

基于混沌序列和 CBC 模式的数字图像加密算法

廖琪男

(广西财经学院 计算机与信息管理学系, 广西南宁 530003)

摘 要: 为了实现对数字图像信息的有效保护, 提出了一种基于 Lorenz 混沌序列和类似 CBC 模式的图像加密算法. 首先对 Lorenz 系统输出的三维混沌序列进行改进, 使其具有理想的伪随机特性. 然后, 根据这三维序列移位图像的像素位置. 将图像分块, 根据这三维序列和 CBC 模式改变每一块的像素值, 从而实现图像加密; 解密时, 给出一种基于邻域相邻像素特性的加密图像抗剪切攻击恢复算法. 最后应用评价指标对加解密效果和安全性进行分析.

关键词: Lorenz 混沌序列; 链式加密; 图像加密; 图像抗剪切恢复

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2011)03-0165-05

Digital Image Encryption Algorithm Based on Chaos Sequence and CBC Mode

LIAO Qi-nan

(Department of Computer and Information Managing,
Guangxi University of Finance and Economics, Nanning 530003, China)

Abstract: In order to protect digital image's information, an image encryption algorithm based on Lorenz chaos sequence and similar CBC (Cipher Block Chaining) mode is presented. Firstly, 3D Lorenz chaotic sequences are improved to be with ideal pseudo-randomness. Then, the image's pixel positions are shifted by using the 3D sequence. The image is divided into blocks, and the pixel value in each block is altered based on the 3D sequence and CBC, so that the image will be scrambled and encrypted. While doing the decryption, a method is provided based on the neighboring pixels characteristic to renew the image attacked by shearing. Lastly, the effects of encryption, decryption and security are also analyzed by using the method of accessing.

Key words: Lorenz chaos sequence; chaining encryption; image encryption; renew the encrypt image sheared

1 引言

为了有效保护数字图像信息, 提高图像加密的效率和安全性, 有许多图像加密算法被提出来^[1-6]. 文献[1]提出一种基于混沌序列的像素置乱和像素值变换的数字图像加密算法; 文献[2]提出, 将图像块的重要信息嵌入到由混沌系统决定的另一图像块中的最低位, 以提高加密图像的抗剪切能力. 这种算法, 一旦受到轻微的噪声干扰就无法恢复被剪切部分的图像. 当被剪切块的重要信息对应的隐藏块也被剪切时, 该图块也将无法恢复; 文献[3]给出一种

基于图像位平面的图像加密算法, 同时给出一种抗剪切恢复算法. 但被剪切像素的恢复依赖于该像素的 8 个位平面的恢复值, 从低位平面到高位平面的像素值的不正确性以指数比例影响到像素值的不正确性, 致使恢复的图像质量不理想.

文中提出了基于 Lorenz 混沌序列和 CBC 模式的图像加密算法, 以及在此基础上的抗剪切攻击解密算法.

2 Lorenz 混沌序列及其改进

Lorenz 系统是一个经典的三维自治系统, 其动

力学方程为:

$$\begin{cases} dx/dt = \sigma(y-x) \\ dy/dt = rx - zx - y \\ dz/dt = xy - bz \end{cases} \quad (1)$$

其中, σ, r, b 为系统参数, 当 $\sigma = 10, r = 28, b = 8/3$ 时, 系统进入混沌状态. 文中采用经典的四阶 Runge-Kutta 法来求解方程. 对于初始条件 (x_0, y_0, z_0) , 可以得到三维混沌序列 $\{(x_i, y_i, z_i) \mid i = 1, 2, 3, \dots\}$, 该序列非周期、不收敛、对初始值 (x_0, y_0, z_0) 非常敏感.

以 $(x_0 = -1.1, y_0 = 0, z_0 = 1.2)$, 积分步长 $h = 0.001$ 来计算 Lorenz 混沌序列, 求出各序列的 100000 项, 得到的 x 序列的后 2000 项、 x 的自相关性和 $x-z$ 的互相关性如图 1 所示.

