论文

基于超混沌系统的图像加密算法

林青, 王延江*, 王珺

中国石油大学(华东)信息与控制工程学院, 青岛 266580

* E-mail: yjwang@upc.edu.cn

收稿日期: 2016-03-25; 接受日期: 2016-06-26; 网络出版日期: 2016-08-29

国家自然科学基金(批准号: 61271407)资助项目

摘要 鉴于目前大多基于混沌序列的图像加密算法, 其置乱与扩散阶段是完全独立的, 用到不同的状态变量, 且密钥流完全依赖于密钥算法, 即密钥算法不变, 对不同的明文进行加密, 使用的密钥流完全是一样的, 难以抵御明文攻击或者选择性明文攻击. 而本文设计了一种具有动态可变的基于超混沌系统的加密算法. 首先, 对超混沌序列进行优化预处理, 得到随机性更理想的混沌序列, 其次利用优化预处理后的混沌序列创建与明文图像相关的动态可选序列, 最后构建与动态序列相关的密钥用于图像加密. 这样若明文与混沌序列发生微小的变化, 都会带来完全不同的密钥流. 通过仿真和大量的分析, 结果证明该算法具有较好的安全性和较高的有效性.

关键词 图像加密, 混沌系统, 超混沌系统, 图像置乱

1 引言

随着计算机网络及通信技术的发展, 数字图像技术的应用及传输也日渐增多. 为了防止网络传输的数字图像信息被非法用户截取和篡改, 必须对其进行加密处理, 以确保其传输的安全性和隐蔽性. 然而, 传统的加密技术只适用于文本文件, 对图像信息进行加密和解密时, 效率低且安全性差^[1]. 目前, 广泛用于图像加密的技术大体上分为两类: (1) 基于像素置换, 如Arnold变换、幻方变换及Hilbert曲线等, 这类变换的最大特点是具有一定的周期性, 其安全性较差; (2) 基于混沌系统的加密技术, 该技术具有遍历性、随机性及对初始值敏感等特点, 非常适于保密通信, 自20世纪90年代以来, 就有很多学者开始研究其在图像加密技术中的研究, 已取得了很大的发展^[2].

最初, 混沌加密技术大都是基于一维和二维的混沌加密系统^[3,4], 其形式简单、运行效率高, 但密钥空间小、不具敏感性, 导致不能抵抗各种攻击. 高维超混沌系统具有更大的Lyapunov指数和Kolmogorov熵, 比一般混沌系统具有更复杂的动力学特性, 如对初始值的敏感性更强, 随机性增大, 因此基于超混沌系统的图像加密技术已成为信息保密科学的趋势^[5].

目前, 某些基于超混沌序列的加密算法密钥弱, 最常见的问题是加密过程简单, 最严重的是密钥流完全依赖于密钥算法, 即密钥算法不变的话, 对不同的明文进行加密, 使用的密钥流都是一样的, 这样难以抵御明文攻击或者选择性明文攻击^[1,6-12]. 通常, 在图像加密系统中, 置乱和扩散是两个完全不同的阶段, 用到不同的密钥, 并且会用到单一的混沌序列进行置乱和扩散. 为了很好地弥补其缺陷, 本文提出了一种新的

引用格式: 林青, 王延江, 王珺. 基于超混沌系统的图像加密算法. 中国科学: 技术科学, 2016, 46: 910-918
Lin Q, Wang Y J, Wang J. The image encryption scheme with optional dynamic state variables based on hyperchaotic system (in Chinese). Sci Sin Tech, 2016, 46: 910-918, doi: 10.1360/N092016-00115

基于超混沌系统的加密方案: (1) 对超混沌序列进行预处理, 得到随机性、相关性、互相关性均达到理想的序列; (2) 构建与明文图像相关的密钥体系, 当为不同的明文图像进行加密时, 即使采用同一种密钥算法, 也会得到不同的密钥流, 能够抵抗已知明文攻击; (3) 置乱和扩散阶段构造密钥机制共享, 以便其发生微小的变化, 不仅会影响到扩散模型, 也会引起置乱阶段的变化; (4) 动态的选择状态序列, 进一步增大密钥空间.

