DOI:10.11721/cqnuj20240103

一种基于 Kolmogorov 方程与 ICMIC 的图像加密方案*

关至轩，胡金涛，田红炯
(上海师范大学 数理学院 数学系，上海 200234)

摘要:针对图像传输的安全性问题,利用 Kolmogorov 方程解的 Markov 性以及无限折叠的迭代混沌映射(iterative chaotic map with infinite collapses,ICMIC)的混沌性,提出了一种可以抵御选择明文攻击的对称加密方案。首先通过设置 Kolmogorov 方程的系数矩阵与初始状态作为密钥参数产生转移概率矩阵,其次将转移概率矩阵输入 ICMIC 并由得到的结果确定密钥序列,最后由密钥序列与明文图像做模 2 加法运算生成密文图像。通过 Matlab 程序对加密方案进行实验仿真,密文图像信息熵为 7.99 以上,NPCR 值超过 99%,UACI 值超过 33%。实验结果表明该加密方案具有较高安全性,可以有效抵御统计攻击与差分攻击等。

关键词:图像加密;Markov 过程;Kolmogorov 方程;ICMIC
中图分类号:TP309.7 **文献标志码**:A **文章编号**:1672-6693(2024)01-0109-09

随着数字图像的广泛运用,图像传输的安全性受到关注,尤其是在国防、商业、医学等特殊领域,对图像保密性有着较高要求。所以,对图像加密方法的研究有着重要意义。目前常用的图像加密方法有矩阵变换[1-2]、DNA 编码[3]、图像位平面加密[4]以及光学加密[5]等等。而混沌系统因初值敏感与长期不可预测性、类随机性、整体稳定、局部不稳定性[6]等特点,能够有效实现密钥对明文的影响扩散到多个密文信息中,所以被更加广泛地应用于图像加密领域。

1989 年,Matthews[7]首次提出了“混沌密码”的概念,利用一维 Logistic 混沌系统设计出一种新的加密方法;1997 年,Fridrich[8]将混沌理论运用到图像加密领域,开创了混沌理论与图像加密相结合的先河。同样,国内学者也发现混沌理论在图像加密中的优势,并结合其他技术与理论提出了一系列新的图像加密方法[9-14]。2006 年,Peng 等人[15]提出了基于复合混沌系统的图像加密方案,并从密钥敏感性与明文敏感性等方面对提出的加密方案进行分析,验证了加密方案的安全性。2019 年,Shi 等人[16]提出了一种基于压缩感知和多维混沌系统的多过程图像加密方案。2020 年,Chen 等人[17]提出了一种基于深度学习压缩感知与复合混沌系统的通用图像加密方案,该方案相较于 Shi 等人提出的加密方案,在信息熵、明文敏感性等方面取得了更好的结果。

目前,基于混沌理论的图像加密方法主要使用混沌系统直接生成密钥,进而产生密文图像。该方法的缺陷是明文与密文存在较强相关性,容易遭受编码攻击。Duan 等人[18]于 2009 年提出了一种基于 Markov 性质的一阶安全算术编码方法并应用于图像加密领域,可以有效抵御从编码角度的攻击。本文在上述研究的基础上提出了一种基于 Kolmogorov 方程与 ICMIC 的加密方案,通过设置 Kolmogorov 方程的系数矩阵与初始状态作为密钥参数产生转移概率矩阵,然后将转移概率矩阵输入 ICMIC 并由输出结果确定密钥序列。相较于 Duan 等人的研究,本文所提加密方案的创新点在于决定密钥序列元素的方式是由一个关于转移概率微分方程的解所决定的,并且将微分方程的参数作为密钥参数发送给接收方,使得整个加密过程与解密过程较为简洁,而且相较于传统的由密钥参数直接决定密钥序列的加密算法,本文提出的加密算法的密钥序列由密钥参数通过转移概率决定,减弱了密钥参数与密钥序列的关联,算法的安全性得到进一步提高。本文通过灰度直方图、相关性分析、信息熵、明文敏感性、密钥空间以及密文敏感性等方面对加密方案进行了分析,实验结果表明,所提加密方案具有较高安全性。

* **收稿日期**:2022-10-13 **修回日期**:2023-11-21 **网络出版时间**:2023-06-20T13:52
资助项目:国家自然科学基金面上项目(No. 12271368)
第一作者简介:关至轩,男,研究方向为动力系统与序列密码,E-mail:1186604684@qq.com;**通信作者**:田红炯,男,教授,E-mail:hjtian@shnu.edu.cn
网络出版地址:https://link.cnki.net/urlid/50.1165.N.20230620.1009.005