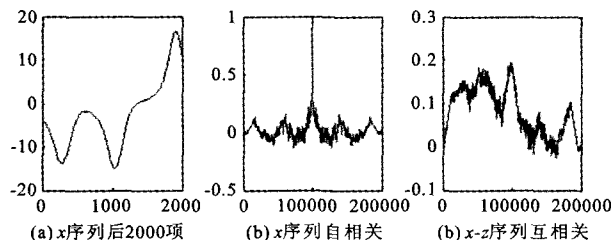


图 1 Lorenz 混沌序列及其自相关和互相关特性

按照 Golomb 对伪随机序列提出的三个公设, 理想的混沌序列应具有统计特性: 均匀分布, 自相关是 δ 函数, 互相关是零. 由此可见, 原方程产生的序列不是很理想的伪随机序列. 为此, 本算法对原方程产生的混沌序列作如下改进^[1]:

(1) 将序列的小数点右移 k 位 ($k = 0, 1, 2, 3, \dots$);

(2) 将序列映射到值域 $(-0.5, +0.5)$.

计算公式为:

$$\begin{cases} x(i) = 10^k x(i) - \text{round}(10^k x(i)) \\ y(i) = 10^k y(i) - \text{round}(10^k y(i)) \\ z(i) = 10^k z(i) - \text{round}(10^k z(i)) \end{cases} \quad (2)$$

其中, round 取最近整数. 上面的序列经式 (2) 处理后 ($k = 4$), 其序列值和整体序列相关性如图 2 所示. 此时, 序列值分布均匀, 自相关为理想的 δ 函数, 互相关近似为零, 是理想的伪随机序列. 实验证明, 原序列对于不同的初值, 其序列相关性相差很大, 而经改进后的序列的相关性却都几乎一致.

3 加密算法

为了提高加密图像的抗剪切能力和抗像素特征值统计攻击能力, 文中算法同时采用像素位置变换和像素值变换加密, 需要产生如下混沌序列.

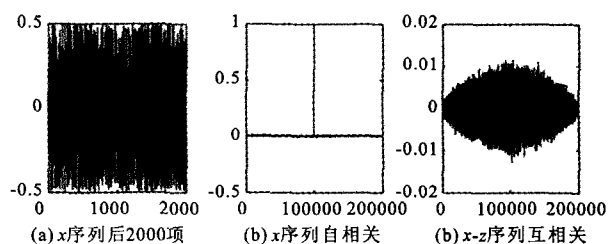


图 2 改进后 Lorenz 混沌序列及其自相关和互相关特性

设数字图像大小为 $m \times n$, 由 Lorenz 系统产生的原序列经式 (2) 处理后生成混沌序列:

$$\{(X_i, Y_i, Z_i) \mid i = 1, 2, 3, \dots, m \times n\} \quad (3)$$

序列 $\{X_i \mid i = 1, 2, 3, \dots, m \times n\}, \{Y_i \mid i = 1, 2, 3, \dots, m \times n\}, \{Z_i \mid i = 1, 2, 3, \dots, m \times n\}$ 将用于数字图像的像素位置加密和像素值加密.

3.1 基于混沌序列的像素位置变换

为了达到较好的置乱效果, 文中应用混沌序列的伪随机性和遍历性, 由混沌序列决定将原像素 (i, j) 变换到新位置 (row, col) .

将混沌序列 $\{X_i \mid i = 1, 2, 3, \dots, m \times n\}$ 按升序或降序排序得到新的有序序列 $\{cX_i \mid i = 1, 2, 3, \dots, m \times n\}$, 将 $cX(i)$ 值用其在 X_i 中的位置索引值替代, 即得到服从 $[1, m \times n]$ 的稳定整数 (排序位置) 分布的混沌随机序列 $\{sX_i \mid i = 1, 2, 3, \dots, m \times n\}$, 依次按该序列值一把原图像的像素 (i, j) 按行列顺序变换到 (row, col) 的新位置为:

$$\begin{cases} row = \lfloor \frac{sX((i-1)n+j)}{n} \rfloor + 1 \\ col = sX((i-1)n+j) \bmod n \end{cases} \quad (4)$$

式中, $i = 1, 2, 3, \dots, m; j = 1, 2, 3, \dots, n$. 上式计算后, 若 $col = 0$, 则 $row = row - 1, col = n$.

如是 24bit 或 48bit 真彩图像, 可以分别用 X, Y, Z 序列把 RGB 分量的像素移位到新的位置, 实现三分量分别置乱.