2 超混沌序列及预处理

本文采用的是超混沌陈系统, 其动力学方程为^[13]

$$\begin{cases} \dot{x} = a(y-x) + \omega, \\ \dot{y} = dx - xz + cy, \\ \dot{z} = xy - bz, \\ \dot{\omega} = yz + r\omega, \end{cases} \quad (1)$$

式中, x, y, z, ω 为系统的状态变量, a, b, c, d, r 为系统的控制参数. 当 $a=35, b=3, c=12, d=7, 0.085 \leq r \leq 0.798$ 时, 系统进入超混沌状态. 系统状态变量的初始值及参数可以作为加密混沌序列的种子密钥.

理想的混沌序列统计特性应满足: 均匀分布, 自相关是冲激函数, 互相关为零^[14]. 此处, 保持参数 a, b, c, d 取值不变, $r=0.5$, 初始值 $x_0=1.256, y_0=1.387, z_0=1.566, \omega_0=1.867$, 采用四阶龙格-库塔(Runge-Kutta)法^[15]得到的混沌序列如图1所示(仅以 x 序列为例). 由图1可见, x

序列的值域范围 $(-25 < x(i) < 20)$ 较大, 不利于批处理, 均匀分布较差, 自相关和互相关均不理想. 因此需对其进行优化预处理. 经过统计分析, 需对混沌序列 x, y, z, ω 做如下处理: (1) 去除各序列值的整数部分, 统一值域在 $(0,1)$ 之间; (2) 为了使序列符合均匀分布, 并增强其随机性, 进一步缩小其取值范围. 所以其预处理过程如下:

$$x(i) = 10^{14}x(i) - \text{floor}(10^{14}x(i)) - 0.5, \quad (2)$$

式中, floor是取整运算. 其他3个序列的预处理过程同式(2).

图2是预处理之后的 x 混沌序列的统计特性. 同样, 其他3个混沌序列也用式(2)进行预处理. 由图2可见, x 序列经预处理之后, 值域范围减小 $(-0.5 < x(i) < 0.5)$, 自相关特性优于预处理前, 互相关性也更理想, 即预处理后的混沌序列伪随机性更强, 更适于图像加密.

3 加密算法

3.1 像素置乱

像素置乱的主要目的是打乱相邻像素的空间相关性, 掩藏图像的原始直观信息. 本文提出的置乱算法如下.

(1) 将大小为 $M \times N$ 的图像按从上到下, 由左至右的顺序排成一列.

图1 (网络版彩图)混沌序列 x 的自相关和互相关特性

(a) x 序列; (b) x 序列的自相关曲线; (c) x, y 的互相关曲线

 图2 (网络版彩图)预处理后混沌序列 x 的自相关和互相关特性

 (a) x 序列; (b) x 序列的自相关曲线; (c) x, y 的互相关曲线

(2) 动态选择与明文图像相关的状态, 其过程如下:

$$S(n) = \text{mod}(P(n-1), 4), \quad (3)$$

式中, mod 是求余数运算, $P(n-1)$ 是明文图像像素, 对于第一个像素, 初始值 $P(-1)$ 可作为种子. 当 $P(n-1)\%4=0$, $P(n-1)\%4=1$, $P(n-1)\%4=2$, $P(n-1)\%4=3$ 时, 依次选择预处理后的 $x(i)$, $y(i)$, $z(k)$, $\omega(l)$ 作为状态值; 若选择的状态序列 S 为 $\{\{x_0, x_1, \dots, x_i\}, \{y_0, y_1, \dots, y_j\}, \{z_0, z_1, \dots, z_k\}, \{\omega_0, \omega_1, \dots, \omega_l\}\}$, 则有 $i+j+k+l=M \times N$.

(3) 所有的像素点重复上述步骤.

(4) 对选择的状态序列 S 进行升序排序, 并构造索引置乱序列 L ; 利用索引置乱序列 L 实现图像像素的置乱, 置乱后的序列记为 $PR(i)$, $i=1, 2, \dots, M \times N$.

3.2 像素扩散

置乱虽然破坏了明文图像相邻像素的相关性, 但其灰度直方图不变, 不能抵御已知明文或选择性明文攻击. 为了提高加密图像的安全性, 需对置乱后的图像进行扩散操作, 即改变像素的值. 本文中设计的基于超混沌序列改变置乱图像像素值的步骤如下.

