doi:10.3969/j.issn.1000-436x.2012.11.015

基于仿射和复合混沌的图像自适应加密算法

文昌辞[1]，王沁[1]，黄付敏[2]，袁志树[3]，陶春生[4]

（1. 北京科技大学 计算机系，北京 100083；2. 中国医学科学院，北京 100005；
3. 空军驻京昌地区军事代表室，北京 100009；4. 中国人民解放军驻二一八厂军事代表室，北京 100009）

摘 要：基于有限整数域上的三维仿射变换和复合混沌，提出了一种新的数字图像加密算法，先置乱图像中像素的位置并根据像素坐标混合像素值，然后依次进行非线性的扩散、代换、再扩散，代换时用图像数据扰动耦合的多个混沌系统以进行自适应加密。算法如此迭代 3 轮，可有效地抵御选择明文攻击；密钥空间巨大，可抵御穷举攻击。其中的置乱操作可以直接作用于任意宽高比的图像，不需要进行预处理。构造的混沌系统形式简单，符合模块化设计思想，易于并行实现。

关键词：图像加密；仿射；混沌；置乱；自适应

中图分类号：TP391 **文献标识码：**B **文章编号：**1000-436X(2012)11-0119-09

Self-adaptive encryption algorithm for image based on affine and composed chaos

WEN Chang-ci[1], WANG Qin[1], HUANG Fu-min[2], YUAN Zhi-shu[3], TAO Chun-sheng[4]

(1. Department of Computer Science, University of Scie echnology Beijing, Beijing 100083, China;
2. Chinese Academy of Medical Science, Beijing 100005, China; 3. Air Force Jing Chang Office, Beijing 100009, China;
4. People's Liberation Army 218 Factory Office, Beijing 100009, China)

Abstract: On the basis of three-dimensional affine transformation in limited integer domain and composed chaos, a novel digital image encryption algorithm was proposed. Firstly, it scrambled pixels' position and confused pixels' value according to corresponding coordination. Secondly, it took a series of nonlinear diffusion, substitution and re-diffusion. In the process of substitution, it introduced pixels' value to perturb multiple chaos systems that were coupled together for self-adaptive encryption. The algorithm proceeded the above two steps for 3 times to defend chosen plaintext attack, and had huge key space to defend violent attack. The scrambling function in it was compatible with images at any ratio of length to width without any preprocessing; the constructed whole chaos system which had a simple form was designed modularly, and could be realized parallel conveniently.

Key words: image encryption; affine; chaos; scramble; self-adaptive

1 引言

传统加密算法如 DES、3-DES、IDEA、AES 针对一维数据流而设计，没有考虑数字图像具有数据量大、相关性强、冗余度高的特点，加密效率不高，并且加密之后可能保留着物体的大致轮廓，因而不适用于加密数字图像。目前，数字图像加密主要有 3 种基本操作：1)置乱空域像素（或变换域系数）的位置；2)代换空域像素（或变换域系数）的值；3)在空域像素（或变换域系数）的值之间进行扩散。

收稿日期：2011-02-12；修回日期：2011-07-06
基金项目：装备预研重点基金资助项目（9140A04040308DZ1002）
Foundation Item: The Equipment Pre-Research Foundation of China（9140A04040308DZ1002）

使用以上3种操作（置乱、代换、扩散）在空域直接加密像素后，破坏了像素间的相关性，很难通过压缩编码算法进行压缩。它的优点是没有数据损失，能精确地恢复出明文，并且算法操作相对简单，不存在从空域映射到变换域的大量浮点运算。文献[1~8]没有综合运用置乱、代换和扩散3种操作，在明密文对中容易分析、构造出线性计算关系，因此安全性不高，算法容易被选择明文攻击破解出等效密钥。文献[1~4]都只置乱了像素的位置，没有代换和扩散。文献[5]改变了像素的值，但没有置乱像素的位置。文献[6]针对有限精度下单一混沌映射周期较短且易于破解的缺点，将2个混沌系统串联起来，增强了混沌系统轨道的安全性；但是该算法采用了流密码的形式，在加密像图像这样的海量数据时，很难保证一次一密，而且它仅采用了与像素值相异或的代换操作，一对明密文即可破解出等效密钥。文献[7]提出了一种改变像素值的矩阵变换加密算法，没有改变像素的位置，通过选择明文求解同余方程组可以破解。文献[8]根据序列中元素的取值来控制图像进行自适应置乱，本意是想增强抵御选择明文攻击的能力，但由于缺少代换和扩散操作，自适应加密的优势没有得到发挥。文献[9]没有与明文相关的自适应操作，通过选择明文攻击可以破解出等效密钥；如果将图像数据通过一个不可逆的变换引入到加密过程中，就可能堵上这个漏洞。文献[10]对一个运用广义猫映射来加密图像的算法进行了分析，发现它虽然含有置乱、代换、扩散操作并且迭代多轮，但由于该算法中的置乱操作存在不动点而且代换和扩散操作比较简单，导致明密文中存在一定程度的线性计算关系，所以安全性不高，该文对其进行了破解。

由于计算机精度有限，基于变换（如DFT、DCT、DWT、FRFT[11]、FRHT[12]、MPDFrRT[13]）域的加密算法在变换与反变换时存在数据精度损失，所以解密后的图像与明文不会完全相同。如果将从空域映射到变换域的浮点操作仅仅作为一个加密运算步骤[11~13]，而未将其结合到压缩编码中，那么所耗费的计算量就太大，加密效率很低。结合图像压缩的加密通常在变换域系数被量化后进行，这样可使压缩尽量不影响加密。此处不对基于变换域的加密算法作深入探讨。

