

二维随机矩阵置乱变换的周期及在 图像信息隐藏中的应用

王泽辉

(中山大学科学计算与计算机应用系 广州 510275)

摘 要 给出了二维随机整数矩阵 \mathbf{A} 决定的置乱变换在任意模 N 下周期 $T(\mathbf{A}, N)$ 的精确表达式及上界估计. 提出了高效算法, 只需 $O((\log_2 N)^2)$ 次模 N 乘法便可得到 $T(\mathbf{A}, N)$, 算法可应用于图像信息隐藏. 采取位置空间与色彩空间的多轮乘积型置乱变换, 可达到高维矩阵置乱的效果. 利用 \mathbf{A} 的随机性、长周期和概率密钥, 建立一个概率密码体制, 可有效防止选择明文攻击, 增强信息隐藏的安全性.

关键词 数字图像; 置乱变换; 周期性; 多项式时间; 选择明文攻击; 安全性

中图法分类号 TP391

On the Period of 2D Random Matrix Scrambling Transformation and Its Applications in Image Information Hiding

WANG Ze-Hui

(Department of Scientific Computation and Computer Applications, Sun Yat-Sen University, Guangzhou 510275)

Abstract This paper provides an precise expression for the period $T(\mathbf{A}, N)$ under a 2-D random integer matrix scrambling transformation modulus N for any N , and provides the estimation of the upper bound of the period $T(\mathbf{A}, N)$. A high efficient algorithm is also presented, which only takes $O((\log_2 N)^2)$ times multiplications modulus N for determining the period $T(\mathbf{A}, N)$. This algorithm can be used in image information hiding. By means of the position space and color space, the 2-D integer matrix multiplicative scrambling transformation can attain the effect as the same as the higher dimensions matrix scrambling transformation. By randomness of the integer matrix \mathbf{A} , its longer period and the probabilistic key, a new probabilistic cryptosystem is constructed, and it can be effectively against chosen plaintext attack and strengthen the security of information hiding.

Keywords digital image; scrambling transformation; periodicity; polynomial time; chosen plaintext attack; security

1 引 言

保护数字图形图像的安全已成为普遍关心的问题. 包括数字图像置乱在内的信息隐藏作为一项重要技术已被广泛地研究^[1]. 基于数字图像的基本表现

形式是矩阵. 置乱技术借助变换 $\mathbf{X}' = \mathbf{A}\mathbf{X} \pmod{N}$ (\mathbf{X} 为相空间坐标向量, 矩阵同余规定为对应元素同余), 改变图像灰度值或颜色值的布局, 达到信息隐藏的目的. 求出变换的精确周期 T 是十分重要的基础问题. 对一幅连续变换 k 次的图像, 解密时光靠肉眼观察还不行. 看似混沌的图像也许正是所需的太

空星云图而非密图,一切靠周期 T ,再变换 $T-k$ 次才能恢复原始图像. 周期的重要性正如 RSA、ECC 算法,能确定周期才能构造公钥/私钥对,进行文本加密. 仅能求周期还不够现代密码学要求:对于输入长度求周期算法必须是多项式时间而破译攻击要花指数时间去猜周期.

文献[2~4]挖掘了 Arnold 变换并进行推广,在图像信息隐藏和图像置乱技术方面作了大量的基础性研究,取得了良好的效果. 国内外也有不少文献不同程度地涉及到这个问题,在 \mathbf{A} 、 N 选特殊值情况下导出周期 T 的求解及应用,文献[5~7]有了比较好的结果,对于相对有序的一类矩阵(如 T 矩阵)得到了变换的周期. 但似乎未见最一般的结果:对矩阵 \mathbf{A} 元素值任意、模数 N 任意时的周期表达式,用 $O((\log_2 N)^2)$ 次模 N 乘法时间求出其周期.

不同于 RSA 的标量求周期,求一般矩阵变换周期困难较大:矩阵变换 $\mathbf{A}^k \mathbf{X}$ 对图形象素坐标的效果相当于伸缩、切割和拼接. Arnold 变换的周期有中间结果是因为 Arnold 矩阵是伸缩因子为 1 的仿射变换矩阵,当 \mathbf{A} 元素任意时伸缩因子剧烈变化, \mathbf{A} 的行列式相当于面积的伸缩比,Arnold 变换刚好为 1,当 \mathbf{A} 、 N 任意时面积的升缩比剧烈变化;而 N 越大对像素的切割、拼接复杂度越大,这就是把 Arnold 变换推广到一般变换求周期的困难所在.

本文提出确定性算法 T_{2D} :随机输入二维整数矩阵的元素值及随机的模数 N ,输出精确周期 $T(\mathbf{A}, N)$,并可证明算法的时间复杂度仅为 $O(\lceil \log_2 N \rceil^2)$,属于多项式时间算法. 应用于不同的 N 阶数字图像隐藏,以概率密钥决定如何在三原色中选二,通过生成长周期二维随机矩阵进行位置空间与色彩空间的 ω 轮乘积型置乱变换,达到高维矩阵置乱的效果,并抵御选择明文攻击等破译算法. 加密与解密主变换 $\mathbf{A}^J \pmod N$, $\mathbf{A}^{T-J} \pmod N$ 所需模 N 乘法次数仅为 $O(\lceil \log_2 N \rceil)$ (作 ω 轮置乱的时间仅为 ω 倍). 强力破译被隐藏数字图像先要猜中随机矩阵的 $O(N^4)$ 个元素,还至少需要 $O(N) = O(2^{\lceil \log_2 N \rceil})$ 的时间猜中周期,需在 6^ω 个中选 1 个概率密钥,随着 N , ω 的加大破译计算量呈指数级增长. 后给出各类 N 值下 $T(\mathbf{A}, N)$ 的上界估计,以方便长周期矩阵的选择.

以往 Arnold 型变换多作为水印等隐藏技术的预处理,本文的结果发现,随机矩阵置乱变换本身可发展成一种密码体制,用于加密重要手稿、图形图像、多媒体(文本图表作为印刷体也是图像的特例),

在数字隐写、数字指纹找到广泛的应用. 大量的数值实验与图像隐藏实验结果表明与理论吻合.