(1) 为了实现动态的构造一个密钥, 在扩散操作过程中利用像素置乱算法步骤中生成的序列 S 进行密钥构造. 由于一般情况下, 图像像素的长度为一个字节, 为了便于计算机运算, 采取密钥的长度也为一个字节, 引用的密钥构造式如下:

$$K(n) = \text{mod}(\text{fix}(S(n) \times 10^3), 256), \quad (4)$$

式中, fix 函数表示向0取整.

(2) 利用典型的扩散公式(式(5))得到密文像素的值.

$$C(n) = K(n) \oplus C(n-1) \oplus PR(n), \quad (5)$$

式中, $\oplus$ 表示异或运算, $K(n)$, $C(n)$, $C(n-1)$ 和 $PR(n)$ 分别表示密钥元素, 加密图像(密文)中当前和前一刻像素值, 像素置乱之后的序列值. 这类置乱与扩散方法的优点是明文有轻微地变化, 密文中便会引起较大地变化, 并且 $C(-1)$ 可以作为密钥种子.

实验中, 采用大小为 512×512 的标准测试图像Lena, 混沌序列的初始值如文中所述, 密钥种子 $P(-1)$ 及 $C(-1)$ 的值分别为0和1, 得到的置乱图像如图3(b)所示, 得到的加密图像如图3(c)所示. 由图3可以看到, 图像经置乱后已经完全没有原图像的任何轮廓等特征信息, 经加密之后整个图像肉眼观察基本呈现无序雪花状噪声, 因此在不受专业攻击时, 仅肉眼观察的角度来看本文加密效果较为理想. 后续将会从各种统计特性和专业攻击等方面定量分析本文加密算法效果.

4 仿真结果及分析

本实验以MATLAB2014为仿真平台, 在Intel(R) Core(TM) i5-5100的CPU, 4G内存, win7操作系统平台

图3 图像的加密效果
(a) 明文图像; (b) 置乱图像; (c) 加密图像

实现,采用的是标准测试图像Lena (512×512). 混沌系统的控制参数为 $a=35$, $b=3$, $c=12$, $d=7$, $r=0.5$, 系统状态的初始值为 $x_0=1.256$, $y_0=1.387$, $z_0=1.566$, $\omega_0=1.867$.

4.1 密钥空间分析

本文采用的算法中, 密钥空间由5个参数(x_0 , y_0 , z_0 , ω_0 , r)组成, 即超混沌系统参数的初始值、及控制参数 r 组成, 根据参考文献[1,5], 采用精确到小数点后15位的双精度表示^[5], 则密钥的空间总数为

$$K = 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \approx 2^{249}. \quad (6)$$

文献[1,5]的密钥空间均为 2^{199} , 由式(6)可以看到, 本文的密钥空间为 2^{249} , 远远高于文献[1,5]. 而且本文算法中明文图像的初始值 $P(-1)$, 密文的初始值 $C(-1)$ 可作为密钥种子, 再考虑到迭代次数, 理论上本算法的密钥空间无穷大, 能够实现香农的一次一密密钥体制, 能够有效地抵抗穷举攻击.

4.2 密钥敏感性分析

敏感性是有效密码系统的基本特征^[16,17], 主要从两方面论证, 一是使用不同的密钥为同一幅明文图像加密时, 能够产生两幅完全不同的加密图像, 二是解密密钥发生微小的变化, 也不能令加密图像进行正确解密.

本算法中系统参数的初始值为 $x_0=1.256$, $y_0=1.387$, $z_0=1.566$, $\omega_0=1.867$, 图4(b)是加密图像. 图4(c)~(i)分别是控制参数和系统初始值引入微小的变化, 所得到的加密图像以及它们之间的差分图像. 由差分图像可见, 密文图像间的差别较大. 表1是引入微小变化后, 加密图像间的差异率, 可以看到本文的差异率略高于文献[1]. 由上述可知, 本文算法加密效果较好, 且有较强

的敏感性.

4.3 直方图分析

数字图像的直方图反映的是图像像素值的分布. 图像经过加密之后, 像素值的分布应该是均匀分布的, 以便攻击者通过直方图看不到明文图像的信息, 能够抵御较强的统计分析攻击^[18,19]. 图5(a)~(c)分别是明文图像、置乱图像和加密图像的灰度直方图. 由图5可见, 置乱后图像的直方图没有任何改变, 加密后图像的灰度直方图与明文完全不同, 基本上是服从均匀分布的.