基于有限整数域上的三维仿射变换和混沌，本文提出一种新的空域加密算法，先通过置乱变换打乱像素的位置并根据像素坐标混合像素值，然后依次进行非线性的扩散、代换、再扩散，代换时用图像当前数据扰动耦合的多个混沌系统以进行自适应加密，如此迭代3轮。

2 置乱变换

置乱变换可以快速地打乱像素位置，破坏图像中原有的相关性，把图像变得杂乱无章、无法识别，它既可以单独用于图像加密，也可以作为图像加密系统的一个功能部件。为了保证加密之后还能正确恢复，置乱变换必须可逆，即为一一映射。基于仿射变换、有限整数域上的二维非等长置乱变换和整数提升变换，定义有限整数域上的一种三维仿射变换，记为三维类仿射变换。通过对参数进行适当设置，该变换可以为一一映射。

定义1 定义三维类仿射变换为

$$\begin{pmatrix}x'\\y'\\z'\end{pmatrix}=\begin{pmatrix}a&b&c\\d&e&f\\g&h&l\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}+\begin{pmatrix}r\\s\\t\end{pmatrix}\bmod\begin{pmatrix}M\\N\\L\end{pmatrix}$$
$$=\begin{pmatrix}\lfloor ax+by+cz+0.5\rfloor\\\lfloor dx+ey+fz+0.5\rfloor\\\lfloor gx+hy+lz+0.5\rfloor\end{pmatrix}+\begin{pmatrix}\lfloor r+0.5\rfloor\\\lfloor s+0.5\rfloor\\\lfloor t+0.5\rfloor\end{pmatrix}\bmod\begin{pmatrix}M\\N\\L\end{pmatrix}$$

其中，a,b,c,d,e,f,g,h,l,r,s,t 为实数，M,N,L 为正整数，x,x',y,y',z,z' 为非负整数且 $x,x'\in[0,M-1]$，$y,y'\in[0,N-1]$，$z,z'\in[0,L-1]$，$\lfloor\ \rfloor$ 表示取整运算。

在该变换中，对参数进行适当设置，可得到以下2个式子。

$$\begin{pmatrix}x'\\y'\\z'\end{pmatrix}=\begin{pmatrix}a&0&0\\d&e&0\\g&h&l\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}+\begin{pmatrix}r\\s\\t\end{pmatrix}\bmod\begin{pmatrix}M\\N\\L\end{pmatrix}$$
$$=\begin{pmatrix}ax\\ey+\lfloor dx+0.5\rfloor\\lz+\lfloor gx+hy+0.5\rfloor\end{pmatrix}+\begin{pmatrix}\lfloor r+0.5\rfloor\\\lfloor s+0.5\rfloor\\\lfloor t+0.5\rfloor\end{pmatrix}\bmod\begin{pmatrix}M\\N\\L\end{pmatrix}\quad(1)$$

其中，a,e,l 为非零整数且 $\gcd(a,M)=\gcd(e,N)=\gcd(l,L)=1$，$d,g,h,r,s,t$ 为实数。

$$\begin{pmatrix}x'\\y'\\z'\end{pmatrix}=\begin{pmatrix}a&b&0\\0&e&0\\g&h&l\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}+\begin{pmatrix}r\\s\\t\end{pmatrix}\bmod\begin{pmatrix}M\\N\\L\end{pmatrix}$$
$$=\begin{pmatrix}ax+\lfloor by+0.5\rfloor\\ey\\lz+\lfloor gx+hy+0.5\rfloor\end{pmatrix}+\begin{pmatrix}\lfloor r+0.5\rfloor\\\lfloor s+0.5\rfloor\\\lfloor t+0.5\rfloor\end{pmatrix}\bmod\begin{pmatrix}M\\N\\L\end{pmatrix}\quad(2)$$

其中，a,e,l 为非零整数且 $\gcd(a,M)=\gcd(e,N)=\gcd(l,L)=1$，$b,g,h,r,s,t$ 为实数。

可以证明，如果把式(1)，式(2)用于图像(M 行 N 列)的置乱变换，其中 (x,y,z) 代表置乱前像素坐标和像素值，(x',y',z') 代表置乱后像素坐标和像素值，那么该置乱变换是一一映射。

证明

将三维类仿射变换改写为

$$\begin{cases} z'=\lfloor gx+hy+lz+0.5\rfloor+\lfloor t+0.5\rfloor \bmod L \\ \begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}a&b&c\\d&e&f\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}+\begin{pmatrix}r\\s\end{pmatrix}\bmod\begin{pmatrix}M\\N\end{pmatrix} \\ \quad=\begin{pmatrix}\lfloor ax+by+cz+0.5\rfloor+\lfloor r+0.5\rfloor\\ \lfloor dx+ey+fz+0.5\rfloor+\lfloor s+0.5\rfloor\end{pmatrix}\bmod\begin{pmatrix}M\\N\end{pmatrix} \end{cases}$$

即将该变换分解为串行执行的 2 个操作：根据坐标混合像素值 z 得到 z';置乱像素的坐标位置 (x,y) 到 (x',y')。

1）对于 $z'=(lz+\lfloor gx+hy+0.5\rfloor+\lfloor t+0.5\rfloor)\bmod L$，因为 g,h,t 为常数，而且在坐标位置固定后可将 x,y 也作为常量，所以 $\lfloor gx+hy+0.5\rfloor+\lfloor t+0.5\rfloor$ 可作为常量。又由于 $\gcd(l,L)=1$ 并且 $z,z'\in[0,L-1]$，所以对于每一个特定的 (x,y) 来说，$z\to z'$ 的计算可逆，即对应坐标位置上的像素值变换是一一映射。

