系统对数字图像进行加密，抗攻击能力弱、安全性低、容易被密码分析师破解，从而无法实现气象图的安全传递。因此用正弦混沌映射构造随机矩阵与拟定的 DNA 算法相结合并取补的方法来提高加密方案的安全性与复杂性。

### 3.1 气象图像加密过程

气象图是彩色的，由 R（红）层、G（绿）层、B（蓝）层共 3 层组成。实验证明把图像的 R，G，B 3 层合并为 1 层之后再进行加密计算的方法虽然简单、计算速度快，但是合并为 1 层的图片必定失真。所以本文采取先把气象图片的 R，G，B 层分离出来，分别加密再合并的方法。加密方案如图 2 所示。

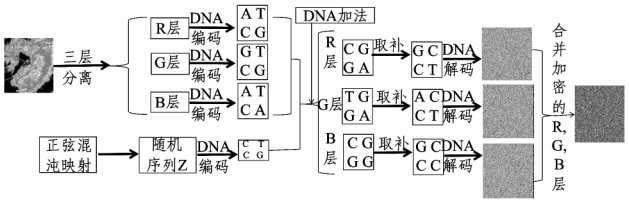



图 2 加密设计图

（1）首先，应用 MATLAB 程序把气象图像的 R，G，B 3 层分离成每个像素在 0－255 的基色矩阵。本文定义明文的大

小为 $m\times n$，那么每一层基色矩阵的大小也为 $m\times n$。这里得到的是十进制二位矩阵，分别记为 $A_{bR}$，$A_{bB}$，$A_{bG}$。

(2)把 $A_{bR}$，$A_{bB}$，$A_{bG}$ 转化为二进制的二位矩阵，分别记为 $A'_{bR}$，$A'_{bB}$，$A'_{bG}$。然后用本文给出的 DNA 编码规则进行 DNA 编码，得到大小为 $m\times 4n$ 的 DNA 矩阵，分别记为 $DNA_{A_{bR}}$，$DNA_{A_{bG}}$，$DNA_{A_{bB}}$。

(3)观察图 1，任意选取混沌效果较好的点，并把其对应的 $\mu$，$x$，$\beta$，$\theta$ 值当做初始值和参数。本文采取 $\mu=4.53696$，$x_0=4.378$，$\beta=1$，$\theta=0$。仅靠观察图像来采取形成混沌的点不够严密，原因是混沌系统在混沌区域可能存在着某些周期性的窗口，仅用 Lyapunov 指数法判断混沌不够精确。谱分析法是判断混沌的重要手段，也是用 Lyapunov 指数法判断混沌条件的辅助手段。为了保证严密性，可以用功率谱密度函数来验证所采取的点是否是真正形成混沌的点。若功率谱图具有单峰(或者几个峰)，则对应于周期(或拟周期)序列；若功率谱图无明显峰值(或峰值连成一片)，则对应混沌序列。

实验证明本文所采取的初始值和参数值使正弦混沌映射的功率谱图峰值连成一片，即可得出所采取的初始值和参数确实形成混沌的结论。

对于正弦混沌映射，当 $\mu=4.53696$，$x_0=4.378$，$\beta=1$，$\theta=0$ 时，经研究得出当精度为 20 位的正弦映射时，第 11 位所得到的序列随机性好。为了方便，以下正弦映射的精度只取 13 位。正弦混沌映射的第 11 位记为 $L$，判定条件为：

$$L=\begin{cases}0, & \text{当 } L_i=0,1,2,3,4 \text{ 时}\\ 1, & \text{当 } L_i=5,6,7,8,9 \text{ 时}\end{cases} \tag{4}$$

将 $L$ 的值作为随机矩阵 $Z_R$，$Z_G$，$Z_B$ 里的元素，直到每个随机矩阵大小为 $m\times 8n$，即 $L$ 共取 $3\times m\times 8n$ 个值。

(4)利用本文所给出的 DNA 编码规则对矩阵 $Z_R$，$Z_G$，$Z_B$ 进行 DNA 编码，并记编码后得到的 DNA 矩阵为 $DNA_{Z_R}$，$DNA_{Z_G}$，$DNA_{Z_B}$。

(5)把所得到的 $DNA_{Z_R}$，$DNA_{Z_G}$，$DNA_{Z_B}$ 分别与 $DNA_{A_{bR}}$，$DNA_{A_{bB}}$，$DNA_{A_{bG}}$ 按照本文所给出 DNA 加法规则对应相加，并分别记结果为 $B_R$，$B_G$，$B_B$。