2 数字图像的多轮乘积型置乱

数字图像的基本表现形式是矩阵,使得以矩阵运算为基础的 MATLAB 几乎可处理现行的各种格式存放的数字图像, MATLAB 的图形处理工具箱支持的图像分为索引图像、灰度图像、二值图像和 RGB 图像 4 种类型,由于 RGB 图像是真彩色图像且 MATLAB 提供了其余类型与 RGB 图像之间的相互转化函数,因此解决了 RGB 图像的信息隐藏问题也就解决了其它类型数字图像以至各种格式数字图像文件的信息隐藏问题.

下文中 \mathbb{Z} , \mathbb{Z}^+ 分别为整数集与自然数集, gcd 、 lcm 分别为最大公约数与最小公倍数记号,整数 $N \in \mathbb{Z}^+$, $\mathbb{Z}_N = \{0, 1, \dots, N-1\}$, $\pmod N$ 表示代数运算及矩阵运算结果都在 \mathbb{Z}_N 取值. $^{\wedge}$ 表示幂运算, $a^{\wedge} b = a^b$, $ord_p(b)$ 表示 b 模 p 之阶,即使 $b' \equiv 1 \pmod p$ 之最小正整数. $\det(\mathbf{A})$ 为矩阵 \mathbf{A} 的行列式, \mathbf{I}_m 为 m 维单位矩阵.

任何一幅 N 阶 RGB 数字图像 P 均可由矩阵 $(\sigma_r(x, y), \sigma_g(x, y), \sigma_b(x, y))_{N \times N}$ 完全决定,其中 $\sigma_r(x, y)$, $\sigma_g(x, y)$, $\sigma_b(x, y)$ 分别代表第 x 行第 y 列像素的红、绿、蓝颜色值, $x, y \in \mathbb{Z}_N$, 色彩空间记为 U , P 对应于 U 上一个 $N \times N \times 3$ 矩阵,可简记为

$$P := (\sigma_r(x, y), \sigma_g(x, y), \sigma_b(x, y))_{N \times N} \in U^{N \times N \times 3} \quad (1)$$

定义 1. 称变换 $\Lambda: U^{N \times N \times 3} \rightarrow U^{N \times N \times 3}$ 为一幅数字图像 P 的二维随机矩阵 \mathbf{A} 任意模 N 的位置空间置乱变换,对式(1)表示的 P ,

$$\Lambda \circ P = (\sigma_r(x', y'), \sigma_g(x', y'), \sigma_b(x', y'))_{N \times N},$$

其中 $\mathbf{A} = (a_{i,j}) \in \mathbb{Z}_N^{2 \times 2}$,

$$(x', y')^T = \mathbf{A}(x, y)^T \pmod N \quad (2)$$

引理 1. 形如式(2)的变换有周期 $T(\mathbf{A}, N)$ (所谓周期是指使 P 经一系列变换后恢复为 P 的最小次数),当且仅当

$$gcd(\det(\mathbf{A}), N) = 1 \quad (3)$$

证明见文献[3]. 变换(2)的参数 $a_{i,j}$ 可随机选择,只要式(3)成立,易知当 $\det(\mathbf{A}) = 1$ 时变换(2)对任意 N 均有周期. 这样与以往结果相比增加了充分大的密钥空间. 例如,当 $N = 2^{16} = 65536$ 时,取 $a_{1,1}$, $a_{2,2}$ 为 $0 \sim 65535$ 之间的偶数,取 $a_{1,2}$, $a_{2,1}$ 为 $1 \sim 65535$ 之间的奇数,或倒过来,则条件(3)必满足,考

考虑到对称矩阵情况,共有 $2 \times 32768^4 \div 2 = 2^{60}$ 种选择。 $T(\mathbf{A}, N)$ 在不引起混淆时简记为 $T(N)$ 。

为了防止仅作空间置乱轮廓被猜,体现仙农的混淆与扩散原则,再引入色彩空间的置乱。

定义 2. 设色彩空间 U 数字化表示后值域是 \mathbb{Z}_M , 固定 (x, y) , 概率密钥 θ 在 $\sigma_r(x, y), \sigma_g(x, y), \sigma_b(x, y)$ 中随机挑选两个不同颜色值记为 $\sigma_1(x, y), \sigma_2(x, y)$ 作置乱, 剩下颜色值记为 $\sigma_3(x, y)$ 不作置乱, $\theta = 1, 2, 3, 4, 5, 6$ 分别代表 $(\sigma_1, \sigma_2) = (\sigma_r, \sigma_g), (\sigma_r, \sigma_b), (\sigma_g, \sigma_r), (\sigma_g, \sigma_b), (\sigma_b, \sigma_r), (\sigma_b, \sigma_g)$. 称变换 $\Gamma: U^{N \times N \times 3} \rightarrow U^{N \times N \times 3}$ 为数字图像在任意模数 M 下二维随机矩阵 \mathbf{F} 的色彩空间置乱变换, $\mathbf{F} = (f_{i,j}) \in \mathbb{Z}_M^{2 \times 2}$, 对 $P := (\sigma_1(x, y), \sigma_2(x, y), \sigma_3(x, y))$,

$$\Gamma \circ P := (\sigma'_1(x, y), \sigma'_2(x, y), \sigma_3(x, y)), \\ (\sigma'_1(x, y), \sigma'_2(x, y))^T =$$

$$F(\sigma_1(x, y), \sigma_2(x, y))^T \pmod{M} \quad (4)$$

我们把式(2),(4)推广为一般的矩阵置乱变换

$$\mathbf{X}' = \mathbf{A}\mathbf{X} \pmod{N} \quad (5)$$

其中 $\mathbf{A} \in \mathbb{Z}_N^{m \times m}$, \mathbf{X}, \mathbf{X}' 是数字图像的 m 维相空间坐标向量及其变换后向量。

