基于混沌与拟仿射的高效选择性彩色图像加密算法

杨耀森 李 博* 孟 浩
(中北大学仪器科学与动态测试教育部重点实验室 山西 太原 030051)

摘 要 一些传统的图像加密算法不仅计算量大,且在新型攻击方式下并不能提供安全保障。针对这些问题,提出一种更具安全性且轻量加密算法,结合数学模型拟仿射变换与混沌序列对彩色图像进行选择性加密。对明文图像进行分块,并计算每块的相关系数;与预定义的阈值相比,具有较大相关系数的块与斜帐篷映射生成的随机数进行异或运算;利用拟仿射生成的两种随机序列对图像进行重新排列。通过检测加密时间、相关系数、直方图、信息熵、秘钥敏感度等证明了该方案具有高效、安全的特性。

关键词 拟仿射变换 斜帐篷映射 图像加密 秘钥敏感度 信息熵

中图分类号 TP309 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.03.053

AN EFFICIENT SELECTIVE COLOR IMAGE ENCRYPTION ALGORITHM BASED ON CHAOS AND QUASI-AFFINE

Yang Yaosen Li Bo* Meng Hao
(*Laboratory of Instrument Science and Dynamic Testing, Ministry of Education, North University of China, Taiyuan 030051, Shanxi, China*)

Abstract Some traditional image encryption algorithms have great computation, and can not provide security under new attack methods. To solve these problems, this paper proposes a more secure and lightweight encryption algorithm, which combines the mathematical model of affine transformation and chaotic sequence to selectively encrypt color images. The plaintext image was divided into blocks, and the correlation coefficient of each block was calculated. Compared with pre-defined thresholds, XOR operations on the blocks with larger correlation coefficients and the random number generated by the skew tent map were performed. Finally, the image was rearranged using two random sequences generated by quasi-affine. The scheme is proved to be efficient and secure by detecting encryption time, correlation coefficient, histogram, information entropy and secret key sensitivity.

Keywords Quasi-affine transformation Skew tent map Image encryption Key sensitivity Information entropy

0 引 言

进入21世纪,图像数据在传输过程中的安全隐患越来越被人们所重视。以分组密码为代表的传统加密方法已经满足不了加密安全性的要求;公钥密码体制密钥长度过长,加密解密耗时。混沌系统因其非周期性、长期不可预测性契合密码学特点,成为图像加密中一种常用的方法[1-3]。文献[4]利用 logistic 系统迭代序列构建出一种彩色图像加密算法,其中创新点为对R、G、B 三通道分别进行加密,降低了各个成分之间的相关性,但该算法的密钥空间仅由 logistic 迭代周期与初值定义,减少了密钥空间,降低了加密的安全性能。为了扩充密钥,一些专家学者们围绕着 fridrich 提出的置乱扩散加密结构,提出了多级、高维混沌系统的加密算法。文献[5]提出将 annold 变换由二维转换到三维,通过提升 annold 维度来增强加密算法安全性。但随着密码分析技术的提高,经典的 arnold 置乱暴露出以下缺点:(1) annold 置乱局限在 $N \times N$ 像素的正方形数字图像上,然而现实中,多数的数字图像都是非方

收稿日期:2019-05-30。国家自然科学基金项目(61471325);山西省重点研发计划项目(201803D121061)。**杨耀森**,硕士生,主研领域:嵌入式开发,图像处理。**李博**,副教授。**孟浩**,硕士生。

形的。(2) 置乱速度慢,要进行至少 10 次以上置乱才可以掩盖图像纹理信息。(3) 由于 arnold 变换固有的周期性较短,单纯凭借置乱次数作为密钥非常容易被破解。为了进一步加强保密性能,文献[6]采用 arnold 置乱与 lorenz 扩散两种混沌系统相结合加密算法。文献[7]设计了一种基于 DNA 互补规则和混沌映射的图像加密方案。文献[8]提出基于动态随机增长技术的混沌块图像加密方案。文献[9]提出一种新的图像加密方案,该方案根据动态 S 盒的概念对图像进行加密。但是要在实时通信中使用所有这些算法,我们仍然需要提高加密方案的速度[10]。而解决这一问题的一个有效而快速的方法是更具体的基于选择性区域的图像加密,尤其是在高速传输的情况下,我们不需要加密所有的数据。