3.2 基于异或运算的像素值变换

为了提高加密的安全性, 以块为单位, 采用类似 CBC (Cipher Block Chaining) 的加密算法, 依次对每一块的所有像素进行链式加密, 方法如下:

(1) 图像分块

设分块大小为 $h \times w$ (分块大小视图像大小与加密安全性而定), 则可将图像分为 $u \times v$ 块, 如图 3 所示. 对于行方向, 前 $v-1$ 块, 每块的宽为 w , 第 v 块的宽度为 $w + (n \bmod w)$; 对于列方向, 前 $u-1$ 块, 每块的高为 h , 第 u 块的高度为 $h + (m \bmod h)$, 即:

$$\begin{cases} m = (u-1)h + (h + (m \bmod h)) \\ n = (v-1)w + (w + (n \bmod w)) \end{cases} \quad (5)$$

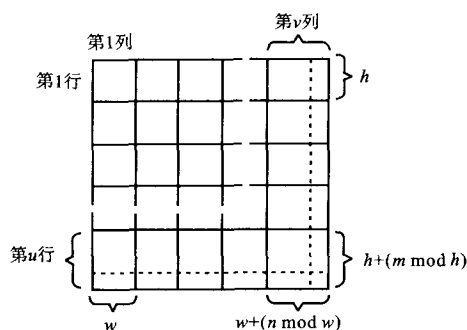


图3 图像分块示意图

(2) 将混沌序列变换为无符号整数

将混沌序列变换为无符号整数作为可供选择的 XOR 操作数:

$$\begin{cases} mX(i) = \text{round}((X(i) + 0.5) \times 10^k) \bmod L \\ mY(i) = \text{round}((Y(i) + 0.5) \times 10^k) \bmod L \\ mZ(i) = \text{round}((Z(i) + 0.5) \times 10^k) \bmod L \end{cases} \quad (6)$$

式中, $i = 1, 2, 3, \dots, m \times n$, $k \geq 4$. L 是图像像素值数, L 的取值与图像类型有关, 如表 1 所示.

表 1 L 取值

图像类型	L 取值
48bit 真彩图像、16bit 灰度图像	65536
24bit 真彩、8bit 灰度图像、256 色索引图像	256
16 色索引图像	4
二值图像	2

(3) 像素值加密

为了使算法实现方便, 把块像素用一维矩阵表示, 则第 i 行第 j 列的第 k 像素表示为 $P(i, j, k)$, 加密后为:

$$\begin{cases} C(i, j, k) = P(i, j, k) \oplus C(i, j, k-1) \oplus mX(p) \\ C(i, j, 0) = f(i, j) \bmod L \end{cases} \quad (7)$$

其中, $P(i, j, k)$ 和 $C(i, j, k)$ 分别为当前被加密像素和加密后像素, $C(i, j, k-1)$ 为前一已加密像素. $C(i, j, 0)$ 为初始密文, 通过 $f(i, j)$ 实现随机取值. $i = 1, 2, 3, \dots, u$; $j = 1, 2, 3, \dots, v$; k 的取值范围与块有关(见图 3 所示), $k = 1, 2, 3, \dots, p$ 为当前被加密像素序号, $p = 1, 2, 3, \dots, m \times n$.

$f(i, j)$ 可以是自定义函数, 也可以通过 mX 、 mY 、 mZ 序列之一取得随机值. 在构造自定义函数 $f(i, j)$ 时, 为了进一步提高加密的安全性, 应考虑 $f(i, j)$ 初值及其对变量 (i, j) 的敏感性, 即要使 $f(i, j)$ 初值为适当常量(根据 L 值确定), (i, j) 的微

小变化, 将引起 $f(i, j)$ 的很大变化. $f(i, j)$ 也可以引入密钥 key , 使 $f(i, j, key)$ 更加安全.

如是真彩图像, 可以分别用 mX, mY, mZ 序列把 RGB 分量的像素值加密. 对于索引图像, 还应该对相应的调色板加密.

图像像素值经随机变换后, 将彻底改变原图像的灰度直方图统计特性.

根据 XOR 运算性质, 解密算法为:

$$\begin{cases} P(i, j, k) = C(i, j, k) \oplus C(i, j, k-1) \oplus mX(p) \\ C(i, j, 0) = f(i, j) \bmod L \end{cases} \quad (8)$$

4 抗剪切攻击解密算法

文中加密算法是可逆算法, 按加密算法反向运算即可得到无损原图像. 为了抵抗恶意剪切或涂鸦等攻击, 提出一种抗剪切攻击解密恢复算法. 本算法的可靠性是基于文中加密算法的像素置乱和像素值扩散分布均匀的特性. 图 4 是本算法原理示意图. 本算法就是恢复 F 处的像素值.