1 基础知识

1.1 图像加密模型

图像加密模型由待加密图像(明文图像)、加密方案、解密算法、加密图像(密文图像)以及密钥构成。设明文图像为 M,加密方案为 E_{k_1},解密算法为 E_{k_2},密文图像为 C,加密密钥为 k_1 与解密密钥 k_2。加密过程为:1) 发送方将明文图像 M 通过加密密钥 k_1 与加密方案 E_{k_1} 得到密文图像 $C=E_{k_1}(M)$;2) 发送方将密文图像 C 通过信道传输给接收方。解密过程为:1) 接受方收到密文图像 C;2) 接收方通过解密算法 E_{k_2} 与解密密钥 k_2 得到明文图像 $M=E_{k_2}(C)$。

需要特别指出的是,当加密密钥与解密密钥满足 $k_1=k_2$ 时,将该加密方案称为对称加密方案,反之称为非对称加密方案。图像加密模型的流程如图1所示。

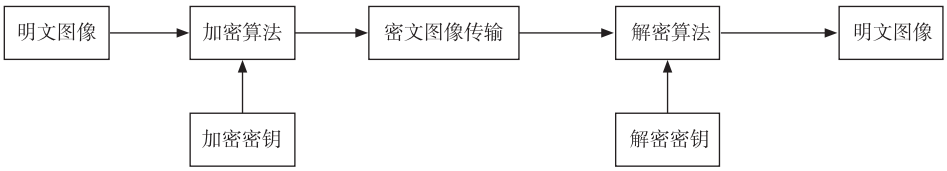


图1 图像加密流程

Fig. 1 Image encrytion flow chart

1.2 混沌系统

混沌是确定性系统中呈现的一种类随机性行为,当输入的初始值有微小的差异时,得到的输出值有较大的差异[19]。本文用到的混沌系统是2001年由 He 等人[20]首次提出的 ICMIC,定义为:

$$x_{n+1}=\sin\frac{a}{x_n}, \tag{1}$$

并且满足 $x_n\in[-1,0)\cup(0,1]$。若系统存在大于0的 Lyapunov 指数,则说明该系统具有混沌性。图2是参数 a 与 Lyapunov 指数的关系,可以看出,ICMIC 的 Lyapunov 指数在一定参数范围内存在混沌性。图3是 ICMIC 的分岔图,同样也可以看出 ICMIC 具有混沌性。

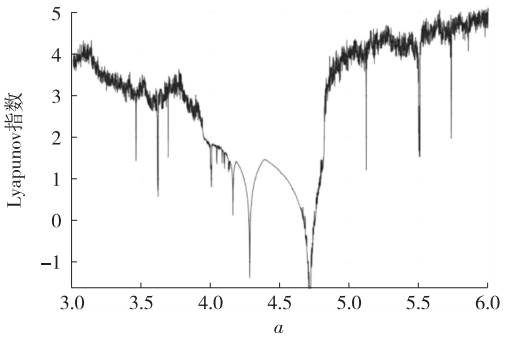


图2 ICMIC 的参数与 Lyapunov 指数的关系

Fig. 2 Relationship between ICMIC parameters and Lyapunov exponent

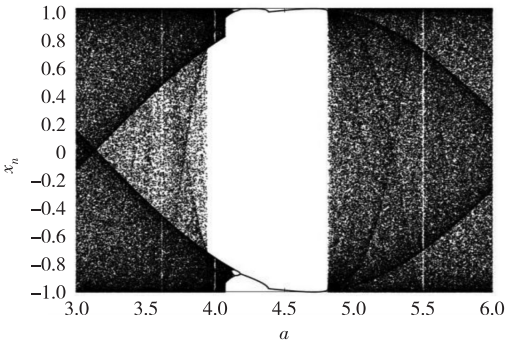


图3 ICMIC 的分岔图

Fig. 3 Bifurcation diagram of ICMIC

1.3 Markov 过程

设$(\Omega,\mathcal{F},P)$为概率空间,T 是给定的参数集,$\{X(t,\omega)\}_{t\in T}$ 为定义在$(\Omega,\mathcal{F},P)$上的随机过程,可以简记为 $\{X(t)\}_{t\in T}$ 或$\{X_t\}_{t\in T}$。φ 为$\{X_t\}_{t\in T}$ 的状态空间($X_t\in\varphi,t\in T$)。如果$\{X_t\}_{t\in T}$ 满足:

$$P(X_{t+1}\mid X_t,\cdots,X_1)=P(X_{t+1}\mid X_t), \tag{2}$$

则称随机过程$\{X(t)\}_{t\in T}$ 是一个 Markov 过程。对于齐次 Markov 过程(与 t 无关),设:

$$p(s,t;i,j)=P(X_t=k\mid X_s=i),s\leqslant t,i,j\in\varphi,$$

则齐次 Markov 过程的转移概率可以记为 $p(s,t;i,j)=p_{ij}(t-s)$,对于任意的 $s\leqslant\tau\leqslant t$,转移概率满足:

$$p(s,t;i,j)=\sum_{k\in\varphi}p(s,\tau;i,k)p(\tau,t;k,j), \tag{3}$$

称上式为 Chapman-Kolmogorov 方程，简称 C-K 方程。

设 $\boldsymbol{P}(t-s)=(p_{ij}(t-s))$ 为转移概率矩阵。当初始时刻 t 为 0 时，由式(3)可以得到：

$$\boldsymbol{P}(s)\boldsymbol{P}(t)=\boldsymbol{P}(s+t)。\tag{4}$$

由文献[21]可知，在一定条件下，由式(4)可以得到关于转移概率矩阵 $\boldsymbol{P}(t)$ 的微分方程：

$$\begin{cases}\boldsymbol{P}'(t)=\boldsymbol{P}(t)\boldsymbol{Q},\\ \boldsymbol{P}(0)=\boldsymbol{I}。\end{cases}\tag{5}$$

称上式为 Kolmogorov 微分方程，其中系数矩阵 $\boldsymbol{Q}=(q_{ij})$ 满足保守性[21]。加密方案用到的系数矩阵 $\boldsymbol{Q}=\begin{pmatrix}-\lambda & \lambda\\ \mu & -\mu\end{pmatrix}$，其中：$\lambda,\mu\in(0,+\infty)$。

2　算法描述

2.1　加密过程

加密具体步骤如下：

步骤 1，选择一个大小为 $M\times N$ 的明文图像，像素矩阵为 $\boldsymbol{P}$。并设置系数矩阵 $\boldsymbol{Q}$，时间参数 t 以及密钥序列首位元素 z_0 的状态(z_0 可取 0 或 1)。

步骤 2，由系数矩阵 $\boldsymbol{Q}$ 得到 Kolmogorov 方程：

$$\begin{pmatrix}p'_{00}(t) & p'_{01}(t)\\ p'_{10}(t) & p'_{11}(t)\end{pmatrix}=\begin{pmatrix}p_{00}(t) & p_{01}(t)\\ p_{10}(t) & p_{11}(t)\end{pmatrix}\begin{pmatrix}-\lambda & \lambda\\ \mu & -\mu\end{pmatrix},\tag{6}$$

求解此方程，得到在时间 $(i+1)t$ 下的转移概率 $P(z_{i+1}=1|z_i)$，$P(z_{i+1}=0|z_i)$，其中 $i=0,1,\cdots,M\times N-1$。

步骤 3，设置参数 a，将像素矩阵 $\boldsymbol{P}$ 的所有元素相加 $\sum\limits_{i=M}\sum\limits_{j=N}P_{ij}$，再将转移概率输入下式：

$$T_{n+1}=\sin\frac{a}{\left(\sum\limits_{i}\sum\limits_{j}P_{ij}\right)\times T_n},\tag{7}$$

并进行 M 次迭代，最后取绝对值得到 $P^*(z_{i+1}=1|z_i)$，$P^*(z_{i+1}=0|z_i)$。

步骤 4，设置随机数序列 $R=r_0r_1\cdots r_{M\times N-1}(r_{i+1}\in(0,1))$，计算

$$|P^*(z_{i+1}=1|z_i)-r_{i+1}|\text{ 与 }|P^*(z_{i+1}=0|z_i)-r_{i+1}|,$$

若 $|P^*(z_{i+1}=1|z_i)-r_{i+1}|\leqslant|P^*(z_{i+1}=0|z_i)-r_{i+1}|$，则 $z_{i+1}=1$，反之 $z_{i+1}=0$。

步骤 5，由步骤 1、2、3 和 4 得到密钥序列 $Z=z_0z_1\cdots z_{M\times N-1}$。将像素矩阵的每个元素用 8 位二进制数表示，再转换为序列得到明文序列 $X=x_0x_1\cdots x_{M\times N-1}$。

步骤 6，通过将明文序列的每个元素与密钥序列中对应的元素做模 2 加法运算 $y_i=z_i+x_i \bmod 2$，得到密文序列 $Y=y_0y_1\cdots y_{M\times N-1}$。