为了满足实时通信的需要,本文提出了一种高效、安全的图像选择性加密方案。具体为:将图像划分为若干块,计算每个块的相关系数,超过定义阈值的块将会与斜帐篷映射生成的随机值进行像素值的异或以去除图像像素之间的相关性。为了抵抗多次攻击,利用数学模型拟仿射变换对整个图像进行洗牌。通过对直方图、对比度、熵、相关度、密钥空间、密钥敏感度和抗差分攻击等方面进行分析,验证了该方案的安全性。该方案在各种安全通信应用中具有较强的实用性和鲁棒性。

1　拟仿射变换与混沌系统

1.1　拟仿射变换

图像加密算法中常用的是 arnold 变换。arnold 变换是一种线性变换,通过下式对像素点坐标(x,y)进行像素坐标的置乱。

$$\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}1&1\\1&2\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}\bmod N \tag{1}$$

arnold 变换复杂度不高,固有周期短,且秘钥空间小,安全性不高。故本文提出复杂度更高的拟仿射变换。

拟仿射变换是在仿射变换的基础上提出的,仿射变换一般形式:

$$\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}e\\f\end{pmatrix}\quad\begin{vmatrix}a&b\\c&d\end{vmatrix}\neq 0 \tag{2}$$

由式(2)可知,仿射变换也是一种线性变换,相比 arnold 变换,仿射变换加大了系数维度,引入了相位,复杂了置乱密码。但经仿射变换后参数不一定是整数,且在实际图像应用中图像尺寸大小有限,故需要在仿射变换的基础上限定(x,y)的取值范围并加入非线性取整操作,进而提出有限整数域的拟仿射变换(QATLIG)。QATLIG 的构造需要两个条件:

(1) 变换是离散点域$\{(x,y):0\leqslant x<M,0\leqslant y<N\}$到其自身的单映射。即对于不同的$(x,y)$,在映射集合中有不同的象。

(2) 变换是离散点域$\{(x,y):0\leqslant x<M,0\leqslant y<N\}$到其自身的满映射。即变换可逆。

由下列公式可知 QATLIG 分为两步:第一,需要对像素坐标进行线性提升变换;第二,确定好线性提升变换的次数,在最后一次线性变换后对相位参数进行四舍五入取整,即为新的像素坐标。

$$\begin{cases}\begin{pmatrix}\dot{x}\\\dot{y}\end{pmatrix}=\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}\quad\begin{vmatrix}a&b\\c&d\end{vmatrix}=\pm 1\\\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}(\dot{x}+round(e+0.5))\bmod N\\(\dot{y}+round(f+0.5))\bmod M\end{pmatrix}\end{cases} \tag{3}$$

对于式(3),如果$\begin{vmatrix}a&b\\c&d\end{vmatrix}=\pm 1$,且 a、b、c、d 为实数,(x,y)为整数,e、f 为实数,则满足 QATLIG 构造条件。$round(\ )$为取整函数,$\begin{pmatrix}e\\f\end{pmatrix}$为相位偏移量。mod 为取余函数,由于拟仿射变换添加了自适应取整参数,所以该变换为非线性。

值得一提的是,在变换计算过程避免不了负数坐标的结果,若不及时处理则会出现元素冲突情况。处理时,只需将负数 X 加上 N 或负数 Y 加上 M 即可。

解密过程即为拟仿射逆变换:

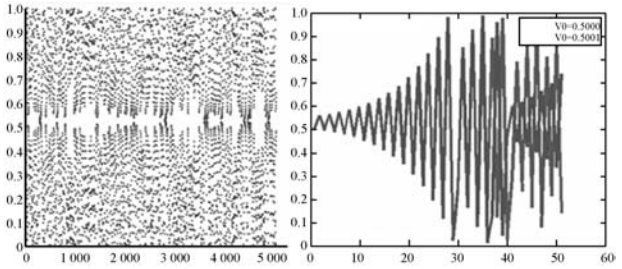
$$\begin{cases}\begin{pmatrix}\dot{x}\\\dot{y}\end{pmatrix}=\begin{pmatrix}x'-round(e+0.5)\\y'-round(f+0.5)\end{pmatrix}\\\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}a&b\\c&d\end{pmatrix}^{-1}\begin{pmatrix}\dot{x}\\\dot{y}\end{pmatrix}\bmod\begin{pmatrix}N\\M\end{pmatrix}\quad\begin{vmatrix}a&b\\c&d\end{vmatrix}=\pm 1\end{cases} \tag{4}$$

1.2　混沌系统

混沌系统具有非周期性,遍历性和对初值的敏感性三大特性。故将混沌系统用于图像加密具有保密性强、随机性好、秘钥空间大等优势,同时具有良好的抗干扰性、抵御攻击的能力。本文在进行灰度扩散时使用斜帐篷混沌映射。其动力学方程为:

$$V_{n+1}=f(V_n,r)=\begin{cases}\dfrac{V_n}{r} & V_n\in[0,r]\\[2ex]\dfrac{(1-V_n)}{(1-r)} & V_n\in[r,1]\end{cases} \tag{5}$$

