

基于多轮扩散的彩色图像加密算法

柴秀丽, 郭峻言

(河南大学 图像处理与模式识别研究所, 河南 开封 475004)

摘 要: 为了保护彩色图像信息的安全, 提出了一种基于多轮扩散的彩色图像加密算法. 该算法首先对 Lorenz 混沌系统及 Chen 混沌系统的混沌序列进行改进; 然后利用改进后的 Lorenz 序列对明文图像进行置乱; 最后结合改进后的 Lorenz 混沌序列和改进后的 Chen 混沌序列以及彩色图像自身的像素分布特征, 利用多轮扩散对置乱后的图像进行像素值改变, 实现彩色图像加密. 理论分析和仿真实验表明, 该算法具有足够大的密钥空间, 在抵抗密文攻击、差分攻击、选择明文攻击及统计攻击方面都具有良好的性能, 可以广泛地应用于多媒体数据的保密通信中.

关键词: 保密通信; 多轮扩散; 图像置乱; 彩色图像加密

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2014)05-0062-05

Color Image Encryption Algorithm Based on Several Rounds of Proliferation

CHAI Xiu-li, GUO Jun-yan

(Institute of Image Processing and Pattern Recognition, Henan University, Kaifeng 475004, China)

Abstract: In order to achieve effective protection of the color image information, a new color image encryption algorithm is proposed based on several rounds of proliferation. Firstly, the chaotic sequences generated by 'Lorenz' chaotic system and 'Chen' chaotic system are improved to get two groups of different chaotic sequences. Then, the pixels' positions of the image are scrambled by improved 'Lorenz' chaotic sequences. Finally, by using both of the two groups of improved chaotic sequences and the distribution of pixels in the color image, we change the pixels' values of the scrambled image through several rounds of proliferation and get the ciphered image. Theoretical analysis and simulation results show that this algorithm with a sufficiently large key space not only can perfectly resist the ciphertext attack and differential attack, but also is excellent against chosen plaintext attack and statistical attack, which can be widely used in secure communication of multimedia data.

Key words: secure communication; several rounds of proliferation; image scrambling; color image encryption

1 引言

近年来, 为了有效提高图像信息的安全性, 混沌理论的研究已经得到充分发展, 很多研究者提出了基于混沌的图像加密算法和改进算法^[1-3], 但这些算法仍然效率较低、密钥空间较小、抵抗各种攻击能力弱、随机序列仅与初始值有关, 不依赖于明文, 一个明文字节只能影响其加密后的一个密文字节^[4]等缺

陷, 为各种攻击带来可能性.

本文针对以上缺陷, 提出了一种基于多轮扩散的彩色图像加密算法. 该算法可充分抵抗穷举攻击; 加密图像的像素值分布均匀随机, 具有较高的安全性; 加密算法使加密后图像每一个密文值均与所有明文和密文值相关, 并通过初值选取等措施确保算法同时对密钥和明文敏感.

收稿日期: 2013-06-20; 修回日期: 2013-08-15

基金项目: 国家自然科学基金项目(61004006, 61203094); 河南省基础与前沿技术项目(132300410475); 河南省教育厅自然科学研究计划(12A460001, 2011A510001, 2011A520004)

2 Lorenz 混沌系统和 Chen 混沌系统

2.1 Lorenz 混沌序列及其改进

Lorenz 系统^[3]是一个经典的三维混沌系统,其动力学方程为

$$\begin{cases} dx/dt = \delta(y - x) \\ dy/dt = \gamma x - \alpha z - y \\ dz/dt = xy - \lambda z \end{cases} \quad (1)$$

式中, δ, γ, λ 为系统参数,当 $\delta = 10, \gamma = 28, \lambda = 8/3$ 时,系统进入混沌状态,本文采用四阶 Runge-Kutta 数值积分方法来求解微分方程组,对于给定的初始条件 (x_0, y_0, z_0) ,可产生非周期、不收敛、对初始值 (x_0, y_0, z_0) 极端敏感的三维混沌序列 $\{(x_i, y_i, z_i) \mid i = 1, 2, 3, 4, \dots\}$. 以初始值 $x_0 = -1.010, y_0 = 0.1, z_0 = 1.03$,积分步长 $h = 0.001$ 来计算 Lorenz 序列,其混沌吸引子如图 1 所示, x 序列的自相关性如图 2(a) 所示、 $x-z$ 序列的互相关性如图 2(b) 所示.