步骤 7，把密文序列传输给接收方，并将密钥参数 $K=\{\boldsymbol{Q},t,M,a,\sum\limits_{i=M}\sum\limits_{j=N}P_{ij},R\}$ 通过安全信道传输给接收方。

2.2　解密过程

解密具体步骤如下：

步骤 1，接收密文序列与密钥参数。

步骤 2，由加密过程中的步骤 1、2、3、4 得到密钥序列 $Z=z_0z_1\cdots z_{M\times N-1}$。

步骤 3，将密文序列的每个元素与密钥序列中对应的元素做模 2 减法运算，即 $x_i=y_i-z_i \bmod 2$，得到明文序列 $X=x_0x_1\cdots x_{M\times N-1}$。

步骤 4，将明文序列转换为矩阵，并由加密过程的步骤 5 得到出明文的像素矩阵 $\boldsymbol{P}$，最后将像素矩阵 $\boldsymbol{P}$ 转换为图像。

3　实验仿真与分析

3.1　实验仿真

分别使用 2 幅像素值个数为 256×256 的图像 Cameraman 和 Lena 进行实验仿真。仿真实验为基于上述密

钥参数对明文图像进行加密后得到密文图像,然后用同样的密钥参数对密文图像进行解密得到明文图像。加密-解密方案的实验仿真结果如图4、图5所示。

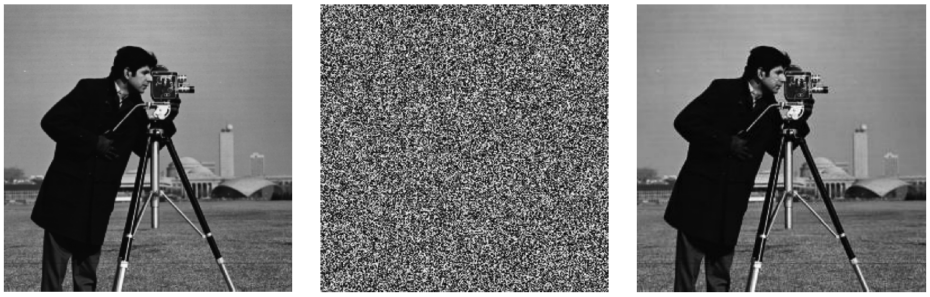


图4 Cameraman的明文图像和密文图像以及恢复图像

Fig. 4 Plaintext image, ciphertext image and recovery image of Cameraman

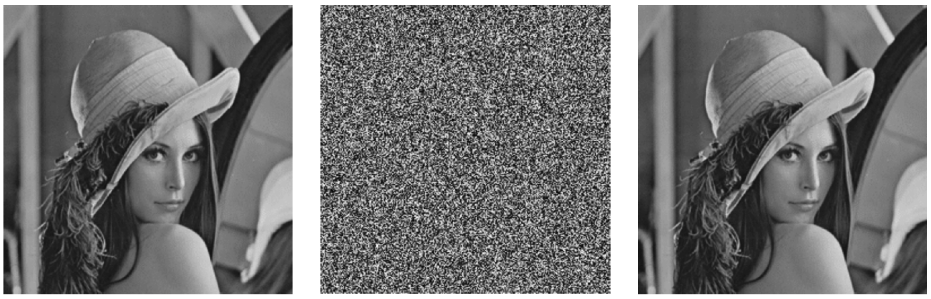


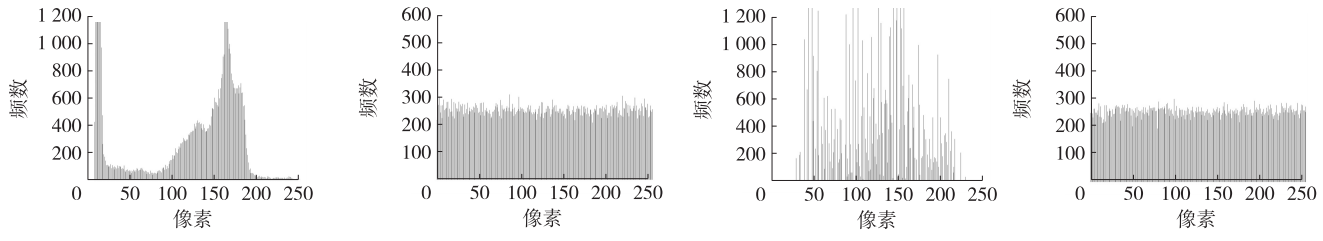
图5 Lena的明文图像和密文图像以及恢复图像

Fig. 5 Plaintext image, ciphertext image and recovery image of Lena

从仿真实验结果不难看出,在没有密钥的情况,密文图像几乎无法得到明文图像的信息,并且像素越多的图像置乱程度更好。

3.2 灰度直方图

将图像中的所有像素按照灰度值的大小统计出现的频率,得到图像的灰度直方图。密文图像的灰度分布越均匀,加密效果越好。通过比较明文图像与密文图像的灰度直方图可以看出加密方案对明文图像与密文图像关系的模糊程度,从像素灰度值的分布可以评价加密方案是否可以抵抗统计攻击。Cameraman和Lena明文图像与密文图像的灰度直方图如图6所示。