推论 1. 变换(5)的周期 $T(\mathbf{A}, N)$ 即是使式(6)成立的最小正整数。

$$\mathbf{A}' \equiv \mathbf{I}_m \pmod{N} \quad (6)$$

后面我们得到求 $T(\mathbf{A}, N)$ 的一般框架, 并对 $m=2$ 描述精确地求出 $T(\mathbf{A}, N)$ 的算法 T_{2D} , 以此为基础, 随机选择 $0 < h < T(\mathbf{A}, N), 0 < k < T(\mathbf{F}, M)$, 可对 P 进行位置-色彩空间置乱变换 $\Gamma^k \circ \Delta^h \circ P$, 把 P 隐藏成 P' , 恢复图像只需作变换 $\Delta^{T(\mathbf{A}, N)-h} \circ \Gamma^{T(\mathbf{F}, M)-k} \circ P'$. 主要变换需作形如 $\mathbf{A}^J \pmod{N}$ 的计算, 后面将给出快速计算算法。

图像隐藏方案. 选择概率密钥 $\Theta = (\theta_1, \theta_2, \dots, \theta_w)$ 控制 w 轮色彩置乱的红蓝绿选择, 每个 θ_i 在 $1 \sim 6$ 之间随机选择, 进行如下 w 轮乘积型置乱:

位置空间置乱₁ \rightarrow 色彩空间置乱₁ \rightarrow 位置空间置乱₂ $\rightarrow \dots \rightarrow$ 位置空间置乱_w \rightarrow 色彩空间置乱_w.

保密概率密钥、 $2w$ 个变换固定密钥, 传输密文。

图像恢复方案. 根据概率密钥及固定密钥, 按置乱逆过程进行 w 轮恢复变换, 得到明文图像。

加强方案. 增加变换域(如小波变换域)上的置乱和系数恢复, 类似于上面操作。

虽然每次色彩空间置乱只选两种基本颜色, 但多次置乱后三种基本颜色都会被挑选多次, 经过位置与色彩的混合置乱可达到高维矩阵置乱的效果。 w 轮混合置乱进行图像隐藏的主变换是 $2w$ 个形如

$\mathbf{A}^J \pmod{N}$ 的计算, 其计算量是累加的, 但矩阵随机生成使得对图像隐藏的攻击(破译)无法采取偶然碰撞的方法, 必须每次都猜对才能恢复图像, 故破译的计算量是累乘的, 随着 N, w 的增大计算量会呈指数级增长。概率密钥的引入可成功抗击选择明文攻击, 其它类型可转成 RGB 图像, 用本法也可用其它概率密钥办法(见第 5 节)实现。

3 确定精确周期算法及时间复杂性分析

下面对一般矩阵 $\mathbf{A} \in \mathbb{Z}_N^{m \times m}$ 求变换(5)的周期 $T(\mathbf{A}, N)$ 。

引理 2. 设 $N = n_1 n_2, \gcd(n_1, n_2) = 1, \gcd(\det(\mathbf{A}), N) = 1$, 则

$$T(\mathbf{A}, N) = \text{lcm}(T(\mathbf{A}, n_1), T(\mathbf{A}, n_2)) \quad (7)$$

引理 3. 设 $N = p^r$, p 为素数, r 为正整数, $\gcd(\det(\mathbf{A}), N) = 1$, 则 $\exists u \in \mathbb{Z}$, 使得

$$T(\mathbf{A}, p^r) = p^u \times T(\mathbf{A}, p) \quad (8)$$

引理 2, 3 的证明主要利用推论 1、二项式定理和数论整除、 lcm 概念, 因篇幅所限略去。下记 $T(\mathbf{A}, p)$ 为 $T(p)$ 。

定理 1. 设 N 有标准因子分解式

$$N = (p_1)^{r_1} (p_2)^{r_2} \cdots (p_s)^{r_s} \quad (9)$$

其中 p_1, p_2, \dots, p_s 为互不相同的素数, r_1, r_2, \dots, r_s 为自然数, $\gcd(\det(\mathbf{A}), N) = 1$, 则变换(5)的周期 $T(\mathbf{A}, N) =$

$$\min\{(p_1^{y_1} p_2^{y_2} \cdots p_s^{y_s}) \mid 0 \leq y_i \leq r_i - 1, \\ y_i \in \mathbb{Z}, i = 1, 2, \dots, s, \mathbf{A}^{\mathbf{Q}l} \equiv \mathbf{I}_m \pmod{N}, \\ l = \text{lcm}(T(p_1), \dots, T(p_s)), \\ \mathbf{Q} = (p_1^{y_1} p_2^{y_2} \cdots p_s^{y_s})\} \quad (10)$$

证明。由引理 2, 3 马上可得

$$T(\mathbf{A}, N) =$$

$$\text{lcm}(p_1^{u_1} \times T(p_1), p_2^{u_2} \times T(p_2), \dots, p_s^{u_s} \times T(p_s)) = \\ (p_1^{u_1} p_2^{u_2} \cdots p_s^{u_s}) l, u_i \in \mathbb{Z}, 0 \leq u_i \leq r_i - 1,$$

由推论 1 的最小值规定可得式(10)。证毕。

推论 2. 设 N 没有重素因子, 则变换(5)的周期为

$$T(\mathbf{A}, N) = l = \text{lcm}(T(p_1), T(p_2), \dots, T(p_s)).$$

定理 1 对任意 m 维矩阵 \mathbf{A} 成立。以下对 $m=2$ 维求出 $T(p_i)$ 的表达式, 从而求得 $T(\mathbf{A}, N)$ 的精确表达式。

命题 1. 当 $p=2$ 时, 使变换(5)有周期的矩阵 \mathbf{A} 分别是

$$\mathbf{A} = \begin{pmatrix} 10 \\ 01 \end{pmatrix}, \begin{pmatrix} 11 \\ 01 \end{pmatrix}, \begin{pmatrix} 10 \\ 11 \end{pmatrix}, \begin{pmatrix} 01 \\ 10 \end{pmatrix}, \begin{pmatrix} 11 \\ 10 \end{pmatrix}, \begin{pmatrix} 01 \\ 11 \end{pmatrix} \pmod{2},$$

其周期分别是 $T(\mathbf{A}, 2) = 1, 2, 2, 2, 3, 3$, 并满足

$$T(\mathbf{A}, p) \leq p^2 - 1, \quad p = 2 \quad (11)$$

设 p 为 p_1, p_2, \dots, p_s 中任一奇素数, $F_p = \mathbb{Z}/(p) = \{0, 1, \dots, p-1\}$ 表示元素个数为 p 的有限域, $F_p[x]$ 为系数在 F_p 的多项式环. $\forall f(x) \in F_p[x] \subset \mathbb{Z}[x]$, 因运算 $f(x)$ 系数可能表现为整数, 相当于 $f(x) \in \mathbb{Z}[x]$.