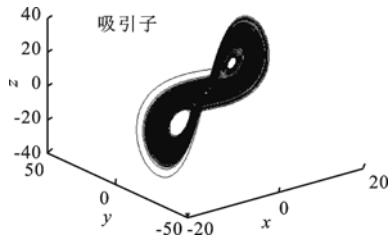


图 1 Lorenz 混沌吸引子

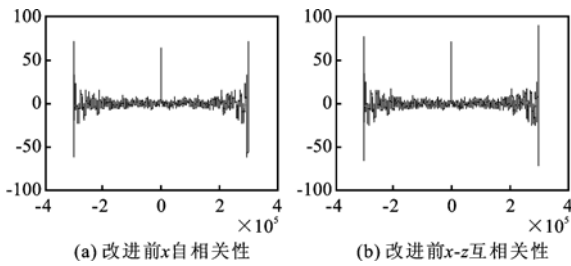


图 2 改进前 x 自相关性和 $x-z$ 互相关特性

参考文献^[3]的改进方法,利用式(2)得到改进后的混沌序列如图 3 所示.此优化序列具有良好的混沌特性、较理想的函数自相关特性和近似为 0 的互相关特性.式中:round 取最近整数, k 为控制参数.

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

2.2 Chen 系统

Chen 系统^[5]的动力学方程可以描述为

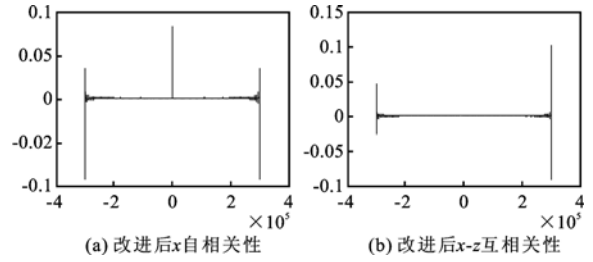


图 3 改进后 x 自相关性和 $x-z$ 互相关特性

$$\begin{cases} X' = a(Y - X) \\ Y' = bY - XZ + (b - a)X \\ Z' = XY - cZ \end{cases} \quad (3)$$

式中, a, b, c 为系统的控制参数,在 $a = 35, b = 28, c = 3$ 时,Chen 系统为混沌的,系统产生的混沌序列有以下问题: X, Y, Z 的值域各有差别,不便于批处理; X, Y, Z 局部的取值表现为一定的单调性,不能抵御线性预测攻击; X, Y, Z 自相关特性不是理想的 δ 函数,互相关特性不是理想的零特性,系统多输出特性也没有得到充分利用.因此采用与 2.1 节相同的处理方法对 Chen 混沌序列进行改进,改进的 Chen 系统混沌序列具有良好的混沌特性、理想的自相关特性和接近于 0 的互相关特性^[5].

3 加密算法和解密算法

本文算法同时采用像素置乱和多轮扩散改变像素值加密,使加密图像像素分布更加随机.设 RGB 彩色图像 A 大小为 $m \times n$.读取原始彩色图像后进行 RGB 分离 $fR = A(:, :, 1); fG = A(:, :, 2); fB = A(:, :, 3)$.

3.1 像素置乱

采用四阶 Runge-Kutta 数值积分方法来求解 Lorenz 微分方程组得到混沌序列 $\{(x_i, y_i, z_i) \mid i = 1, 2, 3, 4, \dots, m+n\}$.利用式(2)改进该序列后得到 $\{(x(i), y(i), z(i)) \mid i = 1, 2, 3, \dots, m+n\}$.利用 $\{x(i), i = 1, 2, 3, \dots, m+n\}$,按升序或降序排序得到新的有序序列 $\{Cx(i), i = 1, 2, 3, \dots, m+n\}$,将 $Cx(i)$ 的值用其在 $x(i)$ 中的位置索引值替代,即得到服从排序位置分布的混沌随机整数序列 $\{Sx(i), i = 1, 2, 3, \dots, m+n\}$,根据混沌随机序列 $Sx(i)$ 对 R 分量的行和列进行置乱,若 $Sx(i) = j$,表示将 fR 的 i 行(列)调换到 j 行(列).

同理用 $y(i)$ 和 $z(i)$ 分别对 G 分量和 B 分量进行行和列置乱.这样原来同一像素位置的 RGB 分量

的像素值已在各自分量上随机分布在不同的位置,从而实现彩色图像的 RGB 置乱,得到置乱后图像的 R、G、B 分量分别为 fR 、 fG 、 fB 。

3.2 像素值扩散

扩散是一种将明文冗余度分散到密文中的方法,即将单个明文或密钥位的影响尽可能扩大到更多的密文里去,不仅将统计关系隐藏起来,也使密码分析者寻求明文冗余度增加了难度。文献[3]中混沌系统产生的随机序列仅与初始值有关,而不依赖于明文,导致一个明文字节只能影响其加密后的一个密文字节,给选择明文攻击和选择密文攻击带来了可乘之机^[4]。针对这个缺点,本文提出多轮扩散机制,使每一位密文都受到每一位明文、密文和密钥的影响。采用改进 Lorenz 混沌序列和改进 Chen 混沌序列,利用异或(XOR)操作对置乱后的 R、G、B 的各个分量的像素值进行改变。对于给定的系统,迭代次数可能与初始条件及系统参数有关,本文将丢弃前4 000次迭代产生的数据^[6]。