a Cameraman明文图像 b Cameraman密文图像 c Lena明文图像 d Lena密文图像

图6 明文图像和密文图像的灰度直方图

Fig. 6 Gray histograms of plaintext image and ciphertext image

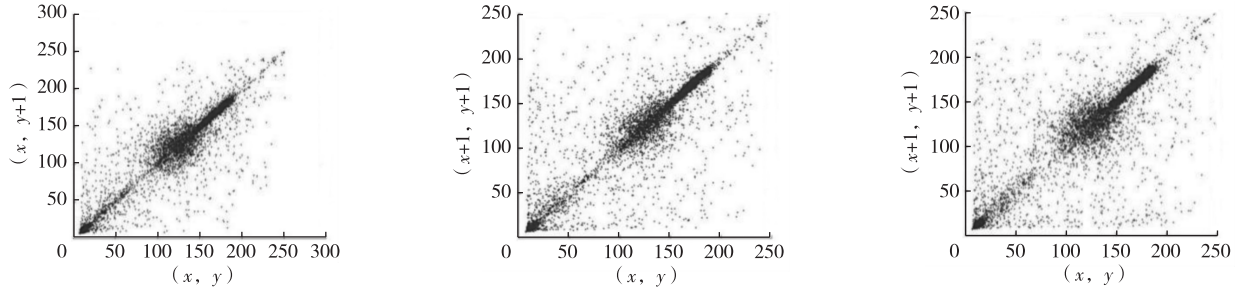
对比图6中明文图像与密文图像的直方图可以发现,明文图像的灰度值都具有一些明显的特征,而密文图像的灰度值几乎均匀分布在某一个值附近。因此,经过加密操作后,明文图像像素值分布的特征在密文图像上被消除,表明加密方案可以有效抵抗统计攻击。

3.3 相关性分析

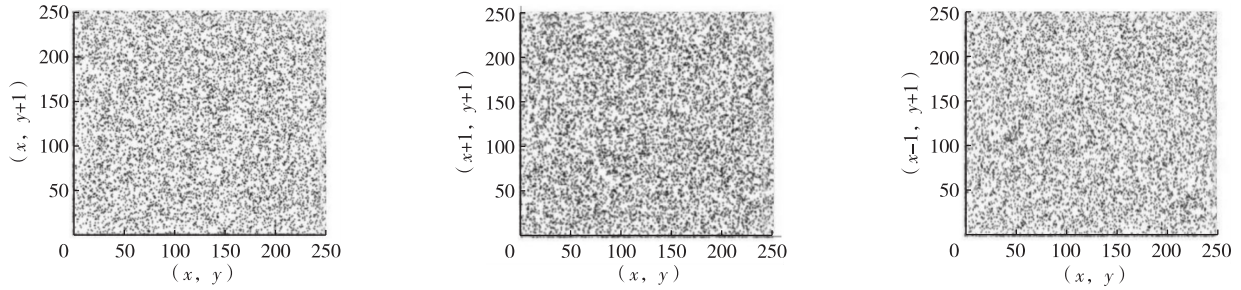
为了较好评估图像的置乱度,从水平、垂直和对角这3个方向分别计算明文图像和密文图像相邻像素点之间的相关系数并进行对比,相关性分析可以有效评估图像的置乱度。给出相关系数的计算公式如下:

$$\sigma_{xy}=\frac{\sum_{i=1}^{N}(x_i-E(x))\times(y_i-E(y))}{\sqrt{(\sum_{i=1}^{N}(x_i-E(x)^2)\times(\sum_{i=1}^{N}(y_i-E(y)^2)}},\tag{8}$$

其中：σ_{xy} 表示某个方向上的相邻像素相关性系数，x_i 与 y_i 表示第 i 个相邻像素对的 2 个像素灰度值，N 表示各个方向上选取像素对总数。对明文图像及对应的密文图像在水平、垂直和对角 3 个方向上随机取 10 000 个像素计算相关性系数，并绘制相关性分布图。图 7、8 分别显示了 Cameraman、Lena 的明文图像与密文图像在水平、垂直和对角方向上的相关性分布。