4.4 相关性分析

一幅图像相邻像素值比较接近, 相关性较高. 图像经置乱加密之后, 相邻像素值毫无规律, 即相关性较低. 计算相邻像素相关性的计算公式^[20]如下:

$$\begin{aligned} E(x_i) &= \frac{1}{N} \sum_{i=1}^N x_i, \\ D(x) &= \frac{1}{N} \sum_{i=1}^N [x_i - E(x_i)]^2, \\ \text{cov}(x, y) &= \frac{1}{N} \sum_{i=1}^N [x_i - E(x_i)][y_i - E(y_i)], \\ r_{xy} &= \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \end{aligned} \quad (7)$$

式中, x, y 表示图像相邻两个像素的灰度值, r_{xy} 表示相邻两个像素的相关系数, N 表示相邻像素对的数目. 随机选取标准测试图像Lena及其加密图像中的相邻的3000个像素, 对其用灰度值描点法及式(7)进行相关性分析. 将所取像素组成像素对, 以前一点的灰度值为横坐标, 以后一点灰度值为纵坐标, 描点得到图6. 可

图 4 敏感性测试

(a) 明文图像; (b) 加密图像; (c) $r_0=0.500000000001$ 加密图像; (d) $x_0=1.256000000001$ 加密图像; (e) $y_0=1.387000000001$ 加密图像; (f) $z_0=1.566000000001$ 加密图像; (g) $w_0=1.867000000001$ 加密图像; (h), (b)和(c)间的差分图像; (i), (b)和(d)间的差分图像

表 1 加密图像间的差异率

图像	加密密钥					差异率	文献[1]
	r_0	x_0	y_0	z_0	w_0		
参数 r_0 改变后的加密图像	0.5×10^{-12}	1.256	1.387	1.566	1.867	99.64%	—
初始值 x_0 改变后的加密图像	0.5	1.256×10^{-12}	1.387	1.566	1.867	99.65%	99.61%
初始值 y_0 改变后的加密图像	0.5	1.256	1.387×10^{-12}	1.566	1.867	99.64%	99.61%
初始值 z_0 改变后的加密图像	0.5	1.256	1.387	1.566×10^{-12}	1.867	99.63%	99.61%
初始值 w_0 改变后的加密图像	0.5	1.256	1.387	1.566	1.867×10^{-12}	99.61%	—

图 5 (网络版彩图)直方图

(a) 明文图像灰度直方图; (b) 置乱后的直方图; (c) 加密图像直方图

见原图像相关度较高,基本处于斜率为1的直线附近,而加密后的图像在一个矩形区域内基本处于均匀分布.利用式(7)对其相关性进行定量分析结果如表2所示.由计算的相关性数据及图6可以看到,明文图像相邻像素具有较高的相关性($r_{xy} \rightarrow 1$),但加密之后图像的相邻元素几乎不相关($r_{xy} \rightarrow 0$).而且相较于文献[21],本算法对于削弱相邻像素相关性取得的效果更佳.

4.5 信息熵分析

信息熵反映了信息的随机性和不可预测性,在数字图像中,像素的灰度值分布越均匀,熵越大,随机性越大,安全性越高.信息熵的公式为

$$H(X) = -\sum_{i=1}^n p(x_i) \log \frac{1}{p(x_i)}, \quad (8)$$

式中, X 是一个随机变量,此处为一幅图像像素灰度值

集合, $p(x_i)$ 是像素值为 x_i 出现的概率, n 是像素的灰度级数.通常,数字图像的灰度级为256,其理想的熵值为8(均匀分布).本文算法中,得到的密文图像的熵为7.9967,接近理想值8,说明此算法随机性好,不确定性高,安全性好.