式中：$V_n \in [0,r]$定义了混沌系统的状态，$r \in (0,1)$作为混沌系统的控制参数。式(5)对任意控制参数 $r \in (0,1)$具有正的 Lyapunov 指数，因此，由式(5)定义的映射总是表现出混沌行为[11]。图 1 显示了斜帐篷映射的随机性和密钥敏感性。



(a) 随机性 (b) 敏感性

图 1 斜帐篷映射

2 图像加密算法

算法的流程如图 2 所示。

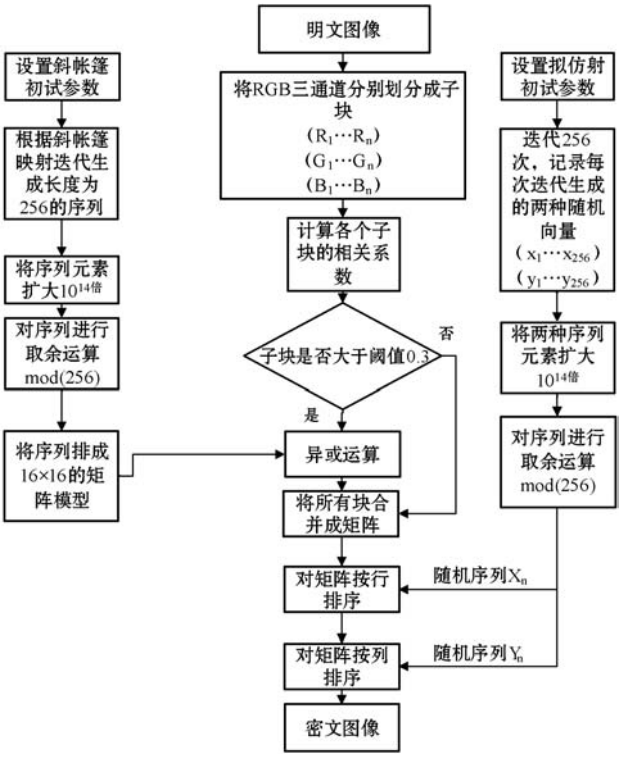


图 2 加密流程图

具体步骤如下：

定义图像为 $\boldsymbol{P}$，矩阵大小为 $m \times n$，则 $\boldsymbol{P}$ 可分割成红、绿、蓝三种颜色的像素矩阵，分别定义为 $\boldsymbol{R}$、$\boldsymbol{G}$、$\boldsymbol{B}$。大小同为 $m \times n$，本文中 $m = n = 256$。

步骤 1 分别将 $\boldsymbol{R}$、$\boldsymbol{G}$、$\boldsymbol{B}$ 分割成大小为 16 × 16 的子块，每个通道有 256 个子块。

$$\boldsymbol{R} = [R_1, R_2, R_3, \cdots, R_{256}]$$

$$\boldsymbol{G} = [G_1, G_2, G_3, \cdots, G_{256}]$$

$$\boldsymbol{B} = [B_1, B_2, B_3, \cdots, B_{256}]$$

计算 $\boldsymbol{R}$、$\boldsymbol{G}$、$\boldsymbol{B}$ 中每个块的相关系数，并将阈值定义为 T，本文中 $T = 0.3$。

步骤 2 设置三种不同的斜帐篷映射的初始条件，即：

$$\begin{cases} r = 0.200\ 0 & V_0 = 0.600\ 0 \\ r = 0.300\ 0 & V_0 = 0.500\ 0 \\ r = 0.400\ 0 & V_0 = 0.700\ 0 \end{cases}$$

根据三种不同的初始条件分别迭代 256 次以生成长度为 256 随机序列 $\boldsymbol{V_R}$、$\boldsymbol{V_G}$、$\boldsymbol{V_B}$。

由于序列元素是分布在(-1,1)上的浮点型实数[12]。为了减少浮点型计算，将随机序列中的元素都与 10^{14} 相乘得到序列 $\boldsymbol{V'_R}$、$\boldsymbol{V'_G}$、$\boldsymbol{V'_B}$，并对三种不同序列进行取模运算以获得 0 到 256 范围内的随机数，运算公式如下：

$$Y = Modulo(V', 256)$$

将新的随机序列以矩阵形式排列得到 $\boldsymbol{Y_R}$、$\boldsymbol{Y_G}$、$\boldsymbol{Y_B}$，大小同为 16 × 16。