定义 2.

(1) $f_1(x), f_2(x) \in \mathbb{Z}[x]$, 设 $f_1(x) = x^k + a_1 x^{k-1} + \dots + a_k$, $f_2(x) = x^k + c_1 x^{k-1} + \dots + c_k$, 如 $a_i \equiv c_i \pmod{p}, i = 1, 2, \dots, k$, 则记 $f_1(x) \equiv f_2(x) \pmod{p}$, 简记为 $f_1(x) \equiv f_2(x)$, 并称“在 $F_p[x]$ 中 $f_1(x) = f_2(x)$ ”.

(2) 对 $h(x), f(x) \in F_p[x]$, 如 $\exists g(x) \in F_p[x]$ 使 $h(x) \equiv g(x)f(x)$ 成立, 则称“在 $F_p[x]$ 中 $f(x)$ 整除 $h(x)$ ”, 简记为 $f(x) | h(x)$.

令 \mathbf{A} 的元素为 $a_{11}, a_{12}, a_{21}, a_{22}$ 可随机取, $f_2(x) = (x-e)^2 - c, c = (2^{-1} \pmod{p}) \times (a_{11} - a_{22})^2 + a_{12} \times a_{21}, e = 2^{-1} \pmod{p} \times (a_{11} + a_{22})$, 考虑下列同余方程之解:

$$(\mathbf{X} - e\mathbf{I})^2 \equiv c\mathbf{I} \pmod{p}, \quad \mathbf{X} \in \mathbb{Z}^{2 \times 2} \quad (12)$$

$$(x-e)^2 \equiv c \pmod{p}, \quad x \in \mathbb{Z}_p \quad (13)$$

根据初等数论二次剩余理论^[8]有下面引理.

引理 4. 对任意奇素数 p 成立

(i) 式(12)在 $\mathbb{Z}^{2 \times 2}$ 中有一个解 $\mathbf{A} = (a_{ij})_{2 \times 2}$, 即

$$f_2(\mathbf{A}) \equiv O \pmod{p} \quad (14)$$

(ii) 当 $c \equiv 0 \pmod{p}$ 时, 式(13)在 \mathbb{Z}_p 有 2 重根 e , 即 $f_2(x) \equiv (x-e)^2$.

(iii) 当 $c^{\wedge}((p-1)/2) \equiv 1 \pmod{p}$ 时, 式(13)在 \mathbb{Z}_p 中有两相异之根 x_1, x_2 .

(iv) 当 $c^{\wedge}((p-1)/2) \equiv -1 \pmod{p}$ 时, 式(13)在 \mathbb{Z}_p 无解, $f_2(x)$ 为 $F_p[x]$ 中不可约多项式.

定理 2. 设 $\gcd(\det(\mathbf{A}), N) = 1$, 对任意奇素数 p 有

(i) 当 $c \equiv 0 \pmod{p}$ 时, 设 e 为式(13)的 2 重根, 则

$$T(p) = \min\{d: \mathbf{A}^d \equiv \mathbf{I} \pmod{p}, d | p \times \text{ord}_p(e)\} \quad (15)$$

(ii) 当 $c^{\wedge}((p-1)/2) \equiv 1 \pmod{p}$ 时, x_1, x_2 为式(13)的两个相异根, 则

$$T(p) = \min\{d: \mathbf{A}^d \equiv \mathbf{I} \pmod{p}, d | \text{lcm}(\text{ord}_p(x_1), \text{ord}_p(x_2))\} \quad (16)$$

(iii) 当 $c^{\wedge}((p-1)/2) \equiv -1 \pmod{p}$ 时,

$$T(p) = \min\{d: \mathbf{A}^d \equiv \mathbf{I} \pmod{p}, d | (p+1) \times \text{ord}_p(\det(\mathbf{A}))\} \quad (17)$$

证明.

(i) 由引理 4, 式(13)在 \mathbb{Z}_p 有 2 重根 e , 记 $d = \text{ord}_p(e)$, 所以 $e^d \equiv 1 \pmod{p}$, 对 $x^d - 1 \equiv (x-e)^d \pmod{p}$ 因式分解得

$$x^d - 1 \equiv h_1(x)(x-e) \pmod{p} \quad (18)$$

所以 $(x^d - 1)^p \equiv h_2(x)(x-e)^p \pmod{p}$, $h_1(x), h_2(x) \in F_p[x]$. 又 $f_2(x) \equiv (x-e)^2$, 由式(14) $f_2(\mathbf{A}) \equiv (\mathbf{A} - e\mathbf{I})^2 \equiv O$, 所以 $(\mathbf{A}^d - \mathbf{I})^p \equiv h_2(\mathbf{A})(\mathbf{A} - e\mathbf{I})^p \equiv O$, 令 $\mathbf{B} = \mathbf{A}^d - \mathbf{I}$, 利用 C_p^i 性质易得 $\mathbf{A}^{dp} \equiv (\mathbf{B} + \mathbf{I})^p \equiv \mathbf{B}^p + \mathbf{I} \equiv (\mathbf{A}^d - \mathbf{I})^d + \mathbf{I} \equiv \mathbf{I} \pmod{p}$, 所以 $T(p) | dp$, 或式(15)成立.