4.1 检测被剪切图像

解密前, 检测被剪切像素. 经过像素置乱和像素值变换双重加密后的图像, 相邻像素几乎不相关, 如图 4(a)所示. 除二值图像外, 如连续出现 2~3 个像素的像素值一样的, 则认为这些像素是被剪切像素. 在本文加密算法下, 多次实验证明, 取连续 3 个像素作为判断条件是很可靠的.

设用 $\text{flag } m \times n$ (对于 RGB 图像, 可用 $m \times n \times 3$) 无符号整数矩阵标记加密图像被剪切像素, 并初始化为零. 从第 1 行第 1 列开始逐行逐列扫描, 如连续 3 个像素值相等, 则与这些像素对应的 flag 置 1.

因为剪切边界邻域像素可能有与剪切区域像素值相同的像素被误判为被剪切像素, 如是 RGB 图像, 被剪切像素 flag 应取各分量的被剪切像素最少的对应 flag 分量作为计算被剪切像素.

flag 标志位(如图 4(b)所示)需变换到被剪切像素在解密后的位置 flag (如图 4(c)所示).

241	35	138	55	55	91	241	35	138	55	55	91	90	F	110	125	160	F
5	45	175	215	250	25	5	F	F	F	250	25	90	100	122	F	F	165
81	75	235	77	215	65	81	F	F	F	225	65	F	120	F	150	160	175
25	175	45	111	89	135	25	F	F	F	F	135	110	F	145	F	170	F
135	80	66	220	125	5	135	F	F	F	F	5	F	135	F	160	F	180
90	250	80	60	85	10	90	250	80	60	85	10	130	F	135	160	180	F

(a) 加密像素值

(b) 被剪像素标记

(c) 解密像素

图 4 抗剪切算法原理示意图

4.2 基于邻域像素相关特性的抗剪切恢复算法

本算法简称 Np 恢复算法. 图像解密后, 被剪切像素已均匀分散在整个图像. 应用 4 邻域相邻像素相关特性, 即高度相关, 被剪切像素的像素值取值可以根据邻域像素决定. 文中算法是:

(1) 根据 flag, 恢复第 1 行、第 1 列、第 m 行和第 n 列被剪切像素值, 取其邻值或邻值平均值;

(2) 从第 2 行第 2 列像素开始, 根据 flag 逐行逐列计算被剪切像素, 如其右邻域像素不被剪切, 则取左右邻域像素值平均值; 否则, 如其下邻域像素不被剪切, 则取上下邻域像素值平均值; 否则, 如其下邻域像素被剪切, 则取左邻域像素值和上邻域像素值的平均值.

5 实验结果分析

文中算法进行了大量的实验, 实验结果都表明本文算法的有效性. 限于篇幅, 在此仅给出验证与分析文中算法的代表性实验.

仿真实验采用 Matlab7.1 平台, Lorenz 系统参数 $\sigma=10, r=28, b=8/3$; 初始值 $(x_0 = -1.1, y_0 = 0, z_0 = 1.2)$, 积分步长 $h=0.001$, 迭代次数 10^5 , 式(2)中 $k=4$, 式(6)中 $k=7$.

(1) 灰度图像加密实验. 图像选用 256 级灰度图像 lena 256×256 , 采用 16×16 分块, 选 X 序列用于位置加密和像素值加密, 取序列的最后 256×256 项, 式(7)中 $f(i, j) = i^2 j + 3ij + ij^2 + 100$. 实验结果如图 5 所示. 图中给出了原图像及其灰度直方图、加密图像及其灰度直方图.