将 $\boldsymbol{R}_p$、$\boldsymbol{G}_p$、$\boldsymbol{B}_p$ 相关系数大于 T 的明文图像块分别与矩阵 $\boldsymbol{Y_R}$、$\boldsymbol{Y_G}$、$\boldsymbol{Y_B}$ 按位做异或运算：

$$diffuse_{\boldsymbol{R}_n} = bitxor(\boldsymbol{R}_n, \boldsymbol{Y_R})$$

$$diffuse_{\boldsymbol{G}_n} = bitxor(\boldsymbol{G}_n, \boldsymbol{Y_G})$$

$$diffuse_{\boldsymbol{B}_n} = bitxor(\boldsymbol{B}_n, \boldsymbol{Y_B})$$

n 为块的序号，$diffuse_{\boldsymbol{R}_n}$、$diffuse_{\boldsymbol{G}_n}$、$diffuse_{\boldsymbol{B}_n}$ 是新的扩散块，$bitxor$ 为异或运算函数。

将三通道所有块重新组合起来，得到扩散图像 $\boldsymbol{P}_{\text{diffuse}}$。

步骤 3 定义拟仿射变换的初始条件 $a = 7.400\ 0$，$b = -6.400\ 0$，$c = -3.162\ 5$，$d = 2.600\ 0$，$e = 1.611\ 5$，$f = 3.274\ 5$。

根据式(4)迭代 256 次，记录每次迭代生成的两种随机向量。

$$\boldsymbol{x}_n = [x_1, x_2, x_3, \cdots, x_{256}]$$

$$\boldsymbol{y}_n = [y_1, y_2, y_3, \cdots, y_{256}]$$

由于在式(4)中进行了取模运算，所以序列分布在图像面积区间内，即：$0 \leqslant \boldsymbol{x}_n \leqslant N$，$0 \leqslant \boldsymbol{y}_n \leqslant M$。

扩散图像 $\boldsymbol{P}_{\text{diffuse}}$ 通过行向量 $\boldsymbol{x}_n$ 按行排序。例如，如果 $\boldsymbol{P}_{\text{diffuse}}$ 和随机行向量 $\boldsymbol{x}_n$ 为：

$$\boldsymbol{P}_{\text{diffuse}} = \begin{pmatrix} P_{11} & P_{12} & \cdots & P_{1N} \\ P_{21} & P_{22} & \cdots & P_{2N} \\ \vdots & \vdots & & \vdots \\ P_{M1} & P_{M2} & \cdots & P_{MN} \end{pmatrix} \tag{6}$$

$$\boldsymbol{x}_n = [256 \quad 2 \quad \cdots \quad 1] \tag{7}$$

则按行排序后的图像 $\boldsymbol{P}_{\text{diffuse}}^{\text{row}}$ 为:

$$\boldsymbol{P}_{\text{diffuse}}^{\text{row}} = \begin{pmatrix} P_{M1} & P_{M2} & \cdots & P_{MN} \\ P_{21} & P_{22} & \cdots & P_{2N} \\ \vdots & \vdots & & \vdots \\ P_{11} & P_{12} & \cdots & P_{1N} \end{pmatrix} \tag{8}$$

同样,使用随机向量 $\boldsymbol{y}_n$ 对 $\boldsymbol{P}_{\text{diffuse}}^{\text{row}}$ 按列排序,得到最终密文图像 $\boldsymbol{P}_{\text{Ciphertext}}$。

解密过程为加密的逆过程,将步骤按相反的顺序执行即可从密文图像中获得原始明文图像。

3　实验结果分析

3.1　QATLIG 周期测试

QATLIG(a,b,c,d,e,f) 关于 $N \times M$ 的周期 T 是指当图像 A 的任意两个像素没有相同的颜色值时,使得 A 经重复同一变换后又回复到 A 的最小变换次数。T 越大,则安全性能就越高。测试结果如表 1 所示。

表 1　不同像素尺寸的周期比较

N	6	7	25	100	256	512
T_1	12	8	50	150	192	384
T_2	140	475	415 901 640	—	—	—

N 代表像素尺寸大小。周期越长,安全性越高。T_1 为 arnold 变换的最小周期,T_2 为拟仿射变换的最小周期。从表中数据可知 QATLIG 变换用于像素的重新排列具有较好的效果。

