

引用格式:魏积愚,李国东,许向亮. 基于 FWHT 的动态多混沌彩色图像加密算法[J]. 微电子学与计算机,2020,37(9):43-49.
[WEI J Y, LI G D, XU X L. Dynamic multi-chaos color image encryption algorithm based on FWHT[J]. Microelectronics & Computer, 2020, 37(9): 43-49.]

基于 FWHT 的动态多混沌彩色图像加密算法

魏积愚,李国东,许向亮

(新疆财经大学 统计与数据科学学院,新疆 乌鲁木齐 830012)

摘 要: 针对彩色图像加密算法中混沌系统单一,密钥与明文关联性差的问题,提出一种基于 FWHT 的动态多混沌彩色图像加密算法. 首先对图像进行快速沃尔什哈达玛变换(FWHT);其次根据各通道像素值控制动态统一混沌系统参数构建不同系统,改进后用于各通道系数置乱;最后利用 Rabinovich 混沌序列控制 PWLCM 映射参数构建 R-P 混沌系统,迭代生成两级复合密钥流双扩散得到密文,叠加为彩色密文图像. 结果显示,密文图像直方图分布均匀,相关性几乎为 0,信息熵大于 7.999 3, NPCR 值和 UACI 值也近似于理论值,可有效抵抗各类攻击,具有较强加密性能.

关键词: 混沌加密;超混沌系统;动态控制;两级密钥;明文关联

中图分类号: TP309

文献标识码: A

文章编号: 1000—7180(2020)09—0043—07

Dynamic multi-chaos color image encryption algorithm based on FWHT

WEI Ji-yu, LI Guo-dong, XU Xiang-liang

(School of Statistics and Data Science, Xinjiang University of Finance and Economics, Urumqi 830012, China)

Abstract: To solve the problem of single chaotic system and poor correlation between key and plaintext in color image encryption, a dynamic multi-chaotic color image encryption algorithm based on FWHT is proposed. First, fast Walsh hadamar transform (FWHT) is applied to the image. Secondly, different systems are constructed based on the dynamic unified chaotic system parameters controlled by the pixel values of each channel, which can be used for channel coefficient scrambling after improvement. Finally, using Rabinovich chaotic sequence to control the PWLCM mapping parameters to construct r-p chaotic system, the two-stage compound key flow was iteratively generated to obtain the ciphertext, and the superposition was made into color ciphertext image. The results showed that the histogram of ciphertext images was evenly distributed, the correlation was almost 0, the information entropy was greater than 7.999 3, the NPCR value and UACI value were also approximate to the theoretical value, which could effectively resist all kinds of attacks and had strong encryption performance.

Key words: chaotic encryption; hyperchaotic system; dynamic control; two levels of key; plaintext association

1 引言

据不完全统计网络传播的信息中有接近百分之七十是由数字图像形式显示出来,因而针对数字图

像加密技术的研究成为广大中外学者讨论的经典问题.

混沌作为非线性动力学系统的一种特别的运动形式,广泛融入于不同社会科学和技术科学中,混沌

加密也成为引发研究人员关注的研究热点,但安全性能方面仍需继续改善加以提高.文献[1-2]针对传统 Cat 映射提出动态猫映射的图像加密算法,改善存在的缺陷使得算法具有更好的加密效果.文献[3-5]利用混沌序列将图像全局置乱和位级置乱相结合,完成了明文关联的图像加密.文献[6]则在依次对像素点三原色顺序置乱和分块置乱后进行小波处理再扩散置乱加密,提高了加密效率.

以上研究显示基于动态参数控制的混沌映射加密算法具有良好的加密性能.在此基础上为解决混沌系统单一,混沌维度较低^[7],产生的混沌序列复杂度低等问题^[8-9],构建 R-P 混沌系统,提出 FWHT 结合动态控制的多混沌彩色图像加密算法.

2 FWHT 变换与混沌系统

2.1 快速沃尔什哈达玛变换(FWHT)

常见的图像加密算法是基于图像空间域的运算,然而空间域运算在图像处理方面存在许多自身不足之处,因此频域处理为我们提供了另一种研究思路方向^[10].常见的频域变换有离散傅里叶变换(FFT)、离散余弦变换(DCT)等,此类变换以指数函数为基本的正交变换,数据在变换过程中必须在复数域处理,运算量庞杂.相比较之下,沃尔什—哈达玛变换(WHT)更加便利有效,只需要做实数域加减法运算,很大程度减少复杂运算.