2）取式（1）进行三维类仿射置乱时，像素坐标位置的变换为

$$\begin{aligned}\begin{pmatrix}x'\\y'\end{pmatrix}&=\begin{pmatrix}a&b&c\\d&e&f\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}+\begin{pmatrix}r\\s\end{pmatrix}\bmod\begin{pmatrix}M\\N\end{pmatrix}\\&=\begin{pmatrix}a&0\\d&e\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}r\\s\end{pmatrix}\bmod\begin{pmatrix}M\\N\end{pmatrix}\\&=\begin{pmatrix}ax+\lfloor r+0.5\rfloor\\ey+\lfloor dx+0.5\rfloor+\lfloor s+0.5\rfloor\end{pmatrix}\bmod\begin{pmatrix}M\\N\end{pmatrix}\end{aligned}$$

其中，r,s 为常量，故 $\lfloor r+0.5\rfloor$ 与 $\lfloor s+0.5\rfloor$ 也为常量。由于 $\gcd(a,M)=\gcd(e,N)=1$，所以 $(x,y)\to(x',y')$ 的计算可逆，像素坐标位置的变换为一一映射。

综上可知，置乱变换式（1）是 $(x,y,z)\to(x',y',z')$ 的一一映射。同理，置乱变换式（2）也是 $(x,y,z)\to(x',y',z')$ 的一一映射。

三维类仿射置乱变换引入实数作为参数，与用整数作为参数相比，置乱的情况更加复杂。它在置乱像素位置的同时根据坐标混合像素值，可以加大图像的信息熵，均衡灰度直方图。较之于仅置乱像素位置的二维置乱变换，它相当于在 $M\times N\times L$ 的三维空间上进行置乱，具有更多大于 0 的 Lyapunov 指数，安全性更高。在实际中，可限制 b (或 d)，g,h 小数部分的二进制形式取 00、01、或 11，r,s,t 小数部分的二进制形式取 0 或 1，使得置乱时乘积计算的复杂度相当于定点乘。

3　加密算法

采用上述置乱变换后，虽然像素位置和像素值被搅乱了，但像素之间没有任何计算关系，容易受到选择明文攻击，因此在三维类仿射变换的基础上引入扩散操作，并且根据加密过程中的数据扰动混沌系统，以进行自适应代换。如此进行三维类仿射置乱、扩散、代换和再扩散，迭代 3 轮后得到密文。算法综合使用了引言中提到的 3 种基本操作，充分发挥了扩散的作用，避免了文献[1~8]中算法设计的不足，并且吸纳了文献[8]中自适应加密的思想，使得在相同密钥情况下每一幅明文的等效密钥都不同，大大增强了算法的安全性。这种设计使得算法迭代 1 轮便可以把图像数据变成类似于随机噪声的形式，而且攻击者很难进行选择明文攻击。算法中迭代轮数越多，明密文之间的非线性关系越复杂，越难进行攻击。为进一步提高算法的安全性并使运算量不至于太大，设置迭代轮数为 3 轮。具体的加解密框架如图 1 所示。

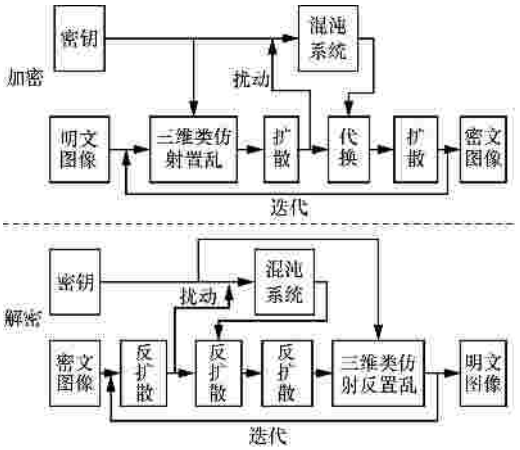

图 1　加密解密框架

3.1　扩散

将图像(M 行 N 列)中的像素按从左到右、从上

到下的顺序，用 $C_i=(P_i+C_{i-1}^2)\bmod L\oplus C_{i-1}$ 逐个进行扩散，P_i 代表第 i 个像素扩散之前的值，C_i 代表扩散之后的值，$i\in[0,MN-1]$，$\oplus$ 表示按位异或操作。当 $i=0$ 时，取 $C_{i-1}=P_{MN-1}$。

3.2 混沌系统

混沌系统具有以下几个适用于加密的特性：1）对参数和初始条件极其敏感；2）输出有界，具有遍历性，类似于随机噪声；3）任意接近的 2 点随着迭代的进行都会指数性发散。在实际中，一维混沌系统容易遭到相空间重构方法攻击，构造复合混沌系统可以解决这一问题。在文献[6]处理混沌系统的基础上，此处选用形式简单的三维 Henon 映射、Logistic 映射、Tent 映射、Cubic 映射和 Chebychev 映射构造新的复合混沌系统。改写这 5 种映射的形式并限制参数和初值的范围，分别记为混沌 0、1、2、3、4，如图 2 所示。

混沌 0：$x_{n+1}=(1.54+b)-x_{n-1}^2-\lambda x_{n-2}$，$\lambda\in(0,0.5),b\in(0,0.46),x_0,x_1,x_2\in[-1,1]$

混沌 1：$x_{n+1}=1-(1.5+\lambda)x_n^2,\lambda\in(0,0.5),x_0\in(-1,1)$

混沌 2：$x_{n+1}=\begin{cases}x_n/\lambda, & 0\leqslant x_n<\lambda\\ (1-x_n)/(1-\lambda), & \lambda\leqslant x_n\leqslant 1\end{cases}$，$\lambda\in(0,0.5),x_0\in(0,1)$

混沌 3：$x_{n+1}=(3.5+\lambda)x_n^3-(2.5+\lambda)x_n$，$\lambda\in(0,0.5),x_0\in(-1,1)$