(6)为了更进一步提高抗攻击性，对 $B_R$，$B_G$，$B_B$ 中的元素(A，T，C，G)按照本文所给出的取补规则进行取补运算，分别得到矩 $B_R'$，$B_G'$，$B_B'$。

(7)把 $B_R'$，$B_G'$，$B_B'$ 转换为二进制矩阵(大小为 m×8n)，然后每行的每 8 个元素为一单位转换成十进制，此时便可得到每个像素值为 0－255 的 3 个十进制密文矩阵，合并这 3 个密文矩阵可得密文图像。

### 3.2 气象图像解密过程

按照上述步骤的逆过程进行解密，解密方案如图 3 所示。

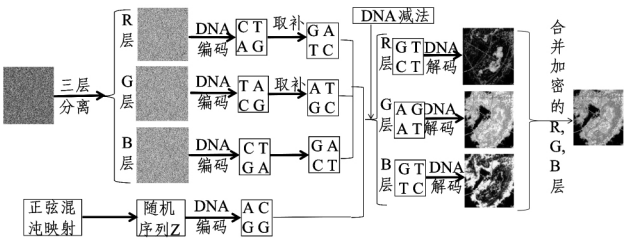



图 3 解密设计图

(1)应用 MATLAB 程序把密文气象图像的 R，G，B 3 层分离成每个像素在 0－255 的矩阵。

(2)把 3 个十进制密文矩阵分别转化成二进制矩阵。

(3)用 DNA 编码规则对上述二进制矩阵进行 DNA 编码，得到矩阵 $B_R'$，$B_G'$，$B_B'$。

(4)对矩阵 $B_R'$，$B_G'$，$B_B'$ 进行去补运算，得到矩阵 $B_R$，$B_G$，$B_B$。

(5)对由正弦混沌映射得到的随机矩阵 $Z_R$，$Z_G$，$Z_B$ 进行 DNA 编码，得到矩阵 $DNA_{Z_R}$，$DNA_{Z_G}$，$DNA_{Z_B}$。

(6)用 DNA 减法，由矩阵 $B_R$，$B_G$，$B_B$ 分别减去矩阵 $DNA_{Z_R}$，$DNA_{Z_G}$，$DNA_{Z_B}$，分别得到 $DNA_{A_{bR}}$，$DNA_{A_{bG}}$，$DNA_{A_{bB}}$。

(7)将 $DNA_{A_{bR}}$，$DNA_{A_{bG}}$，$DNA_{A_{bB}}$ 转换为二进制矩阵为 $A'_{bR}$，$A'_{bB}$，$A'_{bG}$(此时每个矩阵的大小为 $m\times 8n$)，然后每行的每 8 个元素为一单位转换成十进制，此时就可以得到每个像素值为 0－255 的明文气象图的 R，G，B 3 层的基色矩阵，合并这 3 个基色矩阵便可得明文气象图像。

## 4 天气图像加密仿真实验及结果安全性分析

### 4.1 实验仿真

本文借助 Matlab7.11 软件对所提加密算法进行仿真实验并对结果进行安全性分析。选取 302×338×3 的气象图像，根据本文所建立的加密方法对气象图像分层，加密结果如图 4 所示，可见原始图像信息已经被隐藏，已看不到原始图像轮廓。图 4 中的(A)解密图像为正确密钥解密图像，可见该加密方案经解密步骤后几乎可以完全无损地恢复出原始图像。

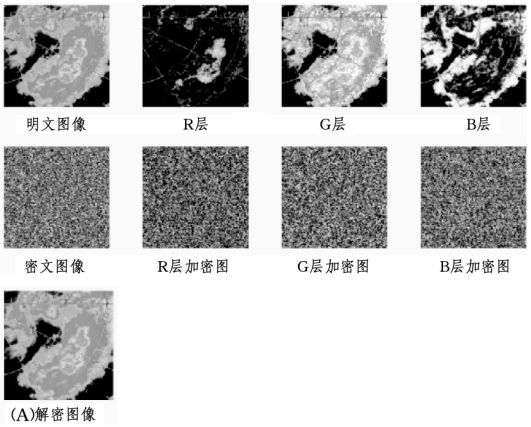



图 4 实验仿真结果

### 4.2 安全性分析

#### 4.2.1 密钥敏感性测试

将分别对初始值和参数 $\mu=4.53696$，$x_0=4.378$，$\beta=1$，$\theta=0$ 进行微小的变动，用错误的密钥对加密的图像进行解密，结果如图 5 所示。可见，本文方法对初始值极敏感。