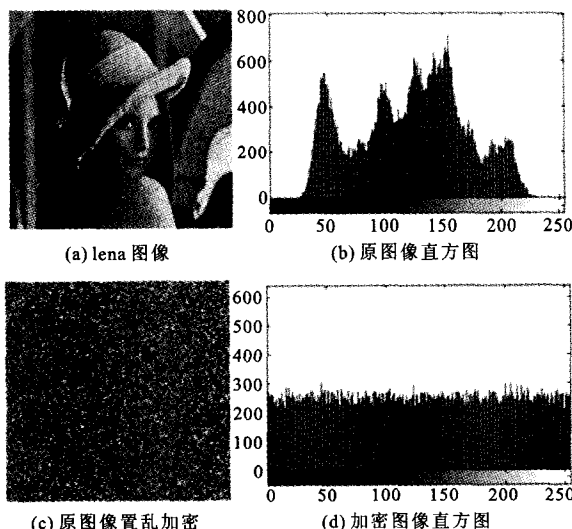


图 5 文中算法 lena 灰度图像加密效果图

(2) 二值图像加密实验. 图像选用 logo $90 \times$

90, 采用 9×9 分块, 选 X 序列用于位置加密和像素值加密, 取序列的最后 90×90 项, 式(7)中 $f(i, j) = i^2 j + 3ij + ij^2 + 1$. 图 6 是实验结果. 图中给出了原图像及其像素值统计直方图、加密图像及其像素值统计直方图.

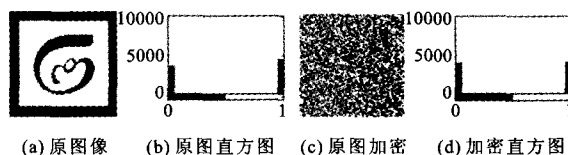


图 6 文中算法 logo 二值图像加密效果图

实验结果表明, 该算法密钥空间大, 具有较好的加解密效果和效率, 并对统计分析具有较好的安全性和较强的抗剪切攻击能力.

5.1 密钥安全性分析

本算法的密钥安全主要由 Lorenz 系统保证, 仅以双精度浮点数初值 (x_0, y_0, z_0) 为密钥, 文中算法的密钥空间就是 $2^{192} \approx 6.28 \times 10^{57}$, 密钥空间足够大. 实验修改初值 x_0 和 y_0 仅相差 10^{-15} , z_0 仅相差 10^{-14} , 得到的解密图像仍然是面目全非的杂乱无章的图像. 这说明本文算法对密钥具有极强的敏感性, 也表明改进后的混沌序列仍对系统初值极其敏感.

5.2 统计特性分析

(1) 灰度直方图

实验结果表明, 文中算法像素值扩散能力很强, 任意加密图像的像素值在整个取值空间范围内均匀分布且像素统计值几乎是趋于一致, 彻底改变了原图像统计特性. 单灰度级图像或其他单色彩色图像的加密也达到同样的效果, 图 7 是 256×256 中灰度级图像的加密前后直方图.

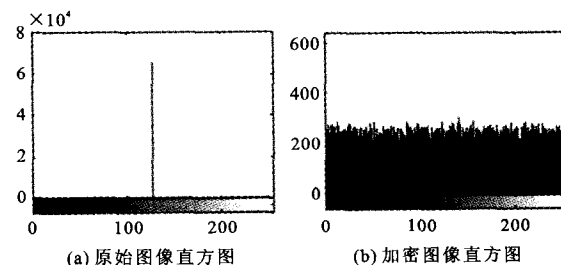


图 7 中灰度级图像加密前后灰度直方图

(2) 相邻像素的相关性

为了分析图像的相关性, 引入了相邻像素的相关系数. 其计算表达式如下:

$$R_{xy} = \text{cov}(x, y) / \sqrt{D(x)D(y)} \quad (9)$$

其中, x 和 y 分别表示图像中两个相邻像素的灰度值, $\text{cov}(x, y) = E((x - E(x))(y - E(y)))$ 为协方差, 方差 $D(x) = E((x - E(x))^2)$, $E(x)$ 为均值.

实验分别对图像 lena 在水平、垂直和对角方向的全部相邻像素对进行了像素相关性测试, lena 灰度图像和 logo 二值图像的相关系数实验结果如表 2 所示.

表 2 相邻像素的相关系数

	lena		logo	
	原图像	加密图像	原图像	加密图像
水平	0.9200	-0.0013	0.9039	-0.0065
垂直	0.9575	0.0035	0.8924	-0.0120
对角	0.8979	0.0016	0.8239	0.0177

为了从视觉上体验相邻像素相关性, 分别在 lena 图像和加密图像的水平方向各随机选择 1000 组相邻像素, 其相关系数分别为 0.9198 和 0.0095, 其相邻像素点灰度值关系如图 8 所示. 可以看出, 原图像相邻像素点围绕 $y=x$ 直线方向高度集中, 加密图像在 0~255 均匀分布. 垂直和对角方向也得到相类似的实验结果.