混沌 4：$x_{n+1}=\cos\left[(2+100\lambda)\arccos(x_n)\right]$，$\lambda\in(0,0.5),x_0\in(-1,1)$

图 2 混沌系统

3.3 扰动混沌系统

在保证加密可逆的前提下，可用中间结果扰动混沌系统，使产生的混沌序列与图像数据密切相关，进一步增强抵御攻击的能力，如图 3 所示。

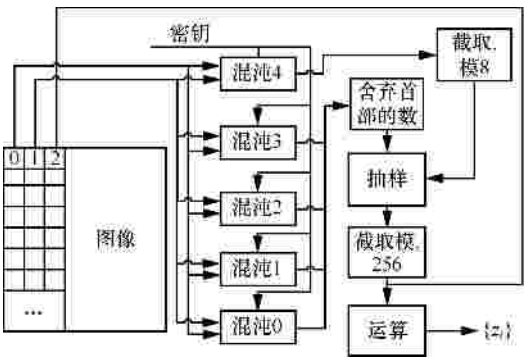

图 3 扰动混沌系统

1) 设加密密钥为 $(k_1k_2,k_3k_4k_5k_6k_7,k_8k_9,k_{10}k_{11},k_{12}k_{13},k_{14}k_{15})$，其中，$k_1$ 代表三维类仿射变换的参数 $(a,b,c,d,e,f,g,h,l,r,s,t)$，$k_2$ 代表从混沌序列首部舍弃数值的个数，其余的子密钥分别代表混沌 0、1、2、3、4 的参数和初值。

2) 在对某一行像素进行代换之前，取该行前 2 个像素值 I_0、I_1，调整子混沌系统的参数和初值，如图 4 所示。

混沌 0：$b=[k_4+0.46\times(I_0+1)/L]/2$

$\lambda=[k_3+(I_0+1)/2L]/2,x_0=[k_5+(I_1+1)/L]/2$

$x_1=[k_6+(I_1+1)/L]/2,x_2=[k_7+(I_1+1)/L]/2$

混沌 1：$\lambda=[k_8+(I_0+1)/2L]/2,x_0=[k_9+(I_1+1)/L]/2$

混沌 2：$\lambda=[k_{10}+(I_0+1)/2L]/2,x_0=[k_{11}+(I_1+1)/L]/2$

混沌 3：$\lambda=[k_{12}+(I_0+1)/2L]/2,x_0=[k_{13}+(I_1+1)/L]/2$

混沌 4：$\lambda=[k_{14}+(I_0+1)/2L]/2,x_0=[k_{15}+(I_1+1)/L]/2$

图 4 调整参数和初值

3) 迭代混沌 4 得到十进制实数序列 $\{y'_{4,i}\}$，取小数部分的第 3 位和第 4 位组成一个位于 0 99 之间的整数，模 8 映射为 $\{y_{4,i}\}$。迭代混沌 0、1、2、3，均舍弃前 k_1 个值，然后根据 $\{y_{4,i}\}$ 对它们抽样，得到 $\{y'_{0,i}\}$、$\{y'_{1,i}\}$、$\{y'_{2,i}\}$、$\{y'_{3,i}\}$。提取这 4 个序列中每个实数的小数点后第 2 位到第 4 位组成一个整数，模 256，对应映射为 $\{y_{0,i}\}$、$\{y_{1,i}\}$、$\{y_{2,i}\}$、$\{y_{3,i}\}$。

4) 用该行第 3 个像素值 I_2 控制混沌系统的耦合方式，计算产生 $\{z_i\}$，如图 5 所示。

3.4 代换

代换每一行像素时都用该行前 3 个像素重新扰动混沌系统，产生新的 $\{z_i\}$，然后通过计算式 $C'_{i+3}=(P'_{i+3}\oplus z_i+z_i^2)\bmod L$，对该行中前 3 个像素以外的所有像素进行计算，$P'_{i+3}$ 代表当前行第 $i+3$ 个像素代换之前的值，C'_{i+3} 代表代换之后的值，$i\in[0,N-4]$。从上到下依次代换每一行。

$$z_i=\begin{cases}(y_{0,i}+y_{1,i})\bmod L\oplus y_{2,i}\oplus y_{3,i}, & \text{if } I_2\bmod 6=0\\ (y_{0,i}+y_{3,i})\bmod L\oplus y_{1,i}\oplus y_{2,i}, & \text{if } I_2\bmod 6=1\\ (y_{0,i}+y_{2,i})\bmod L\oplus y_{1,i}\oplus y_{3,i}, & \text{if } I_2\bmod 6=2\\ (y_{1,i}+y_{2,i})\bmod L\oplus y_{0,i}\oplus y_{3,i}, & \text{if } I_2\bmod 6=3\\ (y_{1,i}+y_{3,i})\bmod L\oplus y_{0,i}\oplus y_{2,i}, & \text{if } I_2\bmod 6=4\\ (y_{2,i}+y_{3,i})\bmod L\oplus y_{0,i}\oplus y_{1,i}, & \text{if } I_2\bmod 6=5\end{cases}$$

图 5 控制耦合方式

4　实验及算法评价

用 VC++实现本文的加解密算法，按照图 6 设置密钥的初值，对 1 024×1 024 大小的 256 色图像 man（如图 7 所示）加密，再解密，分别得到图 8 和图 9。

$k_1:(a=7,b=0,c=0,$
$d=20.5,e=5,f=0,$
$g=21.25,h=37.75,l=71,$
$r=36.5,s=28.5,t=71)$
$k_2=100,k_3=0.06,k_4=0.2$
$k_5=0,k_6=0.1,k_7=1,$
$k_8=0.49,k_9=0.618,k_{10}=0.48,$
$k_{11}=0.617,k_{12}=0.47,k_{13}=0.616,$
$k_{14}=0.46,k_{15}=0.615$