沃尔什函数有三种排列方式,沃尔什排列、佩利排列、哈达玛排列;

$$\begin{cases} \text{Wal}_w(i, t) = \prod_{k=0}^{p-1} [R(k+1, t)]_{g(i)_k} \\ \text{Wal}_p(i, t) = \prod_{k=0}^{p-1} [R(k+1, t)]_{i_k} \\ \text{Wal}_H(i, t) = \prod_{k=0}^{p-1} [R(k+1, t)]_{<i_k>} \end{cases} \quad (1)$$

$R(k+1, t)$ 为任意拉德梅克函数, $g(i)_k$ 为 i 格雷码的第 k 位, i_k 为自然二进制的第 k 位, $<i_k>$ 为倒序二进制的第 k 位, P 为正整数.

$$\begin{aligned} R(n, t) &= \text{sgn}(\sin 2^n \pi t) \\ \text{sgn}(x) &= \begin{cases} 1 & x > 0 \\ -1 & x < 0 \end{cases} \end{aligned} \quad (2)$$

$R(n, t)$ 的取值有且仅有 $+1, -1$, 若 n 已知, 则 $R(n, t)$ 在 $(0 < t < 1)$ 内有 2^{n-1} 个周期, 若是在 $t = (k + \frac{1}{2}) / 2^n$, 那么能够获得离散数据序列 $R(n, k)$, k

$= 0, 1, 2, \dots, 2^n - 1$.

沃尔什函数的三种排列方式中, 哈达玛排列在快速运算方面最具有优势, 2^n 阶哈达玛矩阵有如下形式:

$$\begin{aligned} H_N &= H_{2^n} = H_2 \otimes H_{2^{n-1}} = \begin{bmatrix} H_{2^{n-1}} & H_{2^{n-1}} \\ H_{2^{n-1}} & -H_{2^{n-1}} \end{bmatrix} \\ &= \begin{bmatrix} H_{\frac{N}{2}} & H_{\frac{N}{2}} \\ H_{\frac{N}{2}} & -H_{\frac{N}{2}} \end{bmatrix} \end{aligned}$$

哈达玛矩阵的两个低阶矩阵可依次递推高阶, 矩阵间具有递推关系是它的最大特点.

$$W(u) = \frac{1}{N} \sum_{x=0}^{N-1} f(x) \text{Wal}_H(u, x) \quad (3)$$

沃尔什哈达玛矩阵基本运算原理为将 $f(x)$ 按相应规则变化后进行简单加减运算. 与快速傅里叶变换相似, 沃尔什哈达玛变换也有快速算法, 奇偶分类, 分别进行变换, FWHT 变换原理如下.

$$\begin{cases} W(u) = \frac{1}{2} [W_e(u) + W_o(u)] \\ W(u + \frac{N}{2}) = \frac{1}{2} [W_e(u) - W_o(u)] \end{cases} \quad (4)$$

FWHT 只进行简单加减运算, 比复数运算的傅里叶变换和余弦运算的 DCT 变换要简便更多, 效率更高, 选择 FWHT 变换代替常见的复数变换, 提高图像特征提取效率.

2.2 统一混沌系统

统一混沌系统数学模型如式(5)所示,

$$\begin{cases} \dot{x} = (25\alpha + 10)(y - x) \\ \dot{y} = (28 - 35\alpha)x + (29\alpha - 1)y - xz \\ \dot{z} = xy - (8 + \alpha)z/3 \end{cases} \quad (5)$$

为清晰表现出三类混沌系统的不同状态, 将系统可变参数分别控制为 $\alpha = 0, \alpha = 0.8, \alpha = 1$, 生成广义 Lorenz 混沌、吕混沌系统和广义 Chen 混沌系统. 其对应的混沌吸引子相轨迹如图 1 所示.