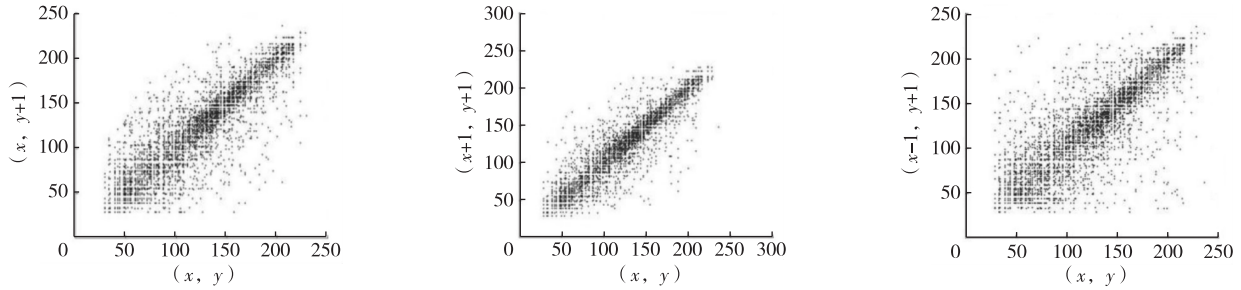
a　明文图像在水平方向的相关性分布　　b　明文图像在垂直方向的相关性分布　　c　明文图像在对角方向的相关性分布



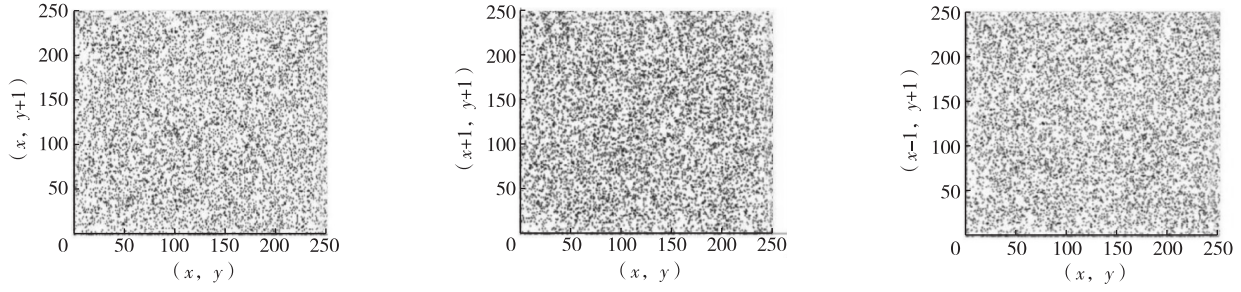
d　密文图像在水平方向的相关性分布　　e　密文图像在垂直方向的相关性分布　　f　密文图像在对角方向的相关性分布

图 7　Cameraman 图像明文与密文在不同方向的相关分布

Fig. 7　Correlation distribution of plaintext and ciphertext in different directions of Cameraman image



a　明文图像在水平方向的相关性分布　　b　明文图像在水平方向的相关性分布　　c　明文图像在对角方向的相关分布



d　密文图像在水平方向的相关性分布　　e　密文图像在垂直方向的相关性分布　　f　密文图像在对角方向的相关性分布

图 8　Lena 图像明文与密文在不同方向的相关分布

Fig. 8　Correlation distribution of plaintext and ciphertext in different directions of Lena image

从图7、图8可以看出,明文图像的像素点经加密后打破了相关性,明文、密文图像在相关性上有了明显的差别,这表明算法可以有效抵御统计攻击。仿真实验所用的Cameraman和Lena的明文、密文图像在水平、垂直和对角这3个方向上相关性系数与文献[16,22-23]的对比如表1所示。从表1可以看出,明文图像在3个方向上的相关性系数均大于0.9,说明明文图像在3个方向的相关性非常强。而密文图像在3个方向上的相关系数趋于0,几乎不相关,说明加密后能够有效抵御统计攻击。

3.4 熵值分析

在图像加密领域,信息熵是评价加密方案的重要标准之一。信息熵可以有效反映图像的不确定性,信息熵越大,图像所含信息的不确定性越大。信息熵的计算公式为:

$$H=-\sum_{i=1}^{L}(p(i)\log_2 p(i)), \tag{9}$$

其中:L 表示图像的灰度等级,$p(i)$表示像素值出现的概率。对于 L 等于256的灰度图像,信息熵的理想值为8,实际实验得到的值越接近8表明加密效果越好。

表2给出本文加密前后图像信息熵与文献[16,22]的对比。由表2可知,明文图像经过加密后信息熵的值提高到了接近8的值,说明加密方案可以有效增加明文图像的不确定性。