(ii) 由引理 4, 式(13)在 \mathbb{Z}_p 有相异根 x_1, x_2 , 记 $d_i = \text{ord}_p(x_i)$, 类似式(18), $\exists h_i(x) \in F_p[x]$ 使 $x^{d_i} - 1 \equiv h_i(x)(x-x_i) \pmod{p}, i = 1, 2$. 所以 $(x-x_i) | (x^{d_i} - 1), i = 1, 2$. 所以 $(x-x_1)(x-x_2) | (x^d - 1), d = \text{lcm}(d_1, d_2)$.

即 $\exists g(x) \in F_p[x]$, 使 $(x^d - 1) \equiv g(x)f_2(x) \pmod{p}$, 所以 $\mathbf{A}^d - \mathbf{I} \equiv g(\mathbf{A})f_2(\mathbf{A}) \equiv O, \mathbf{A}^d \equiv \mathbf{I}, T(p) | d$, 即式(16)成立, 结合有限域的简单结论^[9], (iii)的证明类似于(i)、(ii)证明, 不再赘述. 证毕.

定理 1 与命题 1、定理 2 构成了对一般周期 $T(\mathbf{A}, N)$ 的精确表达式, 借助一个循环语句作有限次判断, 便可得到周期. 构造算法 T_{2D} 只需定理 2 的结论, 理论上更有仔细的分析.

推论 3. 设 $\gcd(\det(\mathbf{A}), N) = 1, m = 2$, 则对任意奇素数 p 可得

(i) 当 $c \equiv 0 \pmod{p}$ 时, 如果 $\mathbf{A}^v \equiv \mathbf{I} \pmod{p}$ 不成立 ($v = p, p-1$), 则

$$T(p) = \min\{pd: \mathbf{A}^{pd} \equiv \mathbf{I} \pmod{p}, d | \text{ord}_p(e)\}.$$

(ii) 当 $c^{\wedge}((p-1)/2) \equiv 1 \pmod{p}$ 时, 如式(5)排除了像 $\mathbf{A} = k\mathbf{I}, k$ 为整数这种简单情况, 则

$$T(p) = \text{lcm}(\text{ord}_p(x_1), \text{ord}_p(x_2)).$$

(iii) 当 $c^{\wedge}((p-1)/2) \equiv -1 \pmod{p}$ 时, 对满足 $\det(\mathbf{A}) = 1$ 的变换, 如果 $p+1 = 2q, q$ 为素数, 则 $T(p)$ 为 $2q$ 或 q .

证明主要利用了有限域及素数的性质, 略.

推论 4. 对任意素数 p 存在 $T^*(p)$ 使 $T(p) | T^*(p), T(p) \leq T^*(p) \leq p^2$, 且对任意奇素数 $2 | T^*(p)$.

证明主要利用定理 2、素数及 lcm 性质, 略.

定理 3. 对于所有形如式(5)且 $m = 2$ 的变换, 当条件(3)成立时其周期有如下估计

$$T(\mathbf{A}, N) \leq N^2 \quad (19)$$

证明. 由定理 1 及式(10),

$$l = \text{lcm}(T(p_1), T(p_2), \dots, T(p_s)), \\ T(\mathbf{A}, N) \leq (p_1^{r_1} (r_1 - 1)) (p_2^{r_2} (r_2 - 1)) \dots \\ (p_s^{r_s} (r_s - 1)) \times l,$$

由式(9), $T(\mathbf{A}, N) \leq N / (p_1 p_2 \dots p_s) l$, 再由推论 4,

$$l \leq T(p_1) T(p_2) \dots T(p_s) \leq p_1^2 p_2^2 \dots p_s^2,$$

所以 $T(\mathbf{A}, N) \leq N / (p_1 p_2 \dots p_s) \times p_1^2 p_2^2 \dots p_s^2 = N p_1 p_2 \dots p_s \leq N^2$. 证毕.

算法 T_{2D} 输入: 随机正整数 $N, a_{i,j} (i, j = 1, 2)$; 构成变换(5), 当式(3)不成立时重选 $a_{i,j}$;

输出: 变换(5)的周期 $T(\mathbf{A}, N)$.

算法 T_{2D} 依据上述结论确定 $T(\mathbf{A}, N)$, 其主要计算形如 $\mathbf{A}^L \pmod{N}$, 把 L 化为 2 进制数 $L = (L_s \dots L_1 L_0)$, $s+1$ 为 L 的比特数, $s = \lfloor \log_2 L \rfloor$. 求 $\mathbf{A}^L \pmod{N}$ 有下列的高效算法.

算法 1.

$G \leftarrow \mathbf{A}$, if $L_0 = 0$ then $\mathbf{A}_2 \leftarrow \mathbf{I}$ else $\mathbf{A}_2 \leftarrow \mathbf{A}$

for $j \leftarrow 1$ to s do

$\{G \leftarrow G \times G \pmod{N}$

if $L_j = 1$ then $\mathbf{A}_2 \leftarrow \mathbf{A}_2 \times G \pmod{N}\}$

参考文献[10]的相应分析, 上述程序至多作 $16 \times s = 16 \lfloor \log_2 L \rfloor$ 次模 N 乘法, 便得到 $\mathbf{A}^L \pmod{N}$, 由定理 3 得 $\lfloor \log_2 L \rfloor = O(\log_2 N)$. 对于固定的 N , 矩阵 \mathbf{A} 的元素有 $O(N^4)$ 种选择, 因此事先对一序列的 N 先作素因子分解(9)是经济的, 算法 T_{2D} 只需查表便得到 $p_i, r_i, i = 1, 2, \dots, s$. MATLAB 有作因子分解的内部函数, 较快速, 在此基础上求 lcm 的时间更短, 细致分析两者时间复杂度至多为 $O(\log_2 N)$.

引理 5. 设 n 代表上述的 N 或任意一个奇素数, 正整数 f 有标准分解

$$f = (q_1)^{v_1} (q_2)^{v_2} \dots (q_w)^{v_w}.$$

其中 q_1, q_2, \dots, q_w 为互不相同的素数, v_1, v_2, \dots, v_w 为自然数.

