ISSN 1000-1239/CN 11-1777/TP
50(2): 319-324, 2013

基于仿射和复合混沌的图像加密新算法

文昌辞[1] 王 沁[1] 刘向宏[2] 黄付敏[3] 袁志树[2]
[1](北京科技大学计算机科学与技术系 北京 100083)
[2](空军京昌代表室 北京 100009)
[3](中国医学科学院北京协和医学院 北京 100730)
(wenchangci@126.com)

An Encryption Algorithm for Image Based on Affine and Composed Chaos

Wen Changci[1], Wang Qin[1], Liu Xianghong[2], Huang Fumin[3], and Yuan Zhishu[2]
[1](*Department of Computer Science and Technology, University of Science and Technology Beijing, Beijing* 100083)
[2](*Air Force Jing Chang Office, Beijing* 100009)
[3](*Peking Union Medical College, Chinese Academy of Medical Sciences, Beijing* 100730)

Abstract With the popular application of multimedia, the security of digital image becomes more and more important. According to the feature of digital image and on the basis of three-dimension affine transformation and chaos, a novel spatial domain encryption algorithm is proposed. Firstly, it scrambles pixel position and confuses pixel value according to the corresponding coordination. Secondly, it takes a series of nonlinear diffusion and substitution in turn for all lines. The algorithm proceeds with the above two steps for at least 3 times, and it can be conveniently converted to the frequency domain algorithm while replacing the processed data in the spatial domain with quantized coefficients in the frequency domain. In the process of substitution, pixel value is introduced to perturb multiple chaos systems that are coupled together for self-adaptive encryption. In the encryption process, the scrambling parameters are generated by chaos systems automatically, and the scrambling function is compatible with images at any ratio of length to width without any preprocessing. Theoretical analysis shows that the algorithm has huge key space to defend against violent attack, the mapping relation between the plaintext and the ciphertext is complex enough to resist chosen plaintext attack efficiently, and the algorithm using simple chaos systems is designed modularly in order to be realized parallelly conveniently. Experimental results show that the algorithm takes good encryption result, gets strong sensitivity, conforms to confusion and diffusion principles in cryptography, and achieves high security.

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

摘 要 随着多媒体的广泛应用,数字图像的安全性变得越来越重要.针对数字图像的特点,基于三维仿射变换和混沌,提出一种新的空域加密算法.先置乱像素的位置并根据像素坐标混合像素的值,然后按行交替进行非线性的扩散、代换,如此迭代至少3轮.代换时用中间结果扰动耦合的多个混沌系统以进行自适应的加密,置乱参数由混沌系统自动生成,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.稍加改动算法使之处理对象为频域量化后系数,便可转换为频域加密算法.理论分析表明:算法密钥空间巨大,可抵御穷举攻击;明密文映射关系复杂,可有效地抵御选择明文攻击;算法符合模块

收稿日期:2011-04-15;**修回日期**:2011-12-26

化设计思想,采用的混沌系统形式简单,易于并行实现.实验结果表明:算法加密效果好,敏感性强,符合密码学中的混淆与扩散原则,安全性高.

关键词 图像加密;仿射;混沌;置乱;自适应

中图法分类号 TP391

传统加密算法如 DES,3-DES,IDEA,AES 等是针对一维数据流而设计的,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,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)置乱像素(或变换域系数)的位置;2)代换像素(或变换域系数)的值;3)在像素(或变换域系数)的值之间进行扩散.在空域直接对像素进行加密得到的密文与明文大小一致,它破坏了像素的空间有序性和局部相关性,密文很难通过压缩编码算法进行压缩;其优点是没有数据损失,可以精确地恢复出明文,并且没有从空域映射到变换域的大量运算.基于变换域的加密算法在变换与反变换时存在数据精度损失,解密后的图像与明文不会完全相同.本文仅研究空域加密.