图 6　密钥初值

图 7　man

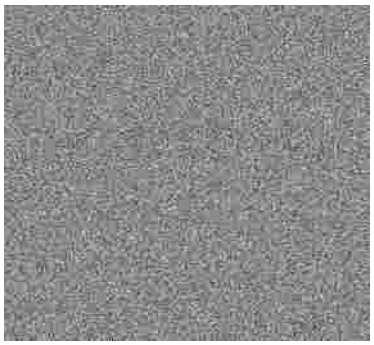

图 8 man 加密后

图 9　正确密钥

4.1　加密视觉效果

数字图像加密要求密文与明文的视觉效果完全不同，目前可以从相邻像素相关性、明密文相似度、信息熵、峰值信噪比和自相关度这 5 个方面评判加密的视觉效果，相关的具体实验数据如图 10~图 18 所示。

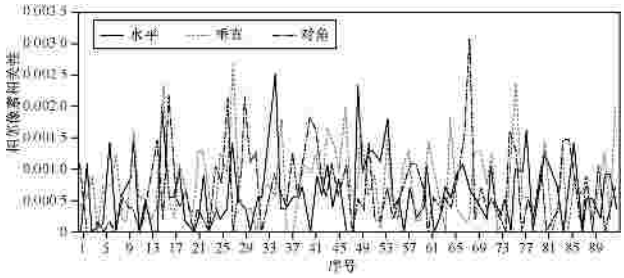

图 10　相邻像素相关性

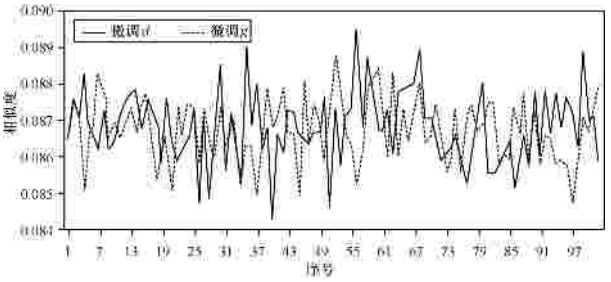

图 11　相似度 1

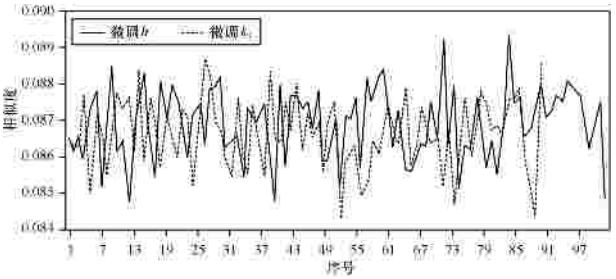

图 12　相似度 2

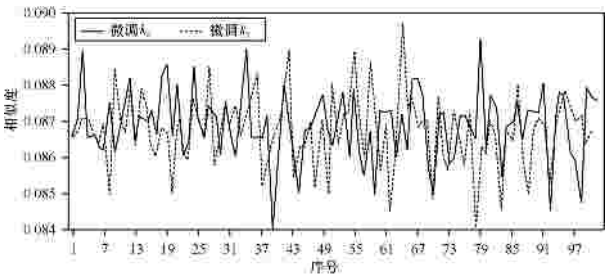

图 13　相似度 3

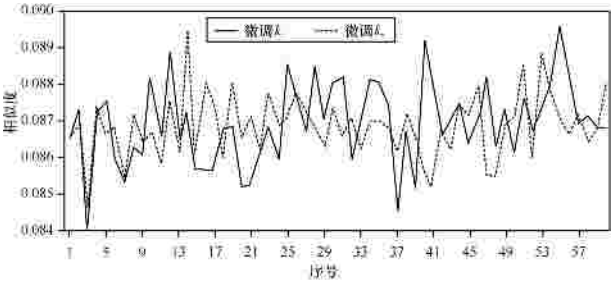

图 14　相似度 4

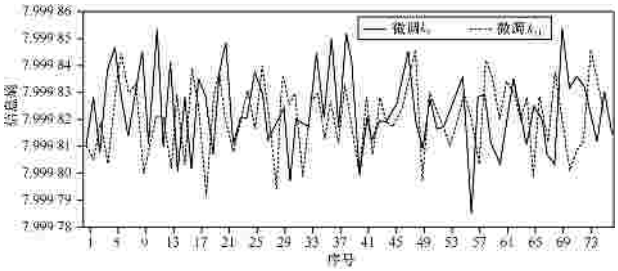

图 15 信息熵 1

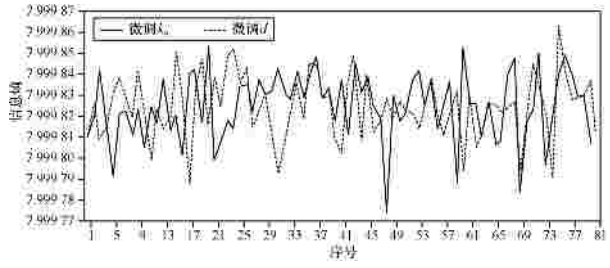

图 16 信息熵 2

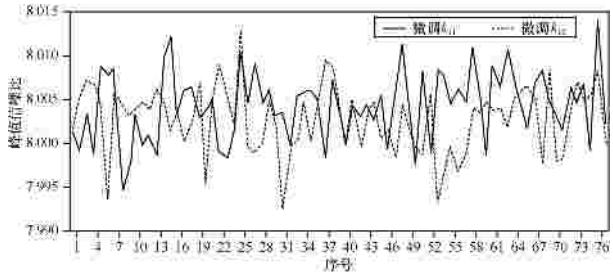

图 17 峰值信噪比

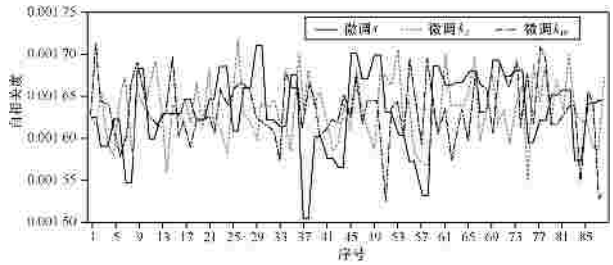

图 18 自相关度

1) 相邻像素相关性

对于图像中的水平、垂直、对角相邻像素，相关性 r_{xy} 通过下式计算：$r_{xy}=|Cov(x,y)|/\sqrt{D(x)D(y)}$，其中，$D(x)=N^{-1}\sum_i(x_i-E(x))^2$，$E(x)=\sum_i x_i/N$，$Cov(x,y)=N^{-1}\times\sum_i(x_i-E(x))(y_i-E(y))$，$x_i$、$y_i$ 代表相邻的像素值。以上述密钥的取值为基数，不断微调 k_{14}，对 man 加密后相邻像素相关性如图 10 所示，微调其他参数略。图像 man 的水平相邻像素相关性为 0.993 268，垂直为 0.994 410，对角为 0.990 168，加密后 3 个方向的相关性均小于 0.003 5，密图无法辨认。

2) 明密文相似度

设明文图像为 $P(M\times N)$，密文图像为 $C(M\times N)$，则两幅图像的相似度为 $XSD=1-\sum_i\sum_j(c_{ij}-p_{ij})^2/\sum_i\sum_j p_{ij}^2$。2 幅图像差别越大相似度越小，完全相同时相似度为 1。不断微调密钥中的参数 d、g 对 man 进行加密，计算得出的相似度如图 11 所示；微调 h、k_3，相似度如图 12 所示；微调 k_5、k_7，相似度如图 13 所示；微调 k_4、k_8，相似度如图 14 所示。可以看出，相似度均小于 0.09，明密文差异显著。