(i) 如果 f 有上界估计: $f \leq F_1$, 则求 $h_1 = \min\{d: \mathbf{A}^d \equiv \mathbf{I} \pmod{n}, d | f\}$ 相当于求

$$h_1 = \min\{(q_1^{y_1} | q_2^{y_2} | \dots | q_w^{y_w}) | \mathbf{A}^Q \equiv \mathbf{I} \pmod{n},$$

$$Q = (q_1^{y_1} | q_2^{y_2} | \dots | q_w^{y_w}),$$

$$0 \leq y_i \leq v_i, i = 1, 2, \dots, w\},$$

只需不超过 $32 \log_2 F_1 \times \lfloor \log_2 n \rfloor$ 次模 n 乘法, 便得 h_1 .

(ii) 如存在正整数 l 使 f 有上界估计: $fl \leq F_2$, 则精确求

$$h_2 = \min\{(q_1^{y_1} | \dots | q_w^{y_w}) l | \mathbf{A}^Q \equiv \mathbf{I} \pmod{n},$$

$Q = (q_1^{y_1} | \dots | q_w^{y_w}), 0 \leq y_i \leq v_i - 1, i = 1, 2, \dots, w\}$, 只需不超过 $16 \log_2 F_2 \times \lfloor \log_2 n \rfloor$ 次模 n 乘法.

证明. 确定 h_1 至多要作 $v_1 + v_2 + \dots + v_w + w$ 次形如 $\mathbf{A}^L \pmod{N}$ 的计算, $f = (q_1)^{v_1} \dots (q_w)^{v_w} (q_w) \geq 2^{v_1} \dots 2^{v_w} = 2^{v_1 + \dots + v_w}$, $v_1 + \dots + v_w + w \leq 2 \log_2 f \leq 2 \log_2 F_2$, 只需不超过 $32 \log_2 F_1 \times \lfloor \log_2 n \rfloor$ 次模 n 乘法, 便得 h_1 , 类似易证(ii). 证毕.

推论 5. 对任意奇素数 p , 求 $T(p)$ 至多要作 $64 \log_2 p \times \lfloor \log_2 p \rfloor$ 次模 p 乘法.

定理 4. 对于形如式(5)的二维随机矩阵任意模数 N 下的置乱变换, 存在一个确定的算法 T_{2D} , 只需不超过 $96 \lceil \log_2 N \rceil^2 + O(\log_2 N)$ 次模 N 乘法便可确定式(5)的精确周期 $T(\mathbf{A}, N)$.

证明. 由推论 5, 对所有的 $i = 1, 2, \dots, s$, 求 $T(p_i)$ 至多要做 $64 \log_2 p_i \times \lfloor \log_2 p_i \rfloor$ 次模 p_i 乘法 ($p_i = 2$ 时间更短), 不超过 $64 \log_2 p_i \times \lfloor \log_2 N \rfloor$ 次模 N 乘法, 全部 s 个共需要的模 N 乘法次数不高于

$$64 (\log_2 p_1 + \dots + \log_2 p_s) \lfloor \log_2 N \rfloor \leq$$

$$64 \log_2 N \lfloor \log_2 N \rfloor \leq 64 \lceil \log_2 N \rceil^2,$$

便可得到 $l = \text{lcm}(T(p_1), T(p_2), \dots, T(p_s))$, 由定理 3 及引理 5 之(ii), 令 $F_2 = N^2$, 求式(9)的 $T(\mathbf{A}, N)$ 只需要不超过 $16 \log_2 N^2 \times \lfloor \log_2 N \rfloor \leq 32 \lceil \log_2 N \rceil^2$ 次模 N 乘法, 加上对 N 作标准分解及求 lcm 时间 $O(\log_2 N)$ 次模 N 乘法, 故精确求 $T(\mathbf{A}, N)$ 只需要不超过 $96 \lceil \log_2 N \rceil^2 + O(\log_2 N)$ 次模 N 乘法. 证毕.

4 周期的上界估计及图像实验例子

定理 5. 在定理 1 的假定下 ($m = 2$), 变换(6) 有更精确上界估计 (s 为 N 的素数因子个数).

(i) 当 N 为奇数时

$$T(\mathbf{A}, N) \leq N^2 / 2^{s-1} \quad (20)$$

当 N 为偶数时

$$T(\mathbf{A}, N) \leq 3/4 \times 1/2^{\max\{s-2, 0\}} \times N^2 \leq 3/4 N^2 \quad (21)$$

(ii) 对满足 $\det(\mathbf{A}) = 1$ 的变换, 当对所有素因子 p 式 $a_{11} + a_{22} \equiv \pm 2 \pmod{p}$ 均不成立时: 如 N 为奇数则 $T(\mathbf{A}, N) \leq 2N$, 如 N 为偶数则 $T(\mathbf{A}, N) \leq 3N$.

证明主要利用初等数论结果, 略.

例 1. $\det(\mathbf{A}) = 1$ 时变换(5)的周期. 例子表明算法适合任意大整数 N , 也验证了定理 5 的估计. 随机选择 $a_{11} = 31, a_{12} = 137, a_{21} = 2003, a_{22} = 8852$, 则 $\det(\mathbf{A}) = 1$, 简记 $T(\mathbf{A}, N) = T(N)$, 调用算法 T_{2D} 求得

$T(12345678) = 14592$; $T(23456789) = 23456790$;
 $T(34567890) = 1246560$; $T(45678901) = 45678902$;
 $T(56789012) = 12169068$; $T(67890123) = 1436824$;
 $T(78901234) = 59389140$; $T(89012345) = 250740$.