文献[1]用 N 维仿射变换进行加密;文献[2]根据序列中元素的值来控制图像进行自适应置乱;文献[3]先将 3 个不同周期的混沌序列"异或"以获得长周期序列,再用于加密;文献[4]引入密文作为控制参数的一部分,用所产生的混沌信号对像素值进行代换;文献[5]多次使用猫映射来实现置乱.文献[1-5]的算法没有综合运用置乱、代换和扩散 3 种操作,安全性不够高,容易被选择明文攻击破解出等效密钥.文献[6]对一种基于猫映射的加密算法进行了分析,指出不改变像素值所导致的安全漏洞.文献[7]含有多轮的置乱、代换、扩散操作,但由于其中的置乱操作存在不动点而且代换和扩散比较简单,导致明密文中存在一定程度的线性计算关系,安全性不高.文献[8]提出的加密算法只适用于长宽相等的图像,应用面较窄.

基于三维仿射变换和混沌,本文提出了一种适用于任意大小图像的加密算法.先置乱像素的位置并根据像素坐标混合像素值,然后按行交替进行扩散、代换,代换时用中间结果扰动耦合的多个混沌系统以进行自适应加密,如此迭代 3 轮以上.

1 置乱变换

置乱变换可以快速地打乱像素位置,破坏图像中原有的空间有序性和局部相关性,把图像变得杂乱无章,无法识别,使图像呈现一种类似噪声的形式.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.

定义 1. 定义有限整数域上的三维类仿射变换为

$$\begin{pmatrix}x'\\y'\\z'\end{pmatrix}=\begin{pmatrix}a&b&c\\d&e&f\\g&h&l\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}+\begin{pmatrix}r\\s\\t\end{pmatrix}\bmod\begin{pmatrix}M\\N\\L\end{pmatrix}=$$

$$\begin{pmatrix}\lfloor ax+by+cz+0.5\rfloor\\\lfloor dx+ey+fz+0.5\rfloor\\\lfloor gx+hy+lz+0.5\rfloor\end{pmatrix}+\begin{pmatrix}\lfloor r+0.5\rfloor\\\lfloor s+0.5\rfloor\\\lfloor t+0.5\rfloor\end{pmatrix}\bmod\begin{pmatrix}M\\N\\L\end{pmatrix},$$

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,可得到以下两个式子:

$$\begin{pmatrix}x'\\y'\\z'\end{pmatrix}=\begin{pmatrix}1+dnq&nq&0\\d&1&0\\g&h&l\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}+\begin{pmatrix}r\\s\\t\end{pmatrix}\bmod\begin{pmatrix}M\\N\\L\end{pmatrix},\tag{1}$$

其中 $q=M/\gcd(M,N)$,$d\in Z_N$,$nq\in Z_M$,$1+dnq\in Z_M$,$\gcd(l,L)=1$,g,h,r,s,t 为任意实数,Z_M 为模 M 剩余类,Z_N 为模 N 剩余类.

$$\begin{pmatrix}x'\\y'\\z'\end{pmatrix}=\begin{pmatrix}1&b&0\\nq&1+bnq&0\\g&h&l\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}+\begin{pmatrix}r\\s\\t\end{pmatrix}\bmod\begin{pmatrix}M\\N\\L\end{pmatrix},\tag{2}$$

其中 $q=N/\gcd(M,N)$,$b\in Z_M$,$nq\in Z_N$,$1+bnq\in Z_N$,$\gcd(l,L)=1$,g,h,r,s,t 为任意实数,Z_M 为模 M 剩余类,Z_N 为模 N 剩余类.

如果把式(1)(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.详细证明略.

式(1)(2)的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(很靠近的两个初值随时间推移按指数方式分离的度量),安全性更高.

2 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,因此引入扩散和代换操作.可以利用此时图像中的数据扰动混沌系统,以行为单位进行扩散和代换.如此迭代三维置乱变换、扩散和代换至少 3 轮后得到密文,其中置乱变换的参数由混沌系统产生.加密算法的具体框架如图 1 所示,解密为加密的逆.设密钥为(k_0k_1,$k_2k_3k_4k_5k_6$,k_7k_8,k_9k_{10},$k_{11}k_{12}$),其中 k_0 代表迭代 k_0+3 轮,k_1 代表舍弃混沌序列前 k_1+100 个数,$k_2k_3k_4k_5k_6$,k_7k_8,k_9k_{10} 和 $k_{11}k_{12}$ 分别代表 Chaos1,2,3,4 的参数和初值.