3.2　加密时间测试

本文在 Windows 7 操作系统上使用 Intel Core i5-6600 CPU@3.30 GHz 和 8.0 GB RAM 对加密时间进行测试。表 7 表明,与文献[13]、文献[14]算法相比,该方案的加密时间要短得多。这些传统算法的工作原理与 AES 非常相似,后者通常执行循环加密,需要很多时间。然而,本文方案是一种单轮图像加密方案,可用于实时在线通信。

表 2　时间分析　　s

加密系统	图像类型	加密时间
文献[14]	彩色图像	8.22
文献[13]	彩色图像	4.57
本文	彩色图像	0.55

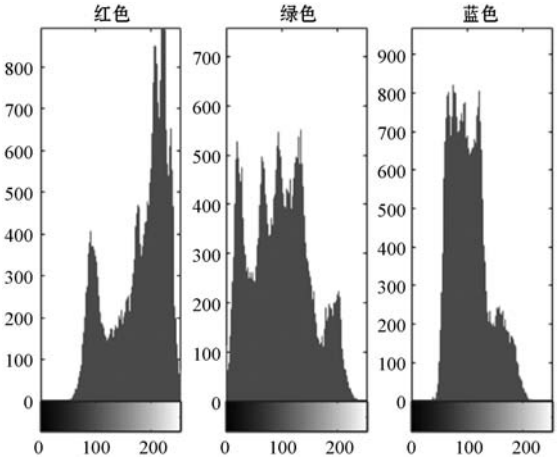
3.3　直方图分析

按照本文算法对 lena 图像进行仿真。结果如图 3 所示。

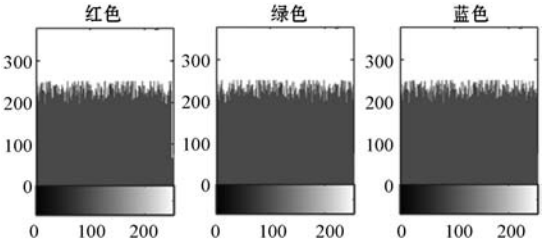
(a) 明文图像　　(b) 密文图像

图 3　加密图像

加密前后 $\boldsymbol{R}$、$\boldsymbol{G}$、$\boldsymbol{B}$ 分量直方图对比如图 4 所示。



(a) 加密前



(b) 加密后

图 4　R、G、B 直方图

由图 3(b)得知经过该比特量化扩散算法,在减少计算量的前提下,密文图像看不出原始图像任何信息,达到了扩散的效果。从图 4 直方图中我们发现加密前后直方图的变化巨大,并且加密后图像的像素值分布得非常均匀,攻击者无法看出原始图像的分布规律,有效地抵制了攻击者的破译。

4　安全性能分析

本文从密钥空间、密钥敏感度分析、信息熵、相关性分析四个角度对加密图像的安全性能进行了测试。

4.1 密钥空间

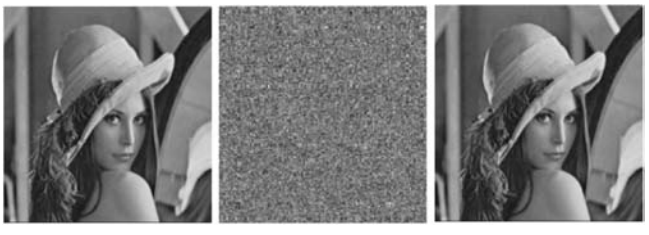
图像加密方案的密钥空间必须至少为 2^{100} 或更大[13],以抵抗暴力攻击。本文采用 8 个密钥进行加密,包括 6 个拟仿射变换,其中 5 个可以选用随机数,另 1 个由约束条件确定,斜帐篷映射为 2 个根据 IEEE 浮点标准,64 位双精度计算精确度为 10^{15}。本文密钥空间如表 3 所示。可以看出,密钥空间为 $2\times10^{15\times7}=2\times10^{105}\approx2^{351}$,远大于文献[13]密钥空间要求。现有的 64 位机器无法通过穷举法进行破译[13]。

表 3 密钥空间

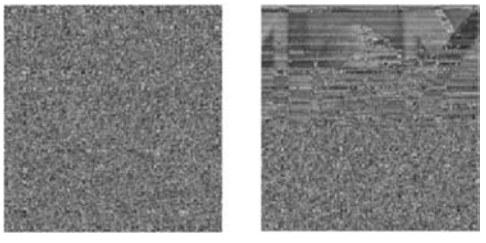
加密系统	密钥	密钥空间
文献[14]	K,x_0,k	1.156×10^{50}
文献[13]	x_0,y_0,λ	$6.553\,6\times10^{48}$
本文	a,b,c,d,e,f,v_0,r	2×10^{105}