例 2. $\det(\mathbf{A}) \neq 1$ 时变换(5)的周期. 例子表明算法适合伸缩比 $\neq 1$ 这些难度大的变换, 同时选择素数幂 p^k , 其结果验证了定理 1. 随机选择 $a_{11} = 2005$, $a_{12} = 3006$, $a_{21} = 45678$, $a_{22} = 68483$, 调用算法 T_{2D} 求得

$$T(7^3) = 294; T(7^4) = 2058;$$

$$T(17^3) = 4624; T(17^4) = 78608;$$

$$T(37^3) = 49284; T(37^4) = 1823508;$$

$$T(47^3) = 101614; T(47^4) = 4775858.$$

例 3. 图像的隐藏. 附图 ylk0.jpg 是军车的图片, 采用 1 轮位置-色彩空间的乘积型置乱得到隐藏图像 ylk1.jpg, 2 轮乘积型置乱得到 ylk2.jpg, 解密时先解第 2 轮置乱得到 ylk3.jpg, 再解第 1 轮置乱得到 ylk4.jpg, 即恢复了原始图像.

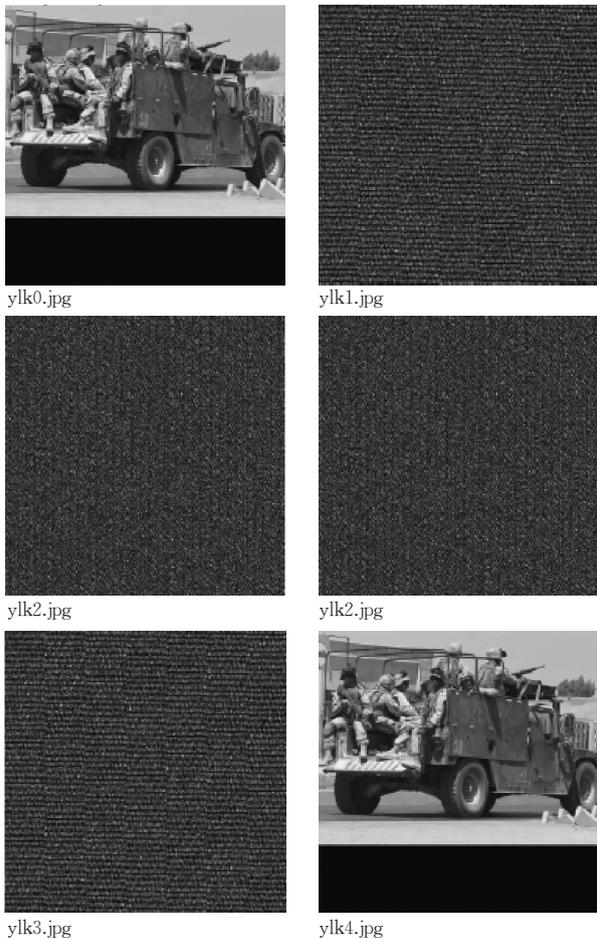


图 1 例子 3 插图

例 4. 随机图像——学生宿舍外墙的隐藏. 附图 wall0.jpg 是作者随机用数码相机拍的一张中山

大学学生宿舍外墙的 jpg 相片, 马上用算法 T_{2D} 作 3 轮隐藏成 wall1.jpg, wall2.jpg, wall3.jpg, 恢复隐藏逐次为 wall4.jpg, wall5.jpg, wall6.jpg, 则 wall6.jpg 是恢复的原始相片(因篇幅所限略).

例 5. 上述结果结合 LSB 等技术, 对图 ylk0.jpg 进行数字隐写变成图 ylk0st.jpg 及提取的隐写信息图 ylk0a.jpg, 限于篇幅略去.

5 针对矩阵置乱的攻击及新算法的有效防范

矩阵置换算法推出后若干文献研究了对它的各种攻击算法, 文献列出大致有如下几种:

(i) 猜测轮廓攻击. 早期技术只做空间位置的置乱, 由于颜色的连续易给人猜出轮廓.

(ii) 对短周期的攻击. 采用纯粹 Arnold 变换, 对特殊的 $N(2$ 的幂) 周期太短, 可以快速攻击.

(iii) 反变换攻击. 由于传统的 Arnold 型置乱信息隐藏, 要连续作 J 次变换, 一幅一幅图像逐渐变成密文图像, 攻击者采用与解密差不多长时间的连续同种变换破译.

(iv) 已知明文攻击. 因早期的置乱算法仅做 1 轮置乱, 置乱矩阵的元素比较简单, 攻击者可利用式(2)构造特殊的 x, y 凑成 \mathbf{A} 的逆矩阵进行破译.

(v) 选择明文攻击. 假定攻击者可得到加密机, 选择一系列明文得到对应密文, 从而解方程求解置乱系数.

(vi) 借用其它对公钥密码的攻击技术, 如针对离散对数问题的攻击.

本文提出的新算法可有效防文献提出的各种针对已往矩阵置乱的攻击. 色彩空间置乱可抵御(i); 随机矩阵及本文结论可用于生成周期变换, 可抵御(ii); 求周期的算法是关于 $\lceil \log_2 N \rceil$ 的多项式时间, 破译需 $O(N) = O(2^{\lceil \log_2 N \rceil})$ 的时间猜中周期, 时间上相差巨大, 可抵御(iii); 攻击(iv)本质上是建立在矩阵元素简单可猜的基础上, 当元素随机时有 $O(N^4)$ 种可能, 对于 ω 轮置乱有 $O(N^{4\omega})$ 种可能. 随着 N 的增大或置乱轮次 ω 的增多, 破译时间是天文数字. 引入概率密钥后, 即使同一幅明文图像在不同时间加密会得到不同密文图像, 即使选择明文攻击即(v)可解出固定密钥, 仍必须猜出 6^ω 种可能之一. 当 $\omega = 20$ 时, $6^\omega = 3.66 \times 10^{15}$, 按前述算法的计算时间统计, 完成整个猜测即使用当前最快速计算机也需耗时 10 万年以上. 故可成功抵御攻

击(v);离散对数问题是对已知周期的攻击,本算法的周期保密,故可抵御(vi),其它攻击都未超过(v),更精确描述如下.