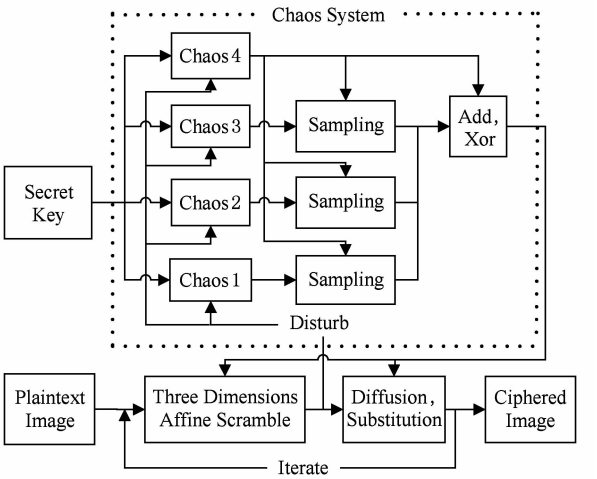


Fig. 1 Encryption frame.

图 1 加密框架

2.1 混沌系统

混沌系统具有以下两个适用于加密的特性:1)对参数和初始条件极其敏感,任意接近的两点随着迭代的进行都会指数性发散;2)输出有界,具有遍历性,类似于随机噪声.在实际中,由于一维混沌系统容易受到相空间重构方法攻击,所以选用形式简单的三维 Henon 映射[9]、Logistic 映射、Cubic 映射和 Chebychev 映射构造复合混沌系统.改写这 4 种映射的形式并限制参数和初值的范围,作为 Chaos1,2,3,4,如图 2 所示:

Chaos1:$x_{n+1}=(1.54+b)-x_{n-1}^2-\lambda x_{n-2}$;
$\lambda\in(0,0.5)$;$b\in(0,0.46)$;$x_0,x_1,x_2\in[-1,1]$.
Chaos2:$x_{n+1}=1-(1.5+\lambda)x_n^2$;
$\lambda\in(0,0.5)$,$x_0\in(-1,1)$.
Chaos3:$x_{n+1}=(3.5+\lambda)x_n^3-(2.5+\lambda)x_n$;
$\lambda\in(0,0.5)$,$x_0\in(-1,1)$.
Chaos4:$x_{n+1}=\cos[(2+100\lambda)\arccos(x_n)]$;
$\lambda\in(0,0.5)$,$x_0\in(-1,1)$.

Fig. 2 Chaos system.

图 2 混沌系统

1) 取 Chaos4 所产生实数序列的小数点后第 3 到第 4 位组成一个位于 0～99 之间的整数,模 8 得到序列$\{x_i^4\}$,$i\in[0,N]$.用$\{x_i^4\}$ 中前 $N-1$ 个数作为间隔对 Chaos1,2,3 所产生的实数序列进行抽样得到$\{x_i^1\}$,$\{x_i^2\}$,$\{x_i^3\}$,$i\in[0,N-1]$.

2) 将$\{x_i^1\}$,$\{x_i^2\}$,$\{x_i^3\}$中数值的小数点后第 2 位到第 4 位组成一个位于 0～999 之间的整数,模 256 得到序列$\{y_i^1\}$,$\{y_i^2\}$,$\{y_i^3\}$,$i\in[0,N-1]$.

3) 根据$\{x_i^4\}$ 中最后一个整数 x_N^4 计算序列$\{z_i\}$.当 $x_N^4 \bmod 3=0$ 时,$z_i=(y_i^1+y_i^2 \bmod 256)\oplus y_i^3$;$x_N^4 \bmod 3=1$ 时,$z_i=(y_i^1+y_i^3 \bmod 256)\oplus y_i^2$;$x_N^4 \bmod 3=2$ 时,$z_i=(y_i^2+y_i^3 \bmod 256)\oplus y_i^1$.