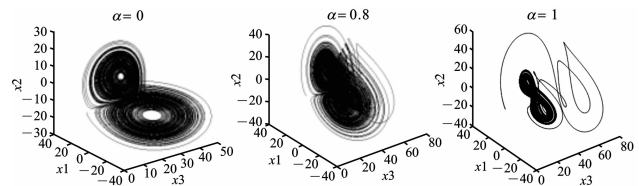


图 1 混沌吸引子相图

2.3 R-P 混沌系统

R-P 混沌系统由 Rabinovich 与 PWLCM 复合构建^[11]. 其中, Rabinovich 超混沌的数学模型如式

(6)所示:

$$\begin{cases} r_1 = kr_2 - ar_1 + r_2r_3 \\ r_2 = kr_1 - br_2 - r_1r_3 \\ r_3 = r_1r_2 - dr_3 + r_4^2 \\ r_4 = r_1r_2 + cr_4 \end{cases} \quad (6)$$

式中, a, b, c, d, k 为 Rabinovich 超混沌系统的系统参数, 当 $a = 1, b = -0.5, c = -2.2, d = 1, k = 8.1$ 时该系统处于超混沌状态。

分段线性映射数学模型如式(7)所示。

$$F(x) = \begin{cases} x/p & x \in [0, p) \\ (x-p)/(0.5-p) & x \in (p, 0.5) \\ F(1-x) & x \in (0.5, 1] \end{cases} \quad (7)$$

p 为控制参数, 在 $x \in (0, 1), p \in (0, 0.5)$ 条件满足的情况下, 该系统处于混沌状态。由于一些一维混沌, 例如常见的抛物线混沌其范围窄, 迭代产生的伪随机序列可能不够均匀, 而分段线性混沌的范围较宽^[12], 产生的混沌伪随机序列相比更加均匀。文章中用 Rabinovich 超混沌序列组合控制 PWLCM 参数与初值构建 R-P 混沌系统, 生成两级复合密钥流用于图像扩散, 具体原理将在扩散阶段详解。

3 加密算法设计

3.1 图像置乱

(1) 选取大小为 $m \times n \times 3$ 的彩色图像 P , 将其分解为 R, G, B 三通道, 从左至右, 上至下顺序转为一维矩阵, 计算总像素值 $I_r, I_g, I_b, A = [I_r, I_g, I_b]$, 若 $I_r(I_g/I_b) = \max(A), a = 0, I_r(I_g/I_b) = \text{median}(A), a = 0.8$, 否则 $a = 1$ 。构建三种混沌系统对应 R, G, B 三通道置乱。

为计算混沌系统初值且使密钥与明文相关^[13-14], 通过原始明文设定四个初值过渡参数 v_1, v_2, v_3, v ;

$$\begin{cases} v_1 = \text{mod}((R(1) \oplus R(2)) \cdots \oplus R(16) \\ \quad + \frac{1}{mm} \sum_1^{mm} R(i), 2^8) \times 10^{-11} \\ v_2 = \text{mod}((G(mm) \oplus G(mm-1)) \cdots \oplus \\ \quad G(mm-15) + \frac{1}{mm} \sum_1^{mm} G(i), 2^8) \times 10^{-11} \\ v_3 = \text{mod}((B(1) \oplus B(mm)) \cdots \oplus B(8) \oplus \\ \quad B(mm-7) + \frac{1}{mm} \sum_1^{mm} B(i)), 2^8) \times 10^{-11} \\ v = (v_1 + v_2 + v_3)/3 \end{cases} \quad (8)$$

给定预设初值, 加和 v_1, v_2, v_3, v 计算出真实初值, v_1, v_2, v_3 分别对应洛伦兹、吕、Chen 混沌系统, v 对应 Rabinovich 超混沌。 $x'_j, y'_j, z'_j, r'_1, r'_2, r'_3, r'_4$ 为各个系统预设初值。

$$\begin{cases} x_j(1) = x'_j + v_j \\ y_j(1) = y'_j + v_j \\ z_j(1) = y'_j + v_j \\ r_1(1) = r'_1 + v \\ r_2(1) = r'_2 + v \\ r_3(1) = r'_3 + v \\ r_4(1) = r'_4 + v \\ j = 1, 2, 3 \end{cases} \quad (9)$$

将初值代入统一混沌系统的三类系统, 产生 3 组长度为 $t+m \times n$ 的序列 $x_1, y_1, z_1, x_2, y_2, z_2$ 和 x_3, y_3, z_3 , 为消除混沌序列的初态效应, 舍去前 t 次数值, 处理存入 $X_{j,i}, Y_{j,i}, Z_{j,i}, i = 1, 2, \dots, mm, j = 1, 2, 3$ 。

$$t = \text{mod}((m^2 + n^2), (m + n)) + 2m + n \quad (10)$$

$$\begin{cases} X_{j,i} = [(abs(x_{j,i}) - [x_{j,i}]) \times 10^{13}] \text{mod} 2^{10} \\ Y_{j,i} = [(abs(y_{j,i}) - [y_{j,i}]) \times 10^{13}] \text{mod} 2^{10} \\ Z_{j,i} = [(abs(z_{j,i}) - [z_{j,i}]) \times 10^{13}] \text{mod} 2^{10} \end{cases} \quad (11)$$