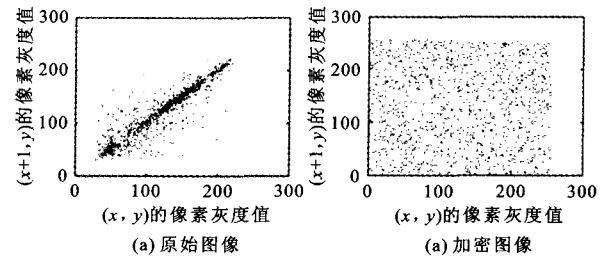


图 8 lena 图像水平方向相邻像素的相关性分布

以上实验数据表明, 原始图像中相邻像素之间存在着高度相关(相关系数在 $\pm 0.80 \sim \pm 1.00$), 而加密图像相邻像素的相关系数几乎为 0, 相邻像素几乎不相关, 说明加密图像的分散性很好.

(3) 信息熵

信息熵可以度量出图像中灰度值的分布, 灰度分布越均匀, 图像信息熵越大, 反之信息熵越小. 信息熵的计算表达式如下^[4]:

$$H(x) = - \sum_{i=1}^n p(x_i) \log_2 p(x_i)$$

(10)

式中, x 为随机变量, $p(x_i)$ 为 x_i 出现的概率, x 表示图像的像素值.

根据上面熵计算表达式计算, 本实验 lena 加密图像 lena 加密图像的信息熵为 7.9970, 都很接近 256 级灰度图像信息熵的理论最大值 8; logo 加密图像的信息熵 $H=1.0000$, 达到二值图像信息熵的理论最大值 1. 这些实验数据说明, 这些图像所有的像素值出现的概率几乎是一致的.

5.3 抗剪切抗涂鸦能力

(1) 被剪切被涂鸦区域检测

文中被剪切区域算法是基于等像素值的, 所以也适用于涂鸦等恶意攻击的不规则区域检测与记录. 这里用 220×150 矩形剪切区域(即图像的二分之一剪切面积)实验.

flag 检测的被剪切像素和对应的灰度图像显示, 剪切区域外被误检 3 个像素, 剪切区域左边界邻域被误检 1 个像素. 大量实验表明, 在文中加密算法基础上, 本被剪切区域检测算法误检率一般多在万分之一以内, 检测算法可靠度可视为 100%, 被剪切检出率可视为 100%. 如表 3 所示.

表 3 被剪切图像检测数据

剪切区域外 误检像素	误检剪切区域 边界邻域像素	220×150 剪切后 被检像素
3	1	33004

(2) 被剪切被涂鸦图像解密恢复

图 9 是文中加密图像被随机剪切二分之一面积(220×150 剪切区域)时的图像解密恢复效果. 直接解密恢复的图像虽有大量的噪声点, 但仍然可识别图像信息, 说明本算法具有比较强的抗剪切能力; Np 恢复算法恢复的图像很理想, 相质还原好, 峰值信噪比 PSNR 达到 26.78. 说明了文中加密算法像素置乱和像素值扩散分布均匀, 从解密后的噪声点分布也证明了这一结论.

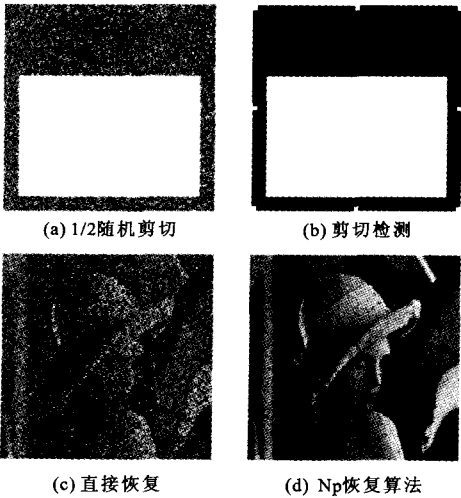


图 9 抗剪切攻击实验效果图

由 CBC 加密原理知, 一个像素被剪切或涂鸦, 将使其及前一像素得不到正确恢复. 按照先像素位置变换后像素值加密, 不能正确恢复的只是被剪切

(下转第 174 页)