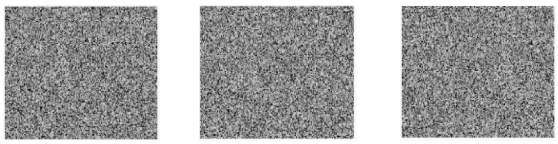
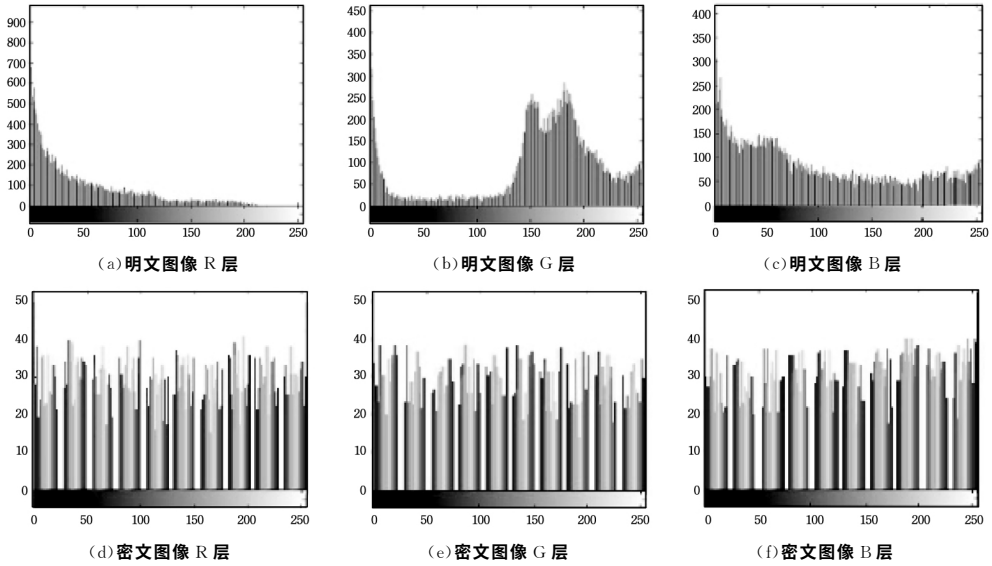



图 5 错误的密钥解密的气象图

4.2.2　直方图分析

直方图反映了数字图像中不同灰度级的像素出现的频率。用一个好的图像加密算法加密得到的密文图像中原始图像的统计特性特点不复存在，攻击者想通过统计特性获取原始图像是徒劳的，从而达到避免信息泄漏的目的，从直方图中直观可见顶端应该平滑且均匀，基本在一条水平线上。

为了直观地判断本文算法的性能，在图 6 中给出了明文气象图的直方图和密文气象图像的直方图。可见，原始图像像素分布极不均匀，存在强烈的统计特性。加密后图像像素分布均匀，顶端基本在一条水平线上，表示不同灰度级的灰度值出现频数基本相等，得出的结论是本文算法能够有效抵抗统计攻击。



(a)明文图像 R 层　(b)明文图像 G 层　(c)明文图像 B 层

(d)密文图像 R 层　(e)密文图像 G 层　(f)密文图像 B 层

图 6　明文气象图和密文气象图的直方图

4.2.3　差分分析

NPCR 表示当明文中任意一个像素值发生微小变化时，经过比较两幅加密图像，计算密文图像中像素值发生变化的比率，NPCR 被定义为：

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N}\times 100\% \tag{5}$$

其中，$\begin{cases}D(i,j)=1, & \text{if } C(i,j)=c'(i,j)\\ D(i,j)=0, & \text{if } C(i,j)\neq c'(i,j)\end{cases}$。

本文提取原始图像 G 层中像素点 $IG(188,190)=200$，将其改为 $IG(188,190)=201$，R，G，B 层的 NPCR 值分别为 0.9972，0.9973，0.9972。NPCR 值接近于 1，证明几乎所有像素点的值都发生了变化，进一步得出该加密算法差分抵抗能力较强的结论。

4.2.4　相关性分析

密文图像的像素值之间的相关性应该降到最低，使其有效地抵抗密文攻击，从而提高密文的安全性。本文在加密前后的气象图中随机选取 30000 对像素点，测试垂直、对角线和水平方向上的相邻像素之间的相关性。结果如表 2 所列，可见明文图像相邻像素之间的相关性接近 1，而密文图像相邻像素之间的相关性趋向于 0，说明利用本文方法加密后，明文图像中的相关统计特性已消失。