将 $m \times n$ 长度序列整合处理生成新的一维混沌序列 U, V, Q ,

$$\begin{cases} U_i = ((X_{1,i} + Z_{1,i}) \text{mod} L) \oplus Y_{1,i} \\ V_i = ((Y_{2,i} + Z_{2,i}) \text{mod} L) \oplus X_{2,i} \\ Q_i = ((X_{3,i} + Y_{3,i}) \text{mod} L) \oplus Z_{3,i} \end{cases} \quad (12)$$

式中, L 为灰度级, 虽然系统本身已经具有高度敏感性, 但是在构造降为一维模型后, 这种性能再次放大, 混沌序列更加复杂、优越, 改变密钥中的任意一部分都会使得整个像素值发生变化。

(2) 对 R, G, B 三通道进行图像预处理-沃尔什哈达玛变换, 获得对应系数矩阵^[15]。

(3) 借助 randperm 函数对 R 通道随机排序获得 $\tilde{R}, \tilde{R}$ 具有一个旧的元素序号矩阵 O_R 和新的元素序号矩阵 T_R , 对 G 通道随机排序获得 $\tilde{G}, \tilde{G}$ 具有一个旧的元素序号矩阵 O_G 和新的元素序号矩阵 T_G , B 通道随机排序获得 $\tilde{B}, \tilde{B}$ 具有一个旧的元素序号矩阵 O_B 和新的元素序号矩阵 T_B , 按 T_R 顺序对 G 系数矩阵排序, T_G 顺序对 B 系数矩阵排序, T_B 顺序对 R 系数矩阵排序, 得到新的位置产生 R', G', B'

$$\begin{cases} R'(i) = R(T_B(i)) \\ G'(i) = G(T_R(i)) \\ B'(i) = R(T_G(i)) \end{cases} \quad (13)$$

(4) 通过冒泡法对构建的 U 、 V 、 Q 序列升序排序, 生成 f_U, f_V, f_Q 三组索引序列, 如任意序列 $\{5, 6, 2, 3, 1, 8\}$, 将该序列升序排序后得到序列 $\{1, 2, 3, 5, 6, 8\}$, 进而得到所需的相应位置序列, 即索引序列 $\{5, 3, 4, 1, 2, 6\}$, 分别用索引序列对 R', G', B' 全局置乱:

$$\begin{cases} XR(i) = R'(f_U(i)) \\ XG(i) = G'(f_V(i)) \\ XB(i) = B'(f_Q(i)) \end{cases} \quad (14)$$

完成 R 、 G 、 B 三通道的全局置乱。

(5) 置乱后的 R 、 G 、 B 系数矩阵进行快速沃尔什-哈达玛逆变换 (IFWHT), 得到重构的置乱图像 XR, XG, XB 。

3.2 图像扩散

(1) 迭代 Rabinovich 混沌系统 $t + m \times n$ 次, 产生四组随机序列, 截取后 $m \times n$ 个数值分别存入 $1 \times m \times n$ 的一维矩阵 H_1, H_2, H_3, H_4 中。使用 H_1, H_2, H_3, H_4 中元素计算得到新的序列 xF 和 pF 。

$$\begin{cases} xF_1(i) = (H_1(i) + H_2(i)) \bmod 1 \\ xF_2(i) = (H_1(i) + H_4(i)) \bmod 1 \\ xF_3(i) = (H_2(i) + H_4(i)) \bmod 1 \\ xP_1(i) = (H_1(i) + H_3(i)) \bmod 1 \\ xP_2(i) = (H_2(i) + H_3(i)) \bmod 1 \\ xP_3(i) = (H_3(i) + H_4(i)) \bmod 1 \end{cases} \quad (15)$$

这里的序列 xF 和 pF 为第二级密钥, 使用 xF 和 $pF/2$ 作为分段线性映射的初始值和参数构成 R - P 系统, 共 $m \times n \times 3$ 组初始值和参数, 每组迭代得到一个新的状态值, 得到 3 条新的序列 xG_1, xG_2, xG_3 , 由 H_j 和 xG_j ($j = 1, 2, 3$) 根据式 (16) 得到整数序列, 记为 xH_j 和 xK_j :

$$\begin{aligned} xK_j &= [(xG_j \times 100) - [xG_j \times 100] \times 10^6] \bmod 256 \\ xH_j &= [(H_j \times 100) - [H_j \times 100] \times 10^6] \bmod 256 \\ j &= 1, 2, 3 \end{aligned} \quad (16)$$