4.6 抗差分攻击能力分析

差分抗攻击能力依赖于其对明文图像的敏感度,对明文图像的敏感性越强,抵抗差分能力就越高.通常用像素变化率(number of pixels change rate, NPCR)和归一化像素值平均改变强度(unified average changing intensity, UACI)两项指标来衡量.假设在两幅明文图像中只有一个像素点不同,在它们的加密图像中点 (i, j) 的值分别为 $C_1(i, j)$ 和 $C_2(i, j)$.如果 $C_1(i, j) = C_2(i, j)$, $D(i, j) = 0$,反之, $C_1(i, j) \neq C_2(i, j)$, 则 $D(i, j) = 1$. 则NPCR和UACI的定义如下:

图 6 (网络版彩图)相邻像素垂直方向上的相关分布

(a) 明文图像相关分布; (b) 密文图像相关分布

表2 相邻像素的相关系数

相邻方向	明文	密文	文献[21]
水平方向	0.9754	-0.0032	0.0064
垂直方向	0.9863	-0.0063	0.0084
对角方向	0.9479	0.0086	0.0107

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N D(i, j) \times 100\%, \quad (9)$$

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\%, \quad (10)$$

式中, M 与 N 分别是图像的行和列. 实验中, 采用Lena图像进行加密, 一幅是原始图像, 另一幅是原始图像任意一个像素点(本例中是第二行第二列)的最低位取反, 即“0”→“1”, 依据式(9)和(10)得到NPCR与UACI的值分别是99.72%和33.74%. 而文献[5]中分别是99.6231%和33.5042%, 文献[22]分别是99.6057%和33.4049%. 很明显, 本文算法的敏感性高于文献[5,22], 所以本算法具有更强的抗差分攻击能力.

4.7 噪声攻击及剪切攻击分析

在通信系统中, 图像的传输不可避免地会遇到

各种数据处理、人为攻击以及噪声污染等, 本文对一些常见的攻击进行了MATLAB仿真.

4.7.1 噪声攻击

噪声攻击分为两大类, 一是加密之前, 原始图像被噪声污染, 二是加密之后, 在传输的过程中被信道中的噪声污染. 此处, 对这两种情况都进行了MATLAB仿真.

图7(a)是加有5%椒盐噪声的图像, 利用本文算法对含有噪声的图像直接进行加密, 得到的密文图像如图7(b)所示, 到了接收端, 对其进行解密, 并用中值滤波器去噪, 得到的最终图像如图7(c)所示. 从图中可以看出, 本算法能够较好地抵抗噪声干扰, 效果较好.

图7(e)是密文图像(图7(d))在传递过程中受到高斯白噪声的干扰(噪声比例为3%), 利用本文算法解密, 得到的图像如图7(f)所示. 可以看到, 重建图像仍

图7 噪声攻击测试

(a) 含有5%椒盐噪声的图像; (b) 加密图像; (c) 解密去噪后的图像; (d) 密文图像; (e) 受高斯噪声污染的加密图像; (f) 解密图像

有噪声, 但能够识别出原始图像的主要信息, 可以根据需要对解密后的图像进行滤波处理. 由上可见, 本算法具有较强的抗噪声攻击能力.

4.7.2 剪切攻击

图像信息在传输过程中, 会遭到人为地破坏, 最常见的就是剪切攻击. 图8(a)和(c)是加密图像在不同位置不同大小的切割, 图8(b)和(d)分别是它们的解密图像. 由解密图像可以看到, 即使剪切攻击丢失了部分图像信息, 但图像的主要信息仍可以恢复出来, 所以本算法能够抵抗剪切攻击.

5 结论

本文提出了一个基于超混沌系统的加密算法. 该算法首先对混沌序列进行预处理改造, 得到随机性及相关性更理想的序列; 其次是利用预处理序列得到与明文图像相关的动态可选的序列 $S(n)$; 最后在置乱和扩散过程中都用到 $S(n)$ 来构造密钥. 分析和仿真结果表明, 预处理后序列对初始值具有更高的敏感性, 使得密钥空间非常大, 而动态选择与图像像素相关的状态能够使不同的明文图像获得不同的密钥, 可以很方

图8 剪切攻击测试

(a) 加密图像; (b) 解密图像; (c) 加密图像; (d) 解密图像

便地构成一次一密的密钥体制, 明文或序列发生微小的变化都会带来完全不同的密钥流. 这些结果都证明了该算法的优越安全性和有效性.