2.2 生成置乱矩阵

用初始密钥作为混沌系统的参数,生成$\{z_i\}$.当 $z_0\%2=0$ 时,选用三维类仿射变换式(1)进行置乱,$q=M/\gcd(M,N)$,$d=\lfloor(M-1)\times z_1/(q\times 256)\rfloor$;否则选用式(2)进行置乱,$q=N/\gcd(M,N)$,$b=\lfloor(N-1)\times z_1/(q\times 256)\rfloor$.设置其他参数为 $n=1$,$g=z_3+1+\lfloor z_4\times 4/255\rfloor/4$,$h=z_5+1+\lfloor z_6\times 4/255\rfloor/4$,$l=1+2\times z_7$,$r=z_8+1+\lfloor z_9\times 2/255\rfloor/2$,$s=z_{10}+1+\lfloor z_{11}\times 2/255\rfloor/2$,$t=z_{12}+1+\lfloor z_{13}\times 2/255\rfloor/2$.

2.3 扰动混沌系统

在对某一行像素进行扩散和代换时,取上一行前 $\lfloor N/2\rfloor$ 个像素值的均值 I_0、后 $N-\lfloor N/2\rfloor$ 个像素值的均值 I_1,按图3重新设置混沌系统的参数和

Chaos1:$b=[k_3+0.46\times(I_0+1)/L]/2$,
$\lambda=[k_2+(I_0+1)/2L]/2$,$x_0=[k_4+(I_1+1)/L]/2$,
$x_1=[k_5+(I_1+1)/L]/2$,$x_2=[k_6+(I_1+1)/L]/2$.
Chaos2:$\lambda=[k_7+(I_0+1)/2L]/2$,$x_0=[k_8+(I_1+1)/L]/2$.
Chaos3:$\lambda=[k_9+(I_0+1)/2L]/2$,$x_0=[k_{10}+(I_1+1)/L]/2$.
Chaos4:$\lambda=[k_{11}+(I_0+1)/2L]/2$,$x_0=[k_{12}+(I_1+1)/L]/2$.

Fig. 3 Disturb the chaos system.

图 3 扰动混沌系统

初值. 对第 1 行像素进行扩散和代换时把最后一行作为上一行.

2.4 扩散和代换

按从上到下的顺序逐行对图像进行扩散和代换,每处理新的一行时都重新扰动混沌系统产生新的$\{z_i\}$. 通过计算式 $C_i=(P_i+C_{i-1}^2) \bmod L$ 对该行中的像素从左到右依次进行扩散,P_i 代表该行第 i 个像素扩散之前的值,C_i 代表扩散之后的值,$i\in[0, N-1]$,C_{-1}代表上一行最后一个像素值. 然后通过计算式 $C_i'=(P_i'+z_i^3) \bmod L$ 对该行中的像素从左到右依次进行代换,P_i' 代表该行第 i 个像素代换之前的值,C_i' 代表之后的值.

3 实验及算法评价

设置密钥的初值 $k_0=0$(即迭代 3 轮),$k_1=123$, $k_2=0.1$,$k_3=0.15$,$k_4=0.12$,$k_5=0.13$,$k_6=0.11$, $k_7=0.16$,$k_8=0.17$,$k_9=0.19$,$k_{10}=0.156$,$k_{11}=0.122$,$k_{12}=0.122\,1$. 对 256×256 大小的 256 色图像 cameraman(如图 4 所示)加密,得到图 5;再解密可完全恢复出图 4.

Fig. 4 Plaintext image.
图 4 明文图像

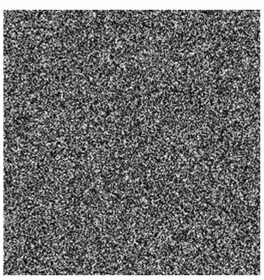


Fig. 5 Ciphertext image.
图 5 密文图像

3.1 加密效果

1) 自相关度

设图像 $P(M\times N)$是一个灰度级为 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 $G_{ij}^{rm}=\{p_{kl}\,|\,|k-i|\leqslant r,|l-j|\leqslant r,\ |p_{kl}-p_{ij}|\leqslant m|\}$,$r$ 和 m 分别为像素间距和灰度差,$0<r\leqslant M/2$,$0\leqslant m<L$. 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 k_1,k_4,k_5,对 cameraman 进行加密,微调其他参数略. 明文 cameraman 的自相关度为 0.874 878,加密后自相关度均小于 0.002 4,密文不可识别.