3) 信息熵

设 v_i 表示 L 级灰度图象的第 i 个灰度值，$p(v_i)$ 表示图像中具有第 i 个灰度值的像素所占的比例。图像的信息熵定义为：$H=-\sum_i p(v_i)\mathrm{lb}p(v_i)$。信息熵可以度量图像中灰度值的分布情况，灰度分布越均匀，信息熵越大，反之信息熵越小，它的最大值为 8。不断微调 k_9、k_{11} 对 man 进行加密，计算得出的信息熵如图 15 所示；微调 k_6、d，信息熵如图 16 所示。图像 man 的信息熵为 7.523 737，加密后信息熵均大于 7.999 77，说明灰度分布很均匀，算法能有效地抵御统计攻击。

4) 峰值信噪比

把加密看作在图像上叠加噪声，峰值信噪比 $PSNR=10\log_{10}(y_{\max}^2/MSE)$，其中，$y_{\max}$ 为像素的最大亮度值，$MSE=(MN)^{-1}\sum_i\sum_j(p_{ij}-c_{ij})^2$，$p_{ij}$ 和 c_{ij} 分别为明密文像素点 (i,j) 的值，峰值信噪比在 20dB 以下意味着密图完全不可辨识。不断微调 k_{11}、k_{12} 对 man 进行加密，峰值信噪比如图 17 所示。可以看出，峰值信噪比均小于 8.015dB，明文被有效地掩盖。

5) 自相关度

设图像 $P(M\times N)$ 是一灰度级为 L 的图像，(i,j) 是其中的一个像素点，r,m 均为整数，则点 (i,j) 的 $r-m$ 相关集为 $G_{ij}^{rm}=\{p_{kl}\,\|\,k-i|\le r,|l-j|\le r,|p_{kl}-p_{ij}|\le m|\}$，$r$ 和 m 分别称为像素间距和灰度差，$0<r\le M/2$，$0\le m<L$。图像 P 的 $r-m$ 自相关度定义为：$R_{rm}=(MN)^{-1}\sum_i\sum_j(|G_{ij}^{rm}|/|G_{ij}^{rL}|)$，$|G_{ij}^{rL}|$ 表示集合 G_{ij}^{rL} 中的元素个数。令 r=1，m=60，不断微调 s、k_3、k_{10}，对 man 加密后的自相关度如图 18 所示。图像 man 的自相关度为 0.966 988，加

密后自相关度均小于 0.001 75，密文不可识别。

4.2　安全性分析

算法耦合了多个混沌系统，在每 1 轮迭代中都有 1 次三维类仿射置乱、2 次非线性的扩散和 1 次自适应代换。其中的三维类仿射置乱采用了矩阵变换的形式，继承了二维非等长置乱变换的优点，能快速地打散并搅匀像素，具有混沌特性；它还继承了拟仿射变换的优点，没有不动点。实验证明，仅 1 次三维类仿射置乱便能使图像完全不可识别并且灰度直方图趋向于均衡化。在三维类仿射置乱的基础上，算法用图像中的像素值扰动敏感性强的混沌系统以进行自适应的代换，而且尽可能多地穿插使用了非线性的扩散操作，这种设计使得明密文对之间的映射关系非常复杂，具有很强的密钥敏感性和密文敏感性，符合密码学中的扩散与混淆原则。