参考文献

- Chen J X, Zhu Z L, Fu C, et al. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. *Commun Nonlinear Sci Numer Simul*, 2015, 20: 846–860
- 李昌刚, 韩正之. 图像加密技术新进展. *信息与控制*, 2003, 32: 339–343
- Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. *Int J Bifurcat Chaos*, 1998, 08: 1259–1284
- 闵乐泉, 杨森, 张兴华. 基于广义混沌同步的数字图像隐藏方案. *北京科技大学学报*, 2003, 25: 477–479
- 钟厚桥, 李建民, 林振荣, 等. 基于超混沌序列的加密方案. *计算机应用研究*, 2013, 30: 3110–3113
- Solak E, Çokal C, Yildiz O T, et al. Cryptanalysis of Fridrich's chaotic image encryption. *Int J Bifurcat Chaos*, 2010, 20: 1405–1413
- Rhouma R, Solak E, Belghith S. Cryptanalysis of a new substitution-diffusion based image cipher. *Commun Nonlinear Sci Numer Simul*, 2010, 15: 1887–1892
- Li C, Li S, Asim M, et al. On the security defects of an image encryption scheme. *Image Vis Comput*, 2009, 27: 1371–1381
- Arroyo D, Li S, Amigó J M, et al. Comment on “Image encryption with chaotically coupled chaotic maps”. *Phys D*, 2010, 239: 1002–1006
- Çokal C, Solak E. Cryptanalysis of a chaos-based image encryption algorithm. *Phys Lett A*, 2009, 373: 1357–1360
- Wang K, Pei K, Zou L, et al. On the security of 3D Cat map based symmetric image encryption scheme. *Phys Lett A*, 2005, 343: 432–439
- Li C, Liu Y, Zhang L Y, et al. Cryptanalyzing a class of image encryption schemes based on Chinese remainder theorem. *Signal Process-Image*, 2014, 29: 914–920
- 武相军, 王兴元. 基于非线性控制的超混沌Chen系统混沌同步. *物理学报*, 2006, 55: 6261–6206
- 王英, 郑德玲, 鞠磊. 基于Lorenz混沌的数字图像加密算法. *北京科技大学学报*, 2004, 26: 678–682
- Liu H, Kadir A, Niu Y. Chaos-based color image block encryption scheme using S-box. *AEU-Int J Electronics Commun*, 2014, 68: 676–686
- Zhang W, Wong K, Yu H, et al. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. *Commun Nonlinear Sci Numer Simul*, 2013, 18: 2066–2080

- 17 Wang Y, Wong K W, Liao X, et al. A new chaos-based fast image encryption algorithm. [Appl Soft Comput](#), 2011, 11: 514–522
- 18 Zhang W, Wong K, Yu H, et al. A symmetric color image encryption algorithm using the intrinsic features of bit distributions. [Commun Nonlinear Sci Numer Simul](#), 2013, 18: 584–600
- 19 Zhang X, Zhao Z, Wang J. Chaotic image encryption based on circular substitution box and key stream buffer. [Signal Process-Image](#), 2014, 29: 902–913
- 20 Gao T, Chen Z. A new image encryption algorithm based on hyper-chaos. [Phys Lett A](#), 2008, 372: 394–400
- 21 卢辉斌, 孙艳. 基于新的超混沌系统的图像加密方案. [计算机科学](#), 2011, 38: 149–152
- 22 朱从旭, 胡玉平, 孙克辉. 基于超混沌系统和密文交错扩散的图像加密新算法. [电子与信息学报](#), 2012, 34: 1735–1742

The image encryption scheme with optional dynamic state variables based on hyperchaotic system

LIN Qing, WANG YanJiang & WANG Jun

College of Information and Control Engineering, China University of Petroleum, Qingdao 266580, China

In view of most of the current image encryption algorithm based on chaotic sequences, the permutation and diffusion procedures are completely independent, use different state variables, and the key stream is completely dependent on the key algorithm, namely, constant algorithm key words of different plaintexts are encrypted, using the key flow is the same, so it is difficult to resist the plaintext attack or selective plaintext attack. This paper has designed a dynamic encryption algorithm based on hyperchaotic system. In this paper, the system is pre-processed to obtain the ideal chaotic sequence which has the better randomness, and the dynamic alternative sequence associated with the plain image is constructed, the secret key related to the dynamic sequence is created, which is used for the permutation and diffusion processes of digital image. In the proposed algorithm, if plain image or the chaotic sequences has minor changes, it will result an entirely different key stream. Experimental simulations and a lot of cryptanalysis have been carried out, the results prove the superior security and high efficiency of the scheme.

image encryption, chaotic system, hyperchaotic system, image permutation

doi: 10.1360/N092016-00115