表1 Cameraman和Lena的相关性系数表

Tab.1 Correlation coefficients of Cameraman and Lena

图像	方向	明文图像	密文图像	文献[16]	文献[22]	文献[23]
Lena	水平	0.962 7	−0.020 6	−0.000 2	0.006 5	−0.020 8
	垂直	0.934 2	0.000 1	−0.000 4	−0.089	0.042 4
	对角	0.905 6	0.005 2	0.000 1	0.008 5	0.021 2
Cameraman	水平	0.957 3	−0.018 2	0.000 4	—	—
	垂直	0.933 4	0.000 1	0.000 1	—	—
	对角	0.901 3	0.005 2	0.000 2	—	—

表2 加密前后图像信息熵对比

Tab.2 Comparison of image information entropy before encryption and after encryption

图像	算法来源	明文图像信息熵	密文图像信息熵
Cameraman	本文	**7.009 7**	**7.990 7**
	[16]	—	7.955 4
Lena	本文	**7.303 5**	**7.990 2**
	文献[16]	—	7.954 4
	文献[22]	—	7.997 0

注:加粗的数字表示该项结果最优。下同。

3.5 密钥敏感性分析

密钥敏感性反映解密算法对密钥的敏感程度。本节使用像素数改变率(number of pixels change rate, NPCR)和统一平均变化强度(unified average changing intensity, UACI)定量分析明文图像与解密图像的差异,分别记为:

$$N(P_1,P_2)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(|\mathrm{sign}(P_1(i,j)-P_2(i,j))|\times 100\%), \tag{10}$$

$$U(P_1,P_2)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|P_1(i,j)-P_2(i,j)|}{255-0}\times 100\%, \tag{11}$$

其中:P_1 与 P_2 为同一幅图像在密钥参数有微小变化前后得到的图像,$P_1(i,j)$为密文图像 P_1 在(i,j)位置的像素值,$P_2(i,j)$为密文图像 P_2 在(i,j)位置的像素值,M 与 N 是图像的长度与宽度。符号函数 sign(x)满足:当 $x\geqslant 0$ 时,sign$(x)=1$;当 $x=0$ 时,sign$(x)=0$;当 $x\leqslant 0$ 时,sign$(x)=-1$。

表 3 给出本文的 NPCR 与 UACI 的数据，结果表明加密方案对密钥参数敏感。

3.6 差分攻击分析

差分攻击分析是密码分析里常用的一种攻击手段，该方法通过对明文进行细微的修改以获取相应的密文，并通过修改后的密文与原密文之间的差异联系来攻击破译密码系统。使用 NPCR 与 UACI 衡量加密方案的抗差分攻击性，设明文图像进行加密后得到的密文图像为 P_1^*，改变明文图像 1 个像素点的像素值后再进行加密得到的密文图像为 P_2^*，利用式(10)与式(11)计算 NPCR 与 UACI。NPCR 与 UACI 的期望值分别为 0.996 1 与 0.334 6。将本文针对实验图像得到的结果与文献[16,22-23]比较，如表 4 所示。

表 3　加密方案密钥敏感性的 NPCR 以及 UACI 值

Tab. 3　NPCR and UACI values of key sensitive in the encryption scheme　%

图像	NPCR	UACI
Cameraman	99.556 0	33.340 5
Lena	99.559 6	33.401 3

从表 4 的数据可以看出，本文所提的加密方案能够更加有效抵御差分攻击。

3.7 时间复杂度分析

在计算机科学与技术领域，算法的时间复杂度是一个函数，可以定性地描述算法的运行时间，所以，时间复杂度是衡量算法整体性能的一个重要指标。使用加密方案的加密算法与解密算法处理图像 Lena 与 Cameraman 若干次取所消耗时间(包括编码时间、加密时间以及解密时间)的平均值与文献[16]比较如表 5 所示。可以看出，本文提出的加密方案具有较高的效率。

表 4　本文加密方案明文敏感性的 NPCR 和 UACI 值

Tab. 4　NPCR and UACI values of cleartext sensitive in the encryption scheme　%

图像	算法来源	NPCR	UACI
Lena	本文	**99.559 6**	**33.401 3**
	文献[16]	99.54	33.03
	文献[22]	98.53	33.37
	文献[23]	98.78	32.99