表 2　明文图像 R，G，B 3 层相邻像素的相关性

| 相邻像素方向 | 明文图像相关系数 | | |
|---|---|---|---|
| | R 层 | G 层 | B 层 |
| 垂直方向 | 0.9475 | 0.9342 | 0.8904 |
| 对角线方向 | 0.9688 | 0.968 | 0.8932 |
| 水平方向 | 0.9444 | 0.9435 | 0.9974 |

彩色图像 R，G，B 分量间相同位置像素的相关性较大，好的加密算法也应当使之大大降低。明文气象图与通过本文的方法得到的密文气象图的 R，G，B 分量间相同位置像素的相关性结果如表 3 所列。由表 3 可知，密文气象图的 R，G，B 分量间相同位置像素的相关性趋向 0，远远小于明文气象图的。把本文的测试结果与 Wang[1]，Lin[2]，Rhouman[3]，柴[4] 的结果进行比较，可知本文的抗统计攻击的能力优于上述文献中的方法。

表 3　R，G，B 3 层之间相同位置像素的相关性

| | R，G 分量之间相同位置像素相关性 | R，B 分量之间相同位置像素相关性 | G，B 分量之间相同位置像素相关性 |
|---|---|---|---|
| 本文明文图像 | 0.9765 | 0.7684 | 0.8992 |
| 本文密文图像 | −0.0026 | −0.0036 | −0.0008 |
| 柴密文图像 | −0.0035 | −0.005 | −0.0013 |
| Wang 密文图像 | −0.0038 | −0.0509 | 0.0127 |
| Liu 密文图像 | 0.2312 | 0.1254 | 0.1611 |
| Rhouman 密文图像 | 0.248 | 0.139 | 0.1713 |

结束语　本文提出了给气象图加密传输的建议，并对此设计了一种基于正弦混沌映射与 DNA 编码相结合的气象图像加解密方案。为了确保图像在加密过程中不受损坏并且最大限度地降低相同位置像素值之间的相关性，首先把明文图像分离成了 R，G，B 3 层，然后别对其进行了加密运算。在加密过程中有效利用了 DNA 强大的并行计算能力和正弦混沌映射的多参数、混沌效果突出的优点，提高了计算机加解密图像的运行速度，同时加强了对初始值的敏感性，加大了密钥空间。最后通过天气图像加密仿真实验及结果安全性分析加以验证，得出了本文采用的加密方法安全、有效、可逆、计算速度快、抵抗统计攻击能力强、密钥敏感性高的结论。所提方法解决了在大数据时代传统的加密和解密技术在操作图像时遇到

(下转第 416 页)

序列在迭代过程中必将退化为周期序列的缺陷，本算法将多个混沌序列进行一个非线性函数运算，以得到周期更长的序列，这个阶段只包括余弦函数运算和取模运算，算法简单、速度较快；最后实验结果和安全性分析表明：该算法具有密钥空间大、加密图像像素分布性均匀、密文相邻像素的相关性极低、密文图像的信息熵接近 8bit、峰值信噪比小、密文对明文和密钥非常敏感、抵抗选择明(密)文的攻击、加密速度快等优点。因此，本文算法在图像保密通信和存储应用中将具有良好的应用前景。

## 参 考 文 献


[1] Liu W B, Chen G R. A three-dimensional smooth autonomous quadratic Chaotic system generate a single four-scroll attractor [J]. Int. J. Bifurc. Chaos, 2004, 14: 1395-1403

[2] Li C B, Sprott J C. Multistability in a butterfly flow[J]. Int. J. Bifurc. Chaos, 2013, 23: 1350199-1350209

[3] 官国荣，吴成茂，贾倩. 一种改进高性能 Lorenz 混沌系统构造及其应用[J]. 物理学报，2015，64(2)：31-44

[4] 朱淑芹，杨淼，张先华，等. 利用 Silnikov 定理构造混沌系统[J]. 北京科技大学学报，2005，27(5)：635-637

[5] Chen G, Ueta T. Yet another chaotic attractor[J]. Int J Bifurcation Chaos, 1999, 9(7): 1465-1466

[6] Lu J, Chen G. A new chaotic attractor coined[J]. Int J Bifurcation Chaos, 2002, 12(3): 659-661

[7] Čelikovsky′ S, Chen G. On a generalized Lorenz canonical form of chaotic systems[J]. Int J Bifurcation Chaos, 2002, 12(8): 1789-1812

[8] Lu J, Chen G, Cheng D, et al. Bridge the gap between the Lorenz system and the Chen system[J]. Int J Bifurcation Chaos, 2002, 12(12): 2917-2926