4.2 密钥敏感度分析

在解密过程中,微改变密钥初值 v_0,即 $v_0=v_0+10^{-12}$,其余密钥保持不变,则解密完全失败,如图 5(d)所示。由于本文算法扩充了密钥空间,而减少了单个密钥精度上的计算量,当精确度达到 10^{-13},如图 5(e)所示,图像开始出现纹理信息。本文对单个密钥的敏感性精度可达 10^{-12},足够抵御穷举攻击。



(a) 明文图像 (b) 加密图像 (c) 解密正确图像



(d) $v_0=v_0+10^{-12}$ (e) $v_0=v_0+10^{-13}$

图 5 敏感度分析

4.3 信息熵

信息熵反映了图像中平均信息量的多少,通过信息熵可以判断一幅图像的随机性。对于一幅图像,灰度值分布得越均匀,图像的信息熵就越大,信息熵越接近于 8,图像的随机性越强[15]。

信息熵计算公式为:

$$H(m)=-\sum_{i=1}^{255}P(x_i)\log_2P(x_i) \tag{9}$$

式中:$P(x_i)$ 表示 $\boldsymbol{R}$、$\boldsymbol{G}$、$\boldsymbol{B}$ 某个分量出现的概率。

由表 4 数据可知,本文算法加密后的 $\boldsymbol{R}$、$\boldsymbol{G}$、$\boldsymbol{B}$ 各个分量值都接近于 8,且平均值高于文献[15-16],证明本文算法加密后的各个像素点具有很强的随机性,具有良好的抵御攻击的能力。

表 4 密文图像信息熵

信息熵	$\boldsymbol{R}$	$\boldsymbol{G}$	$\boldsymbol{B}$
文献[15]	7.941 3	7.791 6	7.695 4
文献[16]	7.998 2	7.692 6	7.524 1
本文	7.997 8	7.994 7	7.996 7

4.4 相关性分析

一幅完整的图像相邻的像素点具有较强的相关性,为了检验本文算法打乱相关性的性能,随机选择明文和密文图像水平、垂直、对角方向各 1 000 对像素点[16],计算相关性系数,公式如下:

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{10}$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{11}$$

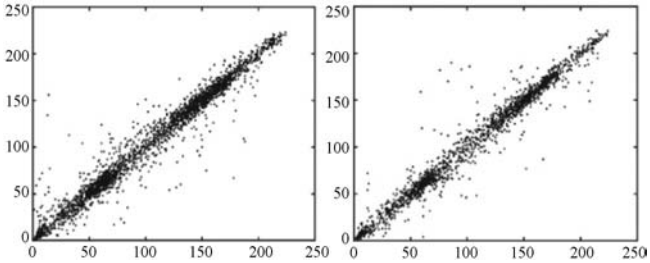
式中:$\operatorname{cov}(x,y)$ 表示相关系数,x_i、y_i 为像素值。

从表 5 中可知,明文图像具有较强的相关性。经过本文算法加密后,相关性不足 0.01,表明密文图像各个像素点基本无相关性。

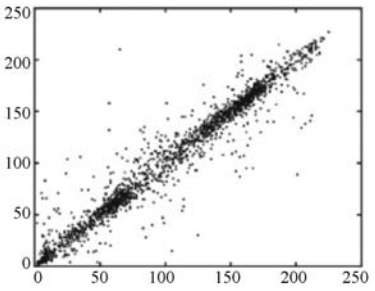
表 5 图像相关性

信道	明文图像			密文图像		
	水平	垂直	对角	水平	垂直	对角
R	0.987 3	0.991 6	0.9593	0.005 2	0.003 2	0.007 4
G	0.963 4	0.976 7	0.952 3	0.001 3	0.023 7	0.008 7
B	0.931 6	0.924 3	0.935 1	0.015 6	0.001 7	0.009 5