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 $XSD=1-\sum_i\sum_j(c_{ij}-p_{ij})^2\Big/\sum_i\sum_j p_{ij}^2$. 两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 k_1,k_2 对 cameraman 进行加密,微调其他参数略. 计算得出的明密文相似度均小于 0.646,明密文差异显著.

3) 信息熵

设 v_i 表示 L 级灰度图像的第 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_{10}对 cameraman 进行加密,微调其他参数略. 明文 cameraman 的信息熵为 6.904 609,加密后信息熵均大于 7.996 3,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 $PSNR=10\lg(\psi_{\max}^2/MSE)$,其中 $\psi_{\max}$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 20 dB 以下意味着密图完全不可辨识. 不断微调 k_{11},k_{12}对 cameraman 进行加密,微调其他参数略. 加密之后,峰值信噪比均小于 7.5 dB,明文被有效地掩盖.

5) 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_{12} 对 cameraman 进行加密,微调其他参数略.明文 cameraman 的水平相邻像素相关性为 0.919 512,垂直为 0.954 885,对角为0.896 048,加密后 3 个方向的相关性均小于 0.012,小于文献[4]中记载的 0.023 25,0.014 36,0.016 88,密图无法辨认.

3.2 安全性分析

本文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、1 组非线性的扩散和 1 组自适应的代换.其中的三维类仿射置乱在置乱像素位置的同时根据像素的当前坐标混合像素值,扩散和代换操作以像素行为单位交替进行,这种设计避免了文献[1-5]和文献[7]中算法设计的不足,使得明密文对之间的映射关系非常复杂,并且能够快速地搅乱图像中像素的值.它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.本文算法中迭代轮数越多,明密文之间的非线性关系越复杂,越难进行选择明文攻击,迭代 3 轮以后,明文中的像素已被充分搅乱.为使运算量不至于太大,限制迭代轮数为 3～6 轮.

1) 密钥空间

k_0 用 2 位二进制数表示,K_1 用 7 位二进制数表示,$k_2k_3k_4k_5k_6k_7k_8k_9k_{10}k_{11}k_{12}$ 均设置为 10 位十进制数,密钥空间为 $2^2\times2^7\times10^{10\times11}>2^{374}$.DES 算法密钥长度为 56 位,文献[3]算法小于 64 位,3-DES 算法为 112 位或 168 位,IDEA 为 128 位,文献[4]、文献[8]为 128 位,文献[5]算法小于 200 位,AES 为 128 位、192 位或 256 位.374 位已超过目前可接受的安全长度,假设密码分析员以每秒搜索 1 000 万亿个密钥的速度穷举攻击,需要 $1.623\,5\times10^{89}$ 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

分别微扰密钥中的各个参数对图 5 进行解密,得到的图像均类似于随机噪声,它们在视觉效果上同图 5 差不多,无法识别.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.

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 $R_{NPC}=\sum_{i,j}q(i,j)/(MN)$,$I_{UAC}=\sum_{i,j}|C_1(i,j)-C_2(i,j)|/(255MN)$,其中当 $C_1(i,j)=C_2(i,j)$ 时 $q(i,j)=0$,否则 $q(i,j)=1$.改动 cameraman 中不同像素,计算出一系列 R_{NPC} 和 I_{UAC}.计算结果表明 $R_{NPC}>0.995$,$I_{UAC}>0.329$,即明文中 1 个像素的微小改变将带来密文中 99.5%以上像素的变化,变化幅度在 32.9%以上.密文敏感性强,算法有很强的抗差分攻击能力.