辑发生改变时,程序员只需要编写一个新的 isotope element,用它来替换旧的 isotope element,系统甚至不需要重启;当仅仅映射关系发生改变时,程序员只需要修改规则文件即可,其他的一切都不用改变。由此可见,对于上下文频频发生变化的普适计算环境下,IPM 的适应性是极高的,它为开发人员减轻了大量的负担,频繁的上下文变更仅需要程序员一个简单的动作即可以完成,整个系统不需要二次开发、重新部署等,代码的维护量大大减少。

IPM 消除了程序中冗繁的条件分支语句,程序员不再需要用大量的分支语句来对上下文环境和方法之间的匹配进行关联,这些关联都由规则文件来完成,易于书写,也易于修改,不仅从结构上更加合理,更加清楚明晰,而且使得程序各模块各部分之间解耦,相互之间的依赖性降低。

综上所述,IPM 较之传统语言在普适计算编程环境中拥有很大的优势,对于普适环境中泛在设备的动态性、异构性以及环境的复杂性和多变性方面都有较好的适应。

5 结束语

文中主要介绍了 IPM 的实施,IPM 的实施是以面向对象模型为基础,针对上下文感知应用方面进行扩展,添加新的语言成分,使程序员在开发上下文感知应用时,只需要关心应用的抽象操作,不必考虑

当时的上下文情况。IPM 使上下文数据与业务逻辑松耦合,比起传统的面向对象编程,更利于上下文感知应用的开发。在以后的工作中,需要对 IPM 的支撑技术如上下文信息的管理、推理、聚合等方面加大研究力度。

参考文献:

- [1] Henricksen K, Indulska J. A software engineering framework for context-aware pervasive computing[C]// Proceedings of the Second IEEE Annual Conference, USA; IEEE, 2004;77-86.
- [2] Brown P J, Jones G J F. Context-aware retrieval: exploring a new environment for information retrieval and information filtering[J]. Personal and Ubiquitous Computing, 2001,5(4):253-263.
- [3] Pascoe J. The stick note architecture: extending the interface beyond the user[C]// Proceedings of International Conference on Intelligent User Interfaces, Orlando, USA; ACM, 1997:261-264.
- [4] Ingar Mæhlum Arntzen. A programmable structure for pervasive computing[C]// Proceedings of the IEEE/ACS International Conference on Pervasive Services, San Diego; IEEE, 2004:29-38.

作者简介:

李明女,(1973-),博士研究生,讲师。研究方向为移动计算、上下文感知。

(上接第 169 页)

像素和部分剪切边界像素所造成的另一个非剪切像素;如反过来,先像素值加密后像素位置变换,则不能得到正确恢复的像素可认为是剪切像素的两倍,图像恢复质量将很差。这是应用文中算法要注意的关键问题。

6 结束语

文中算法有如下特点:(1) 采用以块为单位的类似 CBC 模式加密图像像素,并可随机改变每一块图像的加密初始值,使算法安全性大为提高;(2) 在像素置乱均布和像素值均布两大前提基础上,提出了基于邻域相邻像素特性的加密图像抗剪切攻击恢复算法,并有效实现。

基于邻域相邻像素特性的解密图像的抗剪切恢复算法,随着被剪切面积的增加,被剪切像素点的还原准确性逐渐下降,需进一步改进。

参考文献:

- [1] 李太勇,贾华丁,吴江. 基于三维混沌序列的数字图像加密算法[J]. 计算机应用,2006,26(7):1652-1654.
- [2] 成亚萍,吕巍,张太忠. 一种新的抗剪切的数字图像加密算法[J]. 计算机工程与应用,2008,44(27):130-131.
- [3] 张雪锋,范九伦,康宝生. 一种抗剪切变换攻击的数字图像加密算法[J]. 系统仿真学报,2006,18(8):2260-2263.
- [4] 李鹏,田东平. 基于超混沌序列的数字图像加密算法[J]. 微电子学与计算机,2008,25(3):4-7.
- [5] 谢颢,范九伦. 一种基于位运算的数字图像加密算法[J]. 微电子学与计算机,2009,26(12):117-119.
- [6] 罗军. 基于混沌系统的数字图像加密算法[J]. 计算机工程与设计,2009,30(8):1844-1845.

作者简介:

廖琪男男,(1964-),研究生,高级工程师。研究方向为数字图像处理、数字图像加密、数字图像信息隐藏和数字水印。