(2) 将置乱重构图像 X_R, X_G, X_B 转化为一维向量, xH_1, xH_2, xH_3 和 xK_1, xK_2, xK_3 分别作为 X_R, X_G, X_B 向量的密钥流, 进行正向循环扩散和逆向循环扩散, 规则为: xH_j ($j = 1, 2, 3$) 序列与置乱序列正向扩散得到中间密文图像 E , xK_j ($j = 1, 2, 3$) 与 E 逆向扩散得到双向循环扩散密文图像 (C'_R, C'_G, C'_B), 扩散部分以 R 通道为例, 其余通道对应其余序

列原理相同。

$$\begin{cases} E(i) = E(i-1) \oplus xH_1(i) \oplus X_R(i) \\ C'_R(i) = C'_R(i+1) \oplus xK_1(i) \oplus E(i) \end{cases} \quad (17)$$

(3) 为进一步加强算法安全性, 进行二次扩散。由 xK_1, xK_2, xK_3 生成 3 组键控序列 xM_1, xM_2, xM_3 作为掩码, xL_1, xL_2, xL_3 为动态控制的移位参数。

$$xM_j(i) = \begin{cases} 0 & xK_j(i) < \frac{1}{mn} (\sum_{i=1}^{mn} K_j(i)) \\ 1 & \text{other} \end{cases} \quad (18)$$

$$xL_j(i) = \bmod(\text{round}(xF_j(i) \times 10^{10}), 4) + 1 \quad (19)$$

$$j = 1, 2, 3, i = 1, 2, 3 \dots, m \times n$$

根据序列中“0”和“1”来选择 $C'(i)$ 位变换方向, 首先将一次扩散的密文图像 C' 转为二进制进行位平面分解, 接着设置 xM_1, xM_2, xM_3 为掩码, 对 $C'(i)$ 二进制序列选择移位, “0”向左移, “1”向右移, 移动 $xL(i)$ 位。具体过程如图 (2) 所示。

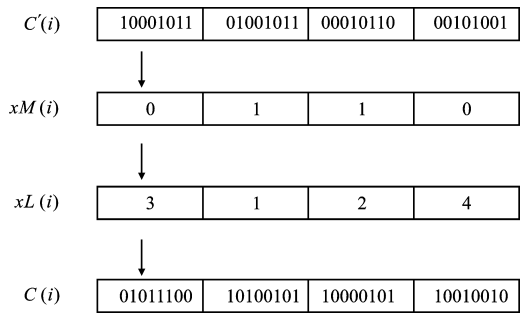


图 2 二次扩散示意图

(4) 移位结束后, 将像素值从二进制恢复到十进制, 并将序列 reshape 为 3 个 $m \times n$ 二维矩阵, 生成 R 、 G 、 B 三通道的密文图像 $C(C_R, C_G, C_B)$ 。将密文图像 C_R, C_G, C_B 叠加为彩色加密图像, 完成彩色图像加密。

3.3 解密算法

解密过程为加密过程的逆过程, 依次对密文图像做扩散和置乱的逆向操作处理。

4 实验仿真及安全性分析

4.1 实验仿真

基于 MATLAB R2017a 平台进行实验仿真, 采用大小为 $512 \times 512 \times 3$ 的经典 Lena 图像和吐鲁番杏花节游客图 Turpan。初始密钥包括广义 Lorenz 混沌映射的初始值 $\text{key1} = [-1, -0.2, 0.5]$; 吕混沌初始值 $\text{key2} = [0.3, 2.5, 3.2]$; 广义 Chen 混沌初

始值 $\text{key3}=[0.27,0.45,0.78]$;Rabinovich 超混沌映射的初始值 $\text{key4}=[0.8,0.5,12.1,3.5]$;R-P 系统初始值由 Rabinovich 超混沌迭代序列值按规则计算得来,同时为了使密钥与明文相关联,所添加的过渡参数由明文自身决定.图 3 为原始图像与其对应密文图像.