1) 密钥空间

k_1 中的 b (或者 d), g, h, r, s, t 均用 8 位二进制数表示，k_1 中的 l 用 7 位二进制数表示，k_2 用 10 位二进制数表示，k_3、k_4、k_5、k_6、k_7、k_8、k_9、k_{10}、k_{11}、k_{12}、k_{13}、k_{14}、k_{15} 这 13 个参数均用 15 位二进制数表示，再加上 k_1 中的 a 与 e，密钥长度大于 $8\times6+7+10+13\times15=260$ bit，密钥空间巨大。DES 算法密钥长度为 56bit，3-DES 为 112bit 或 168bit，IDEA 为 128bit，AES 为 128bit、192bit 或 256bit，文献[4]小于 200bit。260bit 已超过目前可接受的安全长度，假设攻击者以每秒搜索 1 000 万亿个密钥的速度穷举攻击，需要 $3.324\ 8\times10^{55}$ 年以上才能搜索完所有密钥，算法能够有效地抵御穷举攻击。

2) 密钥敏感性

令密钥中的参数 $k_8=k_8+2^{-15}$，解密图 8 得到图 19；令 $k_9=k_9+2^{-15}$，解密得到图 20；令 $k_{13}=k_{13}+2^{-15}$，解密得到图 21；令 $k_{15}=k_{15}+2^{-15}$，解密得到图 22，扰动其他参数略。可以看出，算法具有很强的密钥敏感性，密钥的微小改变都会导致解密失败。

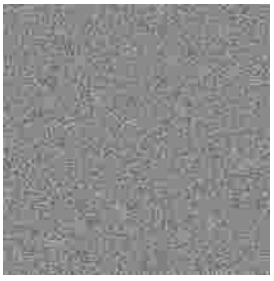

图 19　微扰 k_8

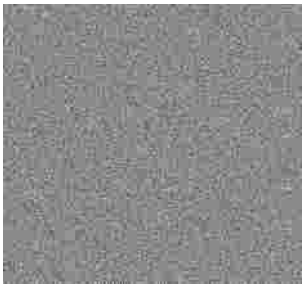

图 20　微扰 k_9

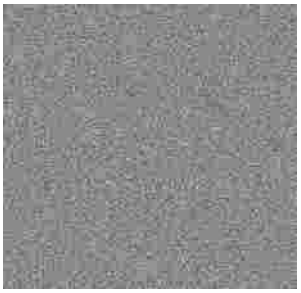

图 21　微扰 k_{13}

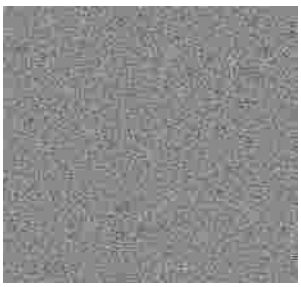

图 22　微扰 k_{15}

3) 密文敏感性

攻击者可能对明文图像作微小改动并观察密文的变化，以发现明密文之间的某些关系。如果微小的改动导致密文很大的变化，那么这种差分攻击就会非常无力，可采用像素改变率 R_{NPC}、平均变化强度 I_{UAC} 来衡量这种敏感程度。设明文对应密文 C_1，将明文中某一个像素点的灰度值加 1 后再加密得到 C_2，则 $R_{\mathrm{NPC}}=\sum_{i,j}q(i,j)/(MN)$，$I_{\mathrm{UAC}}=\sum_{i,j}\left|c_1(i,j)-c_2(i,j)\right|/(255MN)$，其中，当 $C_1(i,j)=C_2(i,j)$ 时 $q(i,j)=0$，否则 $q(i,j)=1$。改动 man 中不同像素，计算出一系列 R_{NPC} 和 I_{UAC}，如图 23 和图 24 所示。可以看出 $R_{\mathrm{NPC}}>0.991\ 85$，$I_{\mathrm{UAC}}>0.332\ 4$，即明文中 1 个像素的微小改变将带来密文中 99.185%以上像素的变化，变化幅度在 33.24%以上。密文敏感性强，算法有很强的抗差分攻击能力。