定理 6. 对 1 轮变换,用自然数 J 连续作 J 次式(5)定义的变换 Δ 去加密数字图像($J < T(\mathbf{A}, N)$), $\Delta^J \circ P = (\sigma(x', y'))_{N \times N}$, 则 $(x', y')^T = \mathbf{A}^J (x, y)^T \bmod N$. 直接求 $\mathbf{A}^J \bmod N$ 只需不超过 $32 \lceil \log_2 N \rceil$ 次模 N 乘法. 解密先精确求 $T(\mathbf{A}, N)$, 再求 $\mathbf{A}^{T-J} \bmod N$, 只需不超过 $96 \lceil \log_2 N \rceil^2 + O(\log_2 N)$ 次模 N 乘法, 而 $(x, y)^T = \mathbf{A}^{T-J} (x', y')^T \bmod N$ 恢复置乱前空间位置. 两者都是输入长度 $\lceil \log_2 N \rceil$ 的平方时间. 但如知道 \mathbf{A} 不知道 J , 采取穷举法求 J , 最多要做 $T(\mathbf{A}, N) - 1$ 次迭代 $P^{k+1} = \Delta \circ P^k$, 要做 $O(N^2)$ 次(特殊时为 $O(N)$)模 N 乘法, 是输入长度 $\lceil \log_2 N \rceil$ 的指数时间. 当不知道置乱矩阵 \mathbf{A} 与 J 时, 先要猜出 \mathbf{A} 的元素值, 有 $O(N^4)$ 种可能(色彩置乱结论类似). 作 w 轮置乱变换, 加密、解密时间是 1 轮之上界的 w 倍, 破译则是 1 轮的 w 次幂. 猜出 w 轮随机密钥需要 6^w 倍时间.

证明. 利用定理 3, 4 及周期定义易得. 证毕.

对于黑白图像, 同样适合, 可以通过在每轮加密迭代的次数引入概率密钥的方法. 本算法的加强方案由空间域发展成变换域, 可利用小波变换的已有结果, 把信息隐藏与图像处理结合.

6 结 论

以算法 T_{2D} 为基础, 采用本文提出的位置色彩空间的多轮乘积型置乱变换及概率加密体制, 可快速进行数字图像的隐藏-恢复, 抗击文献出现的各种针对矩阵置乱的破译攻击算法, 在实际应用中可达到更加安全保密的效果.

致 谢 笔者谨对齐东旭教授致以衷心的感谢!

参 考 文 献

1 Westfeld A., Pfitzmann A.. Attacks on steganographic systems. In: Proceedings of the 3rd International Workshop on In-

formation Hiding, Lecture Notes in Computer Science 1768. Berlin: Springer-Verlag, 2000, 61~76

- 2 Qi Dong-Xu. Fractal and Computer Generation. Beijing: Science Press, 1994(in Chinese)
(齐东旭. 分形及其计算机生成. 北京: 科学出版社, 1994)
- 3 Qi Dong-Xu, Zou Jian-Cheng, Hang Xiao-You. A new scrambling transformation and its applications in image information hiding. Science in China(Series E), 2000, 30(5): 440~447(in Chinese)
(齐东旭, 邹建成, 韩效育. 一类新的置乱变换及其在图像信息隐藏中的应用. 中国科学(E辑), 2000, 30(5): 440~447)
- 4 Zou Jian-Cheng, Ward R. K., Qi Dong-Xu. A new digital image scrambling method based on Fibonacci numbers circuits and systems. In: Proceedings of the 2004 IEEE International Symposium on Circuits and Systems, Vancouver, 2004, 3: 965~968
- 5 Bilgin T.. Matrix transformation on certain sequence spaces. Applied Mathematics and Computation, 2003, 146(2/3): 433~436
- 6 Zou Jian-Cheng, Ward R. K.. Introducing two new image scrambling methods. In: Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Proceedings, Victoria, 2003, 2: 708~711
- 7 Zhang M.-R., Shao G.-C., Yi K.-C.. T-matrix and its applications in image processing. IEE Electronics Letters, 2004, 40(25): 1583~1584
- 8 Pan Cheng-Dong, Pan Cheng-Biao. Elementary Number Theory. 2nd Edition. Beijing: Peking University Press, 2003(in Chinese)
(潘承洞, 潘承彪. 初等数论. 第 2 版. 北京: 北京大学出版社, 2003)
- 9 Hu Guan-Zhang. Application Modern Algebra. 2nd Edition. Beijing: Tsinghua University Press, 1999(in Chinese)
(胡冠章. 应用近世代数. 第 2 版. 北京: 清华大学出版社, 1999)
- 10 Wang Ze-Hui. Modern Cryptography and Technology of Financial Information Security. Guangzhou: Jinan University Press, 2004(in Chinese)
(王泽辉. 现代密码学与金融信息安全技术. 广州: 暨南大学出版社, 2004)
- 11 Chen Bo, Tan Yun-Meng, Wu Shi-Zhong. Research on information hiding techniques. Computer and Digital Engineering, 2005, 33(2): 21~27(in Chinese)
(陈 波, 谭运猛, 吴世忠. 信息隐藏技术综述. 计算机与数字工程, 2005, 33(2): 21~27)

WANG Ze-Hui, born in 1963, associate professor. His research interests include cryptography and information security.



Background

The scrambling transformation is one of the important technologies in digital image information hiding. It is the basis in this technology to compute out the precise period T of the transformation. Many works in some literature have been done on determining the transformation periods of some special matrix or for some classes of modulus. To our knowledge, there is no the general method to determine the transformation period for any matrix of any elements, or for any modulus N period representation. Some methods have been proposed in some literatures for determining the transformation periods for a class of the scrambling transformations without giving the quick transformation period computation

algorithms.

A method for determining the transformation period $T(\mathbf{A}, N)$ for any matrix \mathbf{A} and any modulus N is proposed in this paper. The significant contribution of this paper is the general method and the quick algorithm taking $96(\log_2 N)^2 + O(\log_2 N)$ multiplications modulus N for solving the problems with any periods. A new probabilistic cryptosystem which can be effectively against chosen plaintext attack is constructed. The method given is for 2-dimension images but it can be easily extended to m -dimensions with $m > 2$. This work is supported by the a grant from the Science and Technique Program of Guangdong (No. 2006B15401009).