图 3 原始图像与对应密文图像

4.2 安全性分析

4.2.1 直方图分析

图像非常重要的一个统计特征就是图像的直方图,表示该图像中每一灰度级与该灰度级出现的频率的对应关系.选择 Lena 图像进行分析,图 4 可见,原始 R 、 G 、 B 三通道像素值频率分布直方图显示出像素灰度级分布不均匀,加密后 R 、 G 、 B 三通道像素值频率分布直方图显示出像素灰度级分布很均匀,具有均匀分布特征,很好地掩盖了明文图像的像素分布特征,提高了破译难度.同时选择用单边假设检验,即统计量在数量上衡量前后两个直方图的差别.

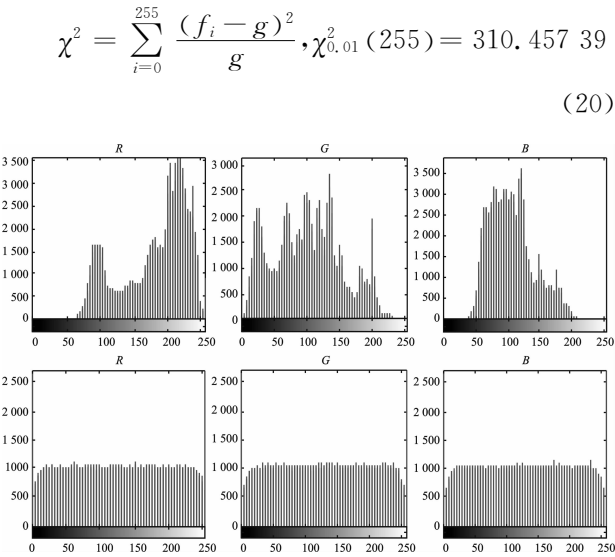


图 4 明密文灰度直方图

由表 1 也可以看出, R 、 G 、 B 分量的明文图像的统计量的计算值远远大于 $\chi^2_{0.01}(255)$ 的值,明文不均匀分布,而 R 、 G 、 B 分量的密 χ^2 统计量的计算值小于 $\chi^2_{0.01}(255)$ 的值,密文像素值近似均匀分布.

表 1 χ^2 检验结果

	R	G	B
明文	$2.482\ 8\times10^{-5}$	$1.319\ 1\times10^{-5}$	$3.367\ 8\times10^{-5}$
密文	230.970 7	258.439 5	216.752 0

4.2.2 相邻像素相关性分析

相关性分析指为衡量两个变量因素的相关密切程度对相应具有相关性的变量元素分析,对 R 、 G 、 B 明文图像和密文图像随机选取 2 000 对相邻的像素点,通过式(21)计算各个方向相邻像素点之间的相关系数.

$$\left\{\begin{aligned}r_{xy}&=\frac{\text{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}}\\\text{cov}(u,v)&=\frac{1}{N}\sum_{i=1}^N(x_i-E(u))(y_i-E(v))\\D(u)&=\frac{1}{N}\sum_{i=1}^N(u_i-E(u))^2\\E(u)&=\frac{1}{N}\sum_{i=1}^Nu_i\end{aligned}\right.$$

(21)

图 5 是 R 、 G 、 B 明文密文图像水平方向相邻像素分布,表 2 是水平、垂直、对角的相关系数,加密前无论是从哪个角度,都是非常接近的,加密后均匀分散,说明置乱程度明显.相比较于文献[7] 整个加密算法对图像像素点产生置乱效果更好,更能够抵抗基于相邻像素相关性的统计攻击.

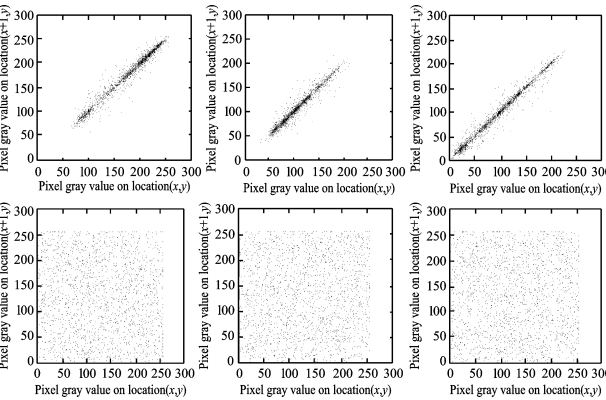


图 5 明密文(水平方向)相邻像素分布图

表 2 相关系数

		R	G	B
明文	水平	0.987 2	0.986 8	0.986 6
	垂直	0.971 2	0.977 3	0.971 8
	对角	0.962 2	0.959 0	0.953 0
密文	水平	0.002 2	0.020 8	0.009 5
	垂直	0.014 5	0.010 7	0.006 8
	对角	0.007 4	0.002 5	0.018 7
文献[7]密文	水平	-0.001 6	-0.025 2	-0.039 5
	垂直	-0.025 1	-0.010 4	0.012 1
	对角	-0.024 1	0.014 9	-0.030 8