4 结 论

本文算法首先采用三维类仿射变换进行初步加密,在置乱像素位置的同时根据像素坐标混合像素值,然后按行交替进行非线性的扩散、自适应的代换,在代换时用中间结果扰动耦合的多个混沌系统,使产生的混沌序列与图像数据密切相关.其中的置乱参数由混沌系统生成,置乱变换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.算法加密效果好,敏感性强,符合密码学中的扩散与混淆原则,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;构造的混沌系统形式简单,计算复杂度不高,易于并行实现.进一步研究的内容是在算法中融入更高维的混沌系统,并且使置乱操作也与图像数据密切相关.

参 考 文 献

[1] Wang Fangchao, Bai Sen, Zhu Guibin, et al. An image encryption algorithm based on N-dimension affine transformation [C] //Proc of the 8th IEEE/ACIS Int Conf on Computer and Information Science. Piscataway, NJ: IEEE, 2009: 579-585

[2] Chen Gang, Zhao Xiaoyu, Li Junli. A self-adaptive algorithm on image encryption [J]. Journal of Software, 2005, 16(11): 1975-1982

[3] Chen Shuai, Zhong Xianxin, Shi Junfeng, et al. Image encryption through discrete digital chaotic sequence [J]. Journal of Electronics & Information Technology, 2007, 9(4): 898-900 (in Chinese)
(陈帅,钟先信,石军锋,等. 基于离散数字混沌序列的图像加密[J]. 电子与信息学报, 2007, 29(4): 898-900)

[4] Peng Fei, Qiu Shuisheng, Long Min. An image encryption algorithm with parameters controlled by external keys [J]. Journal of South China University of Technology: Natural Science Edition, 2005, 33(7): 20-23 (in Chinese)

(彭飞, 丘水生, 龙敏. 外部密钥控制系统参数的图像加密算法[J]. 华南理工大学学报: 自然科学版, 2005, 33(7): 20-23)

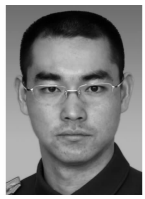
[5] Shang Zhenwei, Ren Honge, Zhang Jian. A block location scrambling algorithm of digital image based on arnold transformation [C] //Proc of the 9th Int Conf for Young Computer Scientists. Piscataway, NJ: IEEE, 2008: 2942-2947

[6] Xu Shujiang, Wang Yinglong, Wang Jizhi, et al. Cryptanalysis of two chaotic image encryption schemes based on permutation and XOR operations [C] //Proc of Int Conf on Computational Intelligence and Security. Piscataway, NJ: IEEE, 2008, 2: 433-437

[7] Ma Zaiguang, Qiu Shuisheng. An image cryptosystem based on general cat map [J]. Journal of China Institute of Communicaitons, 2003, 24(2): 51-57 (in Chinese)
(马在光, 丘水生. 基于广义猫映射的一种图像加密系统[J]. 通信学报, 2003, 24(2): 51-57)

[8] Chen Dongming. A feasible chaotic encryption scheme for image [C] //Proc of Int Workshop on Chaos-Fractals Theories and Applications. Piscataway, NJ: IEEE, 2009: 172-176

[9] Yuan Ning, Xuan Lei. Experimental research on hyper chaos stream cipher affected by parameter change [J]. Journal of Computer Research and Development, 2008, 45 (Suppl): 351-356 (in Chinese)
(袁宁, 宣蕾. 超混沌序列密码受参数变化影响的实验研究[J]. 计算机研究与发展, 2008, 45(增刊): 351-356)



Wen Changci, born in 1980. PhD candidate. His main research interests include information security and computer architecture.

Wang Qin, born in 1961. PhD, professor and PhD supervisor. Her main research interests include information security and computer architecture (wangqin@gmail.com).

Liu Xianghong, born in 1968. Master and senior engineer. His main research interests include information security and image processing.

Huang Fumin, born in 1980. Master. Her main research interests include information security and medical image processing.

Yuan Zhishu, born in 1974. Master, engineer. His main research interests include information security and image processing.