图 6、图 7 给出了加密前后 $\boldsymbol{R}$ 通道的相关性对比图。

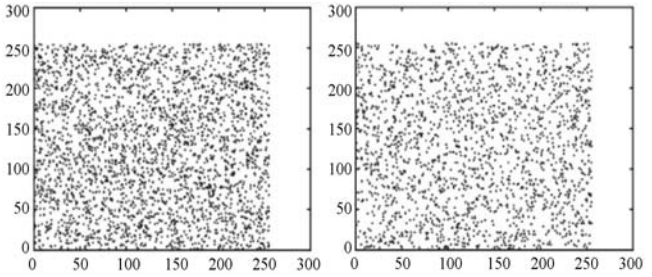


(a) 水平方向 (b) 垂直方向

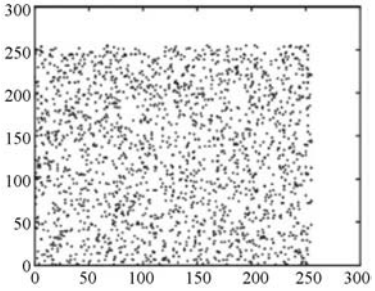


(c) 对角方向

图 6　加密前 R 通道相关性



(a) 水平方向　　(b) 垂直方向



(c) 对角方向

图 7　加密后 R 通道相关性

4.5　抗差分攻击能力分析

差分攻击是通过比较分析有特定区别的明文在通过加密后的变化传播情况来攻击密码算法的。算法对明文的敏感性越强,抗差分攻击能就越强。本文通过像素改变率(NPCR)与归一化像素值平均改变强度(UACI)测试加密算法对名明文图像的敏感性[17]。

$$NPCR = \frac{1}{m \times n}\sum_{i,j} D(i,j) \tag{12}$$

$$UACI = \frac{1}{m \times n}\left[\sum_{i,j}\frac{X(i,j) - X'(i,j)}{255}\right] \tag{13}$$

式中:$X(i,j)$表示原密文像素值,$X'(i,j)$表示新密文的像素值。当 $X(i,j)$ 与 $X'(i,j)$ 相同时 $D(i,j)$ 等于 0,否则等于 1。本文随机选取一个明文图像像素点计算得出密文像素值 $X_1(i,j)$,对选取的明文像素点进行微调,计算得出新密文像素值 $X'_1(i,j)$。在进行 100 组测试之后,计算得出 NPCR 与 UACI 平均值如表 6 所示[18]。

表 6　NPCR 与 UACI 测量结果

度量值	信道	文献[17]	文献[18]	本文算法
NPCR	R	0.991 3	0.993 7	0.995 7
	G	0.995 1	0.994 1	0.994 6
	B	0.992 1	0.991 6	0.993 7
UACI	R	0.330 4	0.331 2	0.332 6
	G	0.332 6	0.331 9	0.335 3
	B	0.331 7	0.333 2	0.334 9

由表 6 可知 $\boldsymbol{R}$、$\boldsymbol{G}$、$\boldsymbol{B}$ 分量 NPCR 平均值都超过 0.99,UACI 平均值超过 0.33,并且超越了文献中 NPCR 与 UACI 的平均值。该结果表明即使对原文图像做一点细微的变化,计算得出的密文图像也有明显的差异,即本文算法具有更强的抗差分攻击能力。

5　结　语

本文提出了一种快速、高效、安全的基于 QATLIG 与混沌映射的选择性加密方案。与已有的算法相比,本文算法对两个方面进行了提升。其一是该方案通过相关系数参数决定了对哪个块进行加密,只有那些具有最大相关系数值的块与斜帐篷图生成的随机值逐像素异或,加快了加密的速度。其二在混淆过程中,利用拟仿射模型对异或运算后得到的图像分别按行和列顺序进行洗牌,补充了密钥空间,加强了保密性能。实验数据表明,该算法优势在于密钥空间大,运算量小,但对于密钥敏感度精确度仍有可提升的空间。加密后的图像像素值分布均匀,信息熵接近于 8,能够很好地抵御攻击。

参　考　文　献

[1] 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):89 - 99.

[2] 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):76 - 87.

[3] 朱淑芹,王文宏,孙忠贵. 对一种基于比特置乱的超混沌图像加密算法的选择明文攻击[J]. 计算机科学,2017,44(11):273 - 278.

[4] 陈善学,唐义嫄. 基于混沌系统的 RGB 彩色图像三重置乱算法[J]. 重庆邮电大学学报(自然科学版),2018,30(6):812 - 818.

[5] Chen G, Mao Y, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals, 2004, 21(3):749 - 761.

[6] 李云. 基于高维混沌系统组合的图像加密新算法[J]. journal6, 2006, 45(1):103 - 104.