4.2.3 密钥敏感性分析

密钥敏感性分析,主要为了研究当整个加密算法运行时,算法原始密钥发生极其微小改变而对密文图像产生的影响.现借助解密系统来分析密钥敏感性,以 R 通道为例,将 Rabinovich 超混沌系统初值发生 10^{-10} 极微小变化,解密密文图像,无法还原原始明文图像,说明密钥敏感性较强,加密性能好,如图 6 所示.

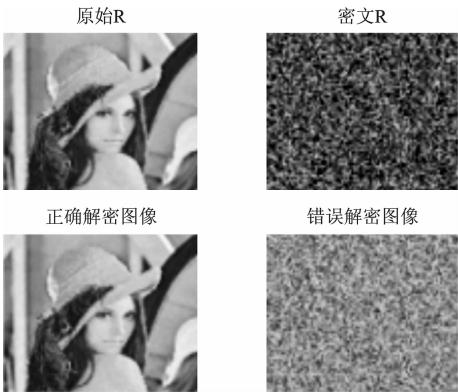


图 6 密钥敏感性测试图

4.2.4 明文敏感性分析

在 R、G、B 原始明文图像中随机选择一像素点,改变其灰度值后加密产生密文图像,对原始密文图像和修改灰度值后密文图像分析,进行 200 次随机实验计算其 NPCR 和 UACI 平均值. NPCR 在这里可以用来比较两个相同密文图像相应位置像素点的值,记录不同像素点个数占全部像素点个数的比例, UACI 比较两个密文图像相应位置的像素点值,记录它们的差值.表 3 显示 NPCR、UACI 的计算结果都接近理论值,且略优于文献[7].说明明文像素点发生极微小变化时,得到的相应密文图像对应像素值相差迥异,该算法具有良好的明文敏感性.

$$\left\{ \begin{aligned} \text{NPCR}(P_1, P_2) &= \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \text{Sign}(P_1(i, j) - P_2(i, j)) \times 100\% \\ \text{UACI}(P_1, P_2) &= \frac{1}{MN} \sum_i^M \sum_j^N \frac{P_1(i, j) - P_2(i, j)}{255 - 0} \times 100\% \\ \text{其中 Sign}(x) &= \begin{cases} 1, x > 0 \\ 0, x = 0 \\ -1, x < 0 \end{cases} \end{aligned} \right. \quad (22)$$

表 3 明文敏感性分析结果

	R	G	B
NPCR	0.996 1	0.995 9	0.995 7
文献[11]	0.995 7	0.998 3	0.994 7
UACI	0.335 6	0.335 8	0.336 1
文献[11]	0.333 6	0.335 8	0.338 6

4.2.5 信息熵

信息熵近似于在数学上的离散随机事件出现的概率,有序的系统显示出较低的信息熵,无序的系统显示出较高的信息熵,信息熵大小与无序程度息息相关,因此,信息熵可以理解为相当于一个度量标准用来度量系统的无序化程度.信息熵反应出一个信息的不确定性,定义公式如下.

$$H(x) = - \sum_{i=0}^{255} p(x_i) \log_2(p(x_i)) \quad (23)$$

同样,信息熵在图像加密中也可以用来度量图像灰度值的分布状态,灰度分布越均匀信息熵越大,图像加密安全性高,遇到攻击时丢失图像信息的可能性更低,相反如果图像的灰度分布不均匀则信息熵就越小,加密的图像数据则安全性较低,遇到攻击时易被窃取,如表 4 所示,该算法加密图像信息熵接近理论值(即 8).