像素值多轮扩散步骤如下:

步骤1 利用式(4)获取 Lorenz 异或操作数矩阵 P_x 、 P_y 、 P_z 。式中: $j = 1, 2, \dots, m \times n$, round 取最近整数, mod 取余, $\{(x(i), y(i), z(i)) \mid i = 1, 2, 3, \dots, m \times n\}$ 为改进后 Lorenz 混沌序列。

$$\begin{cases} P_x(j) = \text{round}((x(4\ 000 + j) + 0.5) * 10^7) \\ \quad \text{mod}256 \\ P_y(j) = \text{round}((y(4\ 000 + j) + 0.5) * 10^7) \\ \quad \text{mod}256 \\ P_z(j) = \text{round}((z(4\ 000 + j) + 0.5) * 10^7) \\ \quad \text{mod}256 \end{cases} \quad (4)$$

步骤2 利用改进后的 Lorenz 混沌序列对加密图像进行第一轮加密,加密公式如式(5)所示:

$$\begin{cases} FR(j) = fR(j) \oplus P_x(j) \\ FG(j) = fG(j) \oplus P_y(j) \\ FB(j) = fB(j) \oplus P_z(j) \end{cases} \quad (5)$$

步骤3 改进后的 Chen 混沌序列为 $\{(X(i), Y(i), Z(i)) \mid i = 1, 2, 3, \dots, m \times n\}$ 。由式(6)得到异或操作数的矩阵 PX 、 PY 、 PZ 。式中: $j = 1, 2, \dots, m \times n$; $\oplus$ 异或操作; mod 取余。

$$\begin{cases} PX(j) = P_x(j) \oplus X(4\ 000 + j) \\ PY(j) = P_y(j) \oplus Y(4\ 000 + j) \\ PZ(j) = P_z(j) \oplus Z(4\ 000 + j) \end{cases} \quad (6)$$

步骤4 利用式(7)对加密后的各个分量进行第二轮加密。FR、FG、FB 为加密后图像的 RGB 分量。式中, $j = 1, 2, \dots, m \times n$ 。当 $j = 1$ 时, FR、FG、FB 的初始值分别为 kR 、 kG 、 kB 。 $kR = \text{sum}R \text{ mod}256$; $kG = \text{sum}G \text{ mod}256$; $kB = \text{sum}B \text{ mod}256$, 其中, sumR、sumG、sumB 分别指原始图像 RGB 各个分量的各个像素的和,即原始图像 RGB 各个分量的各个像素的和对 256 取余后作为 RGB 分量加密后的初始值。

$$\begin{cases} FR(j) = FR(j) \oplus PX(j) \oplus FR(j-1) \oplus \\ \quad FG(j-1) \oplus FB(j-1) \\ FG(j) = FG(j) \oplus PY(j) \oplus FG(j-1) \oplus \\ \quad FR(j-1) \oplus FB(j-1) \\ FB(j) = FB(j) \oplus PZ(j) \oplus FB(j-1) \oplus \\ \quad FG(j-1) \oplus FR(j-1) \end{cases} \quad (7)$$

步骤5 最后利用 R、G、B 分量加密后的密文值对第二轮加密后的矩阵再次进行替代加密,加密公式如式(8)所示:

$$\begin{cases} FR(j) = (FB(j) + FG(j)) \text{ mod}256 \oplus FR(j) \\ FG(j) = (FR(j) + FB(j)) \text{ mod}256 \oplus FG(j) \\ FB(j) = (FR(j) + FG(j)) \text{ mod}256 \oplus FB(j) \end{cases} \quad (8)$$

多轮扩散加密中,通过将上一个密文中的像素分量 RGB 值反馈到下一密文的像素分量 RGB 中,使每一位密文都受到所有明文和密钥的影响,可抵御选择密文攻击以及选择明文攻击,每一个加密后像素点的值均受到上一个像素点的值的影响,而第一个点的加密是由图像自身决定的(kR , kG , kB)计算得出的,即加密后图像的 RGB 值和原始图像自身值有关,增强了对明文的敏感性。

3.3 解密算法

解密算法即为加密算法的逆过程,利用改进的 Lorenz 混沌序列和改进的 Chen 混沌序列从密文图像依次还原为置乱后的图像,然后根据改进的 Lorenz 混沌序列,将其还原为原始明文。

4 仿真实验

本文采用大小 256×256 的标准 lena 彩色图像作为明文,以 MATLAB7.0 为平台,通过实验仿真

来对加密密钥空间及执行效率、密钥的敏感性、灰度直方图、相邻像素相关性、信息熵和明文敏感性进行分析和测试. 仿真结果如图4所示,图4(a)为明文图像,图4(b)为密文图像.