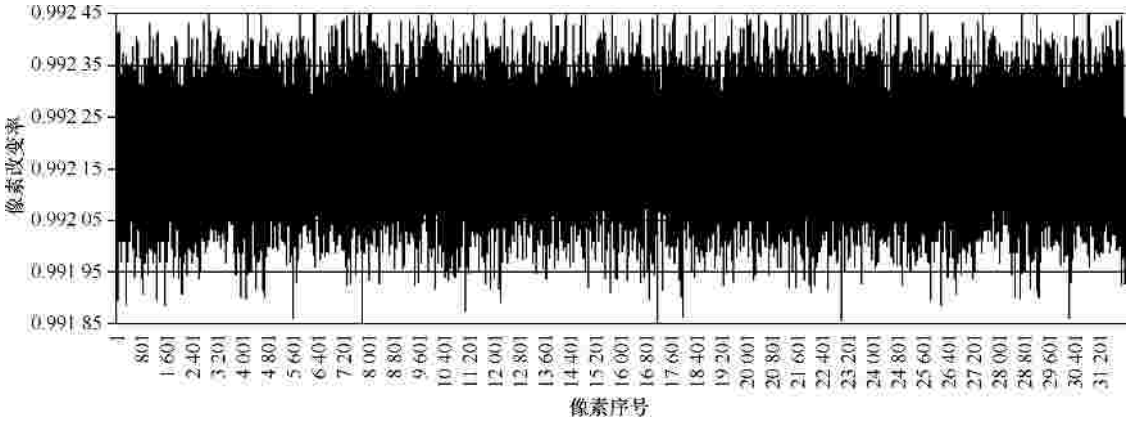

图 23 像素改变率

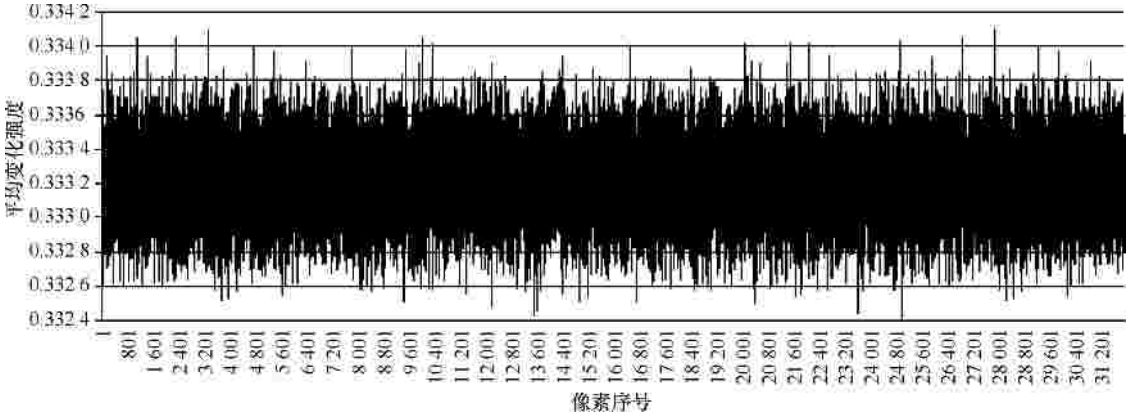

图 24 平均变化强度

5 结束语

本文的加密算法首先采用三维类仿射变换打乱像素的位置并根据像素坐标混合像素值，然后依次进行非线性的扩散、代换、再扩散，在代换时根据图像当前数据扰动耦合的多个混沌系统，使产生的混沌序列与图像本身密切相关。其中的置乱操作可以直接作用于任意大小、任意宽高比的图像，不需要预处理；构造的混沌系统形式简单，符合模块化设计思想，易于并行实现，计算复杂度较小。算法加密视觉效果好，密图无法识别；密钥空间巨大，可有效抵御穷举攻击；密钥敏感性和密文敏感性强，符合密码学中的扩散与混淆原则，可抵御选择明文攻击。进一步的研究内容是在算法中融入更高维的混沌系统，用于产生三维类仿射变换的参数，并且使置乱操作也受图像数据扰动。

参考文献：

[1] HUANG F, FENG Y. An image encryption approach based on a new two-dimensional map[A]. Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing 2006[C]. CA, USA, 2006. 125-130.

[2] MENG J L, PANG H J, GAO W Q. New color image encryption algorithm based on chaotic sequences ranking[A]. Proceedings of International Conference on Intelligent Information Hidi and Multimedia Signal Processing 2008[C]. Harbin, China, 2008. 1348-1351.

[3] HANG H Y. A new image scrambling algorithm based on queue transformation[A]. Proceedings of the Sixth International Conference on Machine Learning and Cybernetics 2007[C]. Hong Kong, China, 2007. 1526-1530.

[4] SHANG Z W, REN H E, ZHANG J. A block location scrambling algorithm of digital image based on arnold transformat on[A]. Proceedings of the 9th International Conference for Young Computer Scientists 2008[C]. Hunan, China, 2008. 2942-2947.

[5] BIBHUDENDRA A, SARAT K P, GANAPATI P. Image encryption by novel cryptosystem using matrix transformation[A]. Proceedings of First International Conference on Emerging Trends in Engineering and Technology 2008[C]. Nagpur, Maharashtra, 2008. 77-81.

[6] **王培荣,徐喆,付冲等.复合混沌数字图像加密算法**[J].**通信学报**,2006, 27(11A):285-289.
WANG P R, XU Z, FU C, *et al*. Composed chaos-based image encryption

algorithm[J]. Journal on Communications, 2006, 27(11A): 285-289.

[7] WANG F C, BAI S, ZHU G B, *et al*. An image encryption algorithm based on N-Dimension affine transformation[A]. Proceedings of the Eighth IEEE/ACIS International Conference on Computer nd Information Science 2009[C]. Shanghai, China, 2009. 579-585.

[8] CHEN G, ZHAO X Y, LI J L. A self-adaptive algorithm on image encryption[J]. Journal of Software, 2005, 16(11):1975-1982.

[9] CHEDDAD A, CONDELL J, CURRAN K, *et al*. A Hash-based image encryption algorithm[J]. Opt Commun, 2010, 283:879-893.

[10] **郭建胜,金晨辉.对基于广义猫映射的一个图像加密系统的已知图像攻击**[J]. **通信学报**, 2005, 26(2):131-135.
GUO J S, JIN C H. An attack with known image to an image cryptosystem based on general cat map[J]. Journal on Communi ions, 2005, 26(2):131-135.

[11] TAO R, MENG X Y, WANG Y. Image encryption with multiorders of fractional Fourier transforms[J]. IEEE Transactions on Information forensics and Security, 2010, 5(4):734-738.

[12] LI X X, ZHAO D M. Optical color image encryption with refined fractional Hartley transform[J]. Optik, 2010, 121(7):673-677.

[13] ZHOU N R, DONG T J, WU J H. Novel image encryption algorithm based on multiple-parameter discrete fractional random transform[J]. Optics Communications, 2010, 283(11):3037-3042.

作者简介：

文昌辞（1980-），男，湖北来凤人，北京科技大学博士生，空军驻京昌地区军事代表室工程师，主要研究方向为信息安全、计算机体系结构。

王沁（1961-），女，湖北武汉人，博士，北京科技大学教授、博士生导师，主要研究方向为信息安全、计算机体系结构与芯片设计、无线传感器网络。

黄付敏（1980-），女，四川攀枝花人，中国医学科学院硕士生，主要研究方向为医学图像处理、信息安全、生物医学信号处理。

袁志树（1974-），男，安徽繁昌人，硕士，空军驻京昌地区军事代表室副总代表，主要研究方向为信息安全、图像处理。

陶春生（1971-），男，湖北黄冈人，硕士，中国人民解放军驻二一八厂军事代表室工程师，主要研究方向为信息安全、信号处理。