表 4 信息熵

	R	G	B
明文	7.260 2	7.565 3	7.003 9
密文	7.999 4	7.999 3	7.999 4

5 结束语

彩色图像相比较于灰度图像所包含的图像信息更多,数据量更大^[16],传统的加密方法难以和图像传输速率相匹配,而近年来基本的混沌动力学系统的加密算法中大多采用低维的混沌系统,这类算法的中混沌系统较为单一,混沌维度较低,产生的混沌序列复杂度低,密钥空间小,图像抗攻击能力差,导致整体加密算法安全性能低^[17].为此提出了基于动态控制的多混沌彩色图像加密算法.该算法中包含三维广义 Lorenz 混沌,吕混沌和广义 Chen 混沌,四维 Rabinovich 混沌及构造的 R-P 混沌系统等多种混沌系统,设计与明文相关联的初值参数,通过混沌系统迭代两级密钥,产生具有更高遍历性和复杂度,更加难以预测混沌序列,在 FWHT 变化基础上分别对彩色图像 R、G、B 三通道动态选择不同混沌系统与密钥流,多轮置乱扩散加密.实验仿真证明,该

算法与明文图像具有极大的关联性,密钥空间大,直方图分布均匀,像素相关性几乎为零、密钥敏感性强且NPCR、UACI和信息熵都接近理想值,可以有效抵抗各类攻击。综上,算法加密效果好,具有实际的应用价值。未来可以考虑对混沌系统继续改进联合,产生更加复杂密钥流用于各类变换,进一步提高算法加密效率和安全性。

参考文献:

- [1] WANG X F, WANG X L, WANG J M, et al. A chaotic image encryption algorithm based dynamic cat map[J]. Journal of Henan Normal University(Natural Science Edition), 2018, 46(5): 110-117.
- [2] SUN Q, HU S. Improved cat map and chaotic system based fast color image encryption algorithm[J]. Application Research of Computers, 2017, 34(1): 233-237.
- [3] CHENG D S, TAN X, XU Z L, et al. Image Encryption Algorithm Research by Combining Four Dimensional Hyper-Chaotic System and Bit Decomposition[J]. Journal of University of Electronic Science and Technology of China, 2018, 47(6): 906-912.
- [4] DENG X H, LIAO C L, ZHU C X, et al. Image encryption algorithms based on chaos through dual scrambling of pixel position and bit[J]. Journal on Communications, 2014, 35(3): 216-223.
- [5] WANG L L, LI G D. Hyperchaotic color image encryption algorithm based on DNA sequence[J]. China Sciencepaper, 2018(13): 1974-1981.
- [6] CHEN S X, TANG Y Y. Triple scrambling algorithm for RGB color image based on chaotic system[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2018, 30(6): 812-818.
- [7] XIE G B, ZHU R Y. Image encryption algorithm based on compound cascade chaotic[J]. Computer Engineering and Applications, 2018, 54(8): 189-194.
- [8] XIAO F, ZHANG L L, FENG F. Parallel Multi-channel Color Image Encryption Based on Hybrid Chaotic System[J]. Microelectronics & Computer, 2016, 33(8): 76-81.
- [9] ZHANG J, HUO D. Quantum Colour Image Encryption Algorithm Based on Chaotic Systems[J/OL]. Journal of Southwest Jiaotong University: 1-7. [2019-04-14].
- [10] LIANG X K, TAO L M, HU B. Image hybrid encryption based on a generalized chaotic mapping and matrix nonlinear transformation[J]. Journal of Image and Graphics, 2019, 24(3): 325-333.
- [11] MA C, WANG A Y, LI G D. Image encryption algorithm based on double scrambling and C-R chaotic system[J]. Computer Engineering and Design, 2019, 40(10): 2773-2777.
- [12] LIANG Y, ZHANG S W. Image encryption algorithm based on bit-level synchronous permutation diffusion and pixel-level annular diffusion[J]. Journal of Image and Graphics, 2018, 23(6): 814-826.
- [13] XIE G B, GAO Z X. Plaintext related color image encryption algorithm based on multiple chaotic maps[J]. Computer Engineering and Design, 2019, 40(4): 920-930.
- [14] LV D M, LI G D, WANG L J. Ectopic XOR Image Encryption Algorithm Based on Variable Parameter Chaos[J]. Packaging Engineering, 2019, 40(17): 227-234.
- [15] LANG J. Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain[J]. Optics Communications, 2015(338): 181-192.
- [16] WEI X, GUO L, ZHANG Q, et al. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system[J]. Journal of Systems and Software, 2012, 85(2): 290-299.
- [17] LIU H, WANG X. Color image encryption based on one-time keys and robust chaotic maps[J]. Computers & Mathematics with Applications, 2010, 59(10): 332.

作者简介:

魏积愚 女, (1995-), 硕士. 研究方向为数字图像加密.

E-mail: 1071648735@qq.com.

李国东 男, (1976-), 博士, 教授. 研究方向为细胞神经网络与数字图像加密.

许向亮 男, (1994-), 硕士. 研究方向为数字图像加密.