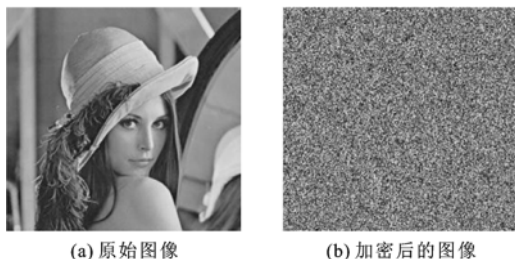


图4 原始图像和加密后的图像

4.1 密钥安全性分析

4.1.1 加密密钥空间及执行效率分析

在本文的算法中,以双精度浮点数初值 $\{x_0, y_0, z_0\}$ 、 $\{X_0, Y_0, Z_0\}$ 为密钥,则密钥空间为 $2^{64} \times 2^{64} \times 2^{64} \times 2^{64} \times 2^{64} \times 2^{64} = 2^{384}$,相当于384比特长度的二进制密钥,密钥空间可以抵御穷举攻击. 在matlab7.0.4、Intel Pentium Dual E2140的CPU、内存2 GB、Windows XP系统的仿真环境下,加密 256×256 图像耗时约0.45 s,表明费时短,效率高.

4.1.2 密钥敏感性测试

本文分别用正确的密钥和由初值 $\{x_0 + 10^{-10}, y_0, z_0, X_0, Y_0, Z_0\}$ 、 $\{x_0, y_0 + 10^{-8}, z_0, X_0, Y_0, Z_0\}$ 作为密钥对密文图像进行解密. 实验结果说明使用与正确密钥十分接近的错误密钥进行解密时,得到的是十分错误的解密图像,本文算法对密钥具有高度的敏感性.

4.2 统计特性分析

4.2.1 灰度直方图分析

灰度直方图是灰度级的函数,它表示图像中具有每种灰度级的象素的个数,反映图像中每种灰度出现的频率,明文图像与密文图像R、G、B分量直方图表明:

明文图像的直方图分布不均匀,密文图像的直方图灰度值呈均匀分布而且平坦,前后对比有显著变化,这表明密文图像的像素值均匀分布在 $[0, 255]$ 内,从而说明本文的算法能够有效地防止统计攻击.

4.2.2 相邻像素相关性分析

通过比较明文和密文图像相邻像素的相关性,可以考察图像进行置乱的程度^[7],相关性通常用相邻像素的相关系数 R_{xy} 来表达:

$$\begin{cases} R_{xy} = \text{cov}(x, y) / \sqrt{D(x)D(y)} \\ \text{cov}(x, y) = E((x - E(x))(y - E(y))) \\ D(x) = E((x - E(x))^2) \end{cases} \quad (9)$$

式中, x, y 为两个相邻像素值. 本文分别在明文图像和密文图像的R分量水平、垂直和对角方向分别随机选择10 000组相邻像素进行相关性测试,明文图像相邻像素分布集中,密文图像分散且均匀. 分别对明文和密文在水平、垂直和对角方向的所有相邻像素对做相关性测试,得到R、G、B分量相邻像素的相关系数如表1所示:明文图像相邻像素高度相关,相关系数接近于1;而密文图像相邻像素已基本不相关,相关系数接近于0,这表明原始图像的统计特征已经被扩散到随机的密文图像中了^[4].

表1 R、G、B分量相邻像素的相关系数

	R分量	G分量	B分量	文献[7]
水平明文	0.944 4	0.940 6	0.897 9	0.933 1
水平密文	-0.005 7	-0.000 58	0.002 3	0.006 4
垂直明文	0.970 7	0.972 5	0.944 1	0.967 5
垂直密文	-0.000 38	-0.001 5	-0.002 1	0.008 4
对角明文	0.920 3	0.925 0	0.858 2	0.923 9
对角密文	-0.002 4	-0.002 4	-0.001 3	0.010 7

表1最后一列为文献[7]算法加密前后的相关系数,通过对比说明本文算法的加密效果好于文献[7]算法的加密效果.