[9] Gao T, Chen Z, Yuan Z, et al. A hyperchaos generated from Chen's system[J]. Int J Mod Phys C, 2006, 17(4): 471-478

[10] Li Y, Tang W K S, Chen G. Hyperchaos evolved from the generalized Lorenz equation[J]. Int J Circ Theory, 2005, 33(4): 235-251

[11] Chen A, Lu J, Lu J, et al. Generating hyperchaotic Lu attractor via state feedback control[J]. Physica A, 2006, 364: 103-110

[12] Wang G, Zhang X, Zhen Y, et al. A new modified hyperchaotic Lu system[J]. Physica A, 2006, 371(2): 260-272

[13] Li Y, Chen G, Tang WKS. Controlling a unified chaotic system to hyperchaotic[J]. IEEE Trans Circuits Syst II, 2005, 52(4): 204-207

[14] 韩双霜，闵乐泉，韩丹丹. 一种新的混沌图像加密算法设计[J]. 河南科技大学学报(自然科学版)，2014，35(5)：37-41

[15] 韩双霜，闵乐泉，韩丹丹. 一种基于三维离散混沌映射的伪随机数生器[J]. 华中科技大学学报(自然科学版)，2013，41(8)：16-19

[16] DraganLambi′c. A new discrete chaotic map based on the composition of permutations[J]. Chaos, Solitons and Fractals, 2015, 78: 245-248

[17] Wang Yong, Wong K W, Liao Xiao-feng, et al. A new chaos-based fast image encryption algorithm[J]. Applied Soft Computing, 2011, 11(11): 514-522

[18] Ye Rui-song. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism[J]. Optics Communications, 2011, 284: 5290-5298

[19] Zhang Guo-ji, Liu Qing. A novel image encryption method based on total shuffling scheme[J]. Optics Communications, 2011, 284: 2775-2780

[20] Rudin L, Osher S, Fatemi E. Nonlinear total variation based on noise removal algorithms[J]. Physica D, 1992, 60: 259-268

[21] Sprott J C. Chaos and time-series analysis[M]. Oxford: Oxford University Press, 2003: 513

[22] 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)：83-93

[23] Behnia S, Akhshani A, Mahmodi H, et al. A Novel Algorithm for Image Encryption Based on Mixture of Chaotic Maps[J]. Chaos, Solitons & Fractals, 2008, 35(2): 408-419

[24] Rodriguez J. Computational Cryptography based on trigonometric algorithms and intensity superposition[J]. The Imaging Science Journal, 2010, 58(1): 61-80

[25] 卢辉斌，孙艳. 基于新的超混沌系统的图像加密方案[J]. 计算机科学，2011，38(6)：49-52


(上接第 406 页)

的计算速度不够快、抗攻击性不够高的困难。因此，本文方法适合如气象等收集大量图片资料的领域，也可以应用于灰度和普通彩色图像加密，并且在其它重要的图像信息保密领域也具有巨大的应用潜力。

## 参 考 文 献


[1] Wang X Y, Teng L, Qin X. A novel colour image encryption algorithm based on chaos [J]. Signal Processing, 2012, 92(4): 1101-1108

[2] Liu H J, Wang X Y. Colour image encryption based on one-time keys and robust chaotic maps [J]. Computers & Mathematics with Applications, 2010, 59(10): 3320-3327

[3] Rhouma R, Soumaya M, Salya B. OCML-based colour image encryption [J]. Chaos, Solitons & Fractals, 2009, 40(1): 309-318

[4] Chai Xiu-li, Gan Zhi-hua. Self-adaptive Bit level Colour Image Encryption Algorithm Based on Spatiotemporal Chaotic System [J]. Computer Science, 2015, 42(7): 204-208

[5] Wolf A, Swift J B. H L Swinney and JA Vastano. Determining Lyapunov' exponents from a time series[J]. Physic, 1985, 16D: 285-317

[6] 罗利军，李银山，李形，等. 李雅普诺夫指数谱的研究与仿真[J]. 计算机仿真，2005，22(12)：285-288

[7] 李银山，李欣业，刘波. 分岔混沌非线性振动及其在工程中的应用[J]. 河北工业大学学报，2004，32(3)：80-83

[8] 李水根，吴纪桃. 分形与小波[M]. 北京：科学出版社，2002

[9] Savi M A. Effects of randomness on chaos and order of coupled logistic maps[R]. Physics Letters A, In Press, Corrected Proof, 2006