[7] Liu H, Wang X, Kadir A. Image encryption using DNA complementary rule and chaotic maps[J]. Applied Soft Computing, 2012, 12(5):1457 - 1466.
[8] Wang X, Liu L, Zhang Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique[J]. Optics and Lasers in Engineering, 2015, 66:10 - 18.
[9] Rehman A U, Khan J S, Ahmad J, et al. A New Image Encryption Scheme Based on Dynamic S-Boxes and Chaotic Maps[J]. 3D Research, 2016, 7(1):84.
[10] Wang X Y, Bao X M. A novel block cryptosystem based on the coupled chaotic map lattice[J]. Nonlinear Dynamics, 2013, 72(4):707 - 715.
[11] Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems[J]. International Journal of Bifurcation and Chaos, 2006, 16(08):2129 - 2151.
[12] Li C, Li S, Lo K T. Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps[J]. Communications in Nonlinear Science and Numerical Simulation, 2011, 16(2):837 - 843.
[13] Ayoup A M, Hussein A H, Attia M A A. Efficient selective image encryption[J]. Multimedia Tools and Applications, 2016, 75(24):17171 - 17186.
[14] Ullah I, Iqbal W, Masood A. Selective region based images encryption[C]//2013 2nd National Conference on Information Assurance(NCIA). IEEE, 2013.
[15] Lei L H, Bai F M, Han X H. New image encryption algorithm based on logistic map and hyper-chaos[C]//2013 International Conference on Computational and Information Sciences. IEEE, 2013.
[16] Huang H, Yang S. Colour image encryption based on logistic mapping and double random-phase encoding[J]. IET Image Processing, 2017, 11(4):211 - 216.
[17] Xiao D, Liao X, Wei P. Analysis and improvement of a chaos-based image encryption algorithm[J]. Chaos, Solitons and Fractals, 2009, 40(5):2191 - 2199.
[18] Khan J S, Ahmad J, Khan M A. TD-ERCS map-based confusion and diffusion of autocorrelated data[J]. Nonlinear Dynamics, 2017, 87:93 - 107.

(上接第 285 页)

基于上述分析,K 值和 d 值在一定范围内变化,最终预测效果不是很大。对于有限的实验条件,可以选择小 K 值和 d 值(尤其是 K 值)来加快模型训练。

4 结 语

针对当前推荐系统冷启动问题导致的推荐效果不准确问题,本文提出了一种融合标签信息的卷积矩阵分解推荐算法 TaSoConvMF。该算法使用卷积神经网络处理资源文档特征,利用标签矩阵和评分矩阵挖掘用户和资源的隐含关联,利用误差逆向传播与坐标下降法对算法进行模型求解。通过在 DoubanSet 等数据集上的多组实验,验证了 TaSoConvMF 算法预测的准确性,并且给出了参数选择上的优选方案。

参 考 文 献

[1] Marz N, Warren J. Big data: Principles and best practices of scalable realtime data systems[M]. Manning Publications Co, 2015.
[2] 欧辉思,曹健. 面向跨领域的推荐系统研究现状与趋势[J]. 小型微型计算机系统,2016,37(7):1411 - 1416.
[3] 高玉凯,王新华,郭磊,等. 一种基于协同矩阵分解的用户冷启动推荐算法[J]. 计算机研究与发展,2017,54(8):1813 - 1823.
[4] 秦晓晖. 基于协同过滤的个性化微博推荐算法研究[J]. 软件工程,2017,20(3):14 - 17.
[5] 吴燎原,蒋军,王刚. 科研社交网络中基于联合概率矩阵分解的科技论文推荐方法研究[J]. 计算机科学,2016,43(9):213 - 217.
[6] 满彤,沈华伟,黄俊铭,等. SCMF:一种融合多源数据的软约束矩阵分解推荐算法[J]. 中文信息学报,2017,31(4):174 - 183.
[7] Salakhutdinov R, Mnih A, Hinton G. Restricted Boltzmann machines for collaborative filtering[C]//Proceedings of the 24th international conference on Machine learning. ACM, 2007: 791 - 798.
[8] Wang C, Blei D M. Collaborative topic modeling for recommending scientific articles[C]//Acm Sigkdd International Conference on Knowledge Discovery & Data Mining. ACM, 2011.
[9] Wang H, Wang N, Yeung D Y. Collaborative deep learning for recommender systems[C]//Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2015:1235 - 1244.
[10] Huang L W, Qu H, Zuo L. Multi-type UAVs cooperative task allocation under resource constraints[J]. IEEE Access, 2018, 6:17841 - 17850.
[11] 张维玉,吴斌,耿玉水,等. 基于协同矩阵分解的评分与信任联合预测[J]. 电子学报,2016,44(7):1581 - 1586.
[12] Wu Y, Hu J. Observer-based output regulation of cooperative-competitive high-order multi-agent systems[J]. Journal of the Franklin Institute, 2018,355(10):4111 - 4130.
[13] Zheng D X, Xiong Y H. A unified probabilistic matrix factorization recommendation algorithm[C]//2018 International Conference on Robots & Intelligent System(ICRIS). IEEE, 2018.