4.2.3 信息熵分析

信息熵是用来度量图像中的灰度值分布是否均匀的一个重要指标. 图像的信息熵越大,则图像灰度值就分布得越均匀. 信息熵的计算公式为

$$H(r) = - \sum_{i=0}^{2^N-1} p(r_i) \log_2 p(r_i) \quad (10)$$

式中, r 为信息源, N 为符号 r_i 的比特位数, $p(r_i)$ 是符号 r_i 出现的概率. 密文图像的理想信息熵为8,利用式(10)测得密文图像的R、G、B信息熵分别为7.989 0、7.990 2和7.990 3,说明密文图像所有的像素值出现概率基本一致.

4.2.4 差分分析

差分分析是明文敏感性测试的常用分析方法. 在随机地改变原始图像的某个像素值以后,像素数变化率NPCR是指加密图像像素值发生改变的数目所占的比例;归一化平均变化强度UACI是指像

素值的变化程度,如果明文图像的某个像素值的改变可以很大程度地改变加密图像,则说明该算法具有较强的抵抗差分攻击能力^[4],令两幅密文图像分别为 A 和 A' ,位置 (i, j) 处的像素值分别记为 $A(i, j)$ 和 $A'(i, j)$,则 NPCR 和 UACI 分别为

$$NPCR = \frac{\sum_{i=1}^M \sum_{j=1}^N D_{i,j}}{M \times N} \times 100\% \quad (11)$$

$$UACI = \frac{1}{M \times N} \left(\sum_{i=1}^M \sum_{j=1}^N \frac{C(i, j) - C'(i, j)}{255} \right) \times 100\% \quad (12)$$

本文中密文图像的理论值 $NPCR_{R,G,B}$ 为 99.609 4%, $UACI_{R,G,B}$ 为 33.463 5%^[8],每次对明文图像随机选择一个像素并使该像素的值加 1,获取密文图像后与原始密文图像进行对比,根据式(11)和式(12)获取 1 组值,在进行 200 组实验后计算得到各平均值为: $NPCR_R = 99.61\%$, $NPCR_G = 99.60\%$, $NPCR_B = 99.62\%$; $UACI_R = 33.43\%$, $UACI_G = 33.47\%$, $UACI_B = 33.49\%$. 文献[4]中 $NPCR = 99.75\%$, $UACI = 33.92\%$,本文算法结果比文献[4]得到的数据更接近于理论值.由此可知,稍微改变明文图像会引起密文图像显著变化,本文算法能够有效地抵御差分攻击.

5 结束语

本文利用改进 Lorenz 混沌序列和改进 Chen 混沌序列基于多轮扩散原理进行彩色图像加密,扩大了密钥空间,可以有效抵御穷举统计;每一位明文和密钥均影响到更多的密文位,解决了一位明文只能影响一位密文的问题,可以有效地抵御选择明文

攻击;加密后的图像像素分布均匀,相邻像素之间的相关性非常趋近于零,可以有效抵御统计攻击;原始图像的稍微变化会引起密文图像的明显变化,能够有效地抵御差分攻击.仿真实验表明该算法加密效果好,具有较高的安全性和实际应用价值.

参考文献:

- [1] Gao Haojiang, Zhang Yisheng, Liang Shuyun, et al. A new chaotic algorithm for image encryption [J]. Chaos, Solitons and Fractals, 2006, 29(2): 393-399.
- [2] 张云鹏,左飞.基于双 Logistic 变参数和 Chebychev 混沌映射的彩色图像密码算法[J].西北工业大学学报,2010,28(4):628-632.
- [3] 廖琪男.彩色图像加密及抗剪切攻击解密算法[J].计算机工程与设计,2011,32(2):509-516.
- [4] 王静,蒋国平.一种超混沌图像加密算法的安全性分析及其改进[J].物理学报,2011,60(6):1-11.
- [5] 赵怀勋,程甲.基于三维超混沌系统的彩色图像加密算法[J].微电子学与计算机,2010,27(2):72-74.
- [6] 朱从旭,孙克辉.对一类超混沌图像加密算法的密码分析与改进[J].物理学报,2012,61(12):120503.
- [7] 卢辉斌,孙艳.基于新的超混沌系统的图像加密方案[J].计算机科学,2011,38(6):149-152.
- [8] Rhouma R, Meherzi S, Belghith S. OCML-based colour image encryption [J]. Chaos, Solitons & Fractals, 2009, 40(1): 309-318.

作者简介:

柴秀丽 女,(1980—),博士,副教授.研究方向为混沌保密通信.

郭峻言 男,(1987—),硕士研究生,助理讲师.研究方向为混沌图像处理.