表 5　处理图像所耗时间平均值

Tab. 5　Average amount of time taken to process images

图像	算法来源	总耗时/s
Lena	本文	**1.989**
	文献[16]	10.968
Cameraman	本文	1.991
	文献[16]	6.799

3.8 密钥空间分析

密钥空间的容量与加密方案的安全性有着很强的关系，密钥空间越大，加密方案的安全性越高。本文的密钥参数包括系数矩阵、明文像素值的和、ICMIC 的控制参数和迭代次数、时间步长。在不考虑随机数序列的情况下，图像在精度为 1 015 的仿真设备上进行加密，密钥空间为 $105\times15=1\ 075>2\ 100$，满足安全要求，表明本文所提出的加密方案有着足够大的密钥空间，可以有效抵御暴力破解。

4 结论

本文提出了一种基于 Kolmogorov 方程与 ICMIC 混沌映射的针对灰度图像的加密方案，利用了 Kolmogorov 方程可以描述随机过程是 Markov 过程这一性质，结合 ICMIC 复杂的动力学行为设计了一套密钥生成算法，并将 Kolmogorov 方程与 ICMIC 的参数作为密钥参数。在解密图像时用相同的密钥参数进行解密恢复图像。通过实验与性能分析，表明本文提出的算法能够有效对明文图像信息进行混淆，当拥有密钥参数的情况下可以较好地恢复明文图像的信息，在相关性分析、信息熵、密钥敏感性等方面的测试均有较好的结果，并且明文敏感性较相关文献更强，能够更好地抵御差分攻击。但是，本文提出的加密算法还有需要改进的地方。比如密文图像的信息熵虽然已经被提高到 7.990 以上，但与部分文献的结果相比还有一定差距，这也是下一步研究所需要关注的问题。

参考文献：

[1] 于洋. 基于矩阵变换的复合图像加密方案[D]. 哈尔滨：东北林业大学，2019.

YU Y. Composite image encryption algorithm based on matrix transformation [D]. Harbin: Northeastern Forestry University,

2019.

[2] 邵利平,覃征,衡星辰,等.基于矩阵变换的图像置乱逆问题求解[J].电子学报,2008,36(7):1355-1363.
SHAO L P,QIN Z,HENG X C,et al. Solving the image scrambling problem based on matrix transformation[J]. Electronic Journal,2008,36(7):1355-1363.

[3] 王一诺,宋昭阳,马玉林,等.基于DNA编码与交替量子随机行走的彩色图像加密算法[J].物理学报,2021,70(23):32-41.
WANG Y N,SONG Z Y,MA Y L,et al. Color image encryption algorithm based on DNA encoding and alternating quantum random walk [J]. Journal of Physics,2021,70(23):32-41.

[4] 刘杨曦.基于图像位平面的加密算法研究[D].南昌:南昌大学,2021.
LIU Y X. An Encryption Algorithm based on image bit plane [D]. Nanchang:Nanchang University,2021.

[5] 姚晨程.光学加密技术在生物图像处理中的应用研究[D].杭州:浙江农林大学,2019.
YAO C C. The Application of Optical Encryption in Biological Image Processing [D]. Hangzhou:Zhejiang A & F University,2019.

[6] 邓涯双.混沌序列密码的理论与应用实现[M].北京:中国社会科学出版社,2018.
DENG Y S. Theory and application of chaotic sequence ciphers[M]. Beijing:China Social Sciences Press,2018.

[7] MATTHEWS R. On the derivation of a "Chaotic" encryption algorithm[J]. Cryptologia,1989,8(1):29-41.

[8] FRIDRICH J. Image encryption based on chaotic maps[C]//TIEN J M. Proceedings 1997 IEEE International Conference on Systems,Man,and Cybernetics. Computational Cybernetics and Simulation. Piscataway:IEEE,1997.

[9] 张翌维,王育民,沈绪榜.基于混沌映射的一种交替结构图像加密算法[J].中国科学(E辑:信息科学),2007,37(2):183-190.
ZHANG Y W,WANG Y M,SHEN X B. An alternating structure image encryption algorithm based on chaotic mapping[J]. Chinese Science (Series E:Information Science),2007,37(2):183-190.

[10] 廖晓峰,岳蓓,周庆,等.用混沌映射的图像加密方案实现FPGA[J].重庆大学学报,2008,31(10):1189-1193.
LIAO X F,YUE B,ZHOU Q,et al. The image encryption algorithm of chaotic map is used to implement FPGA[J]. Journal of Chongqing University,2008,31(10):1189-1193.

[11] 邢宇航,李敏.基于LFSR状态序列的混沌序列图像加密方案[J].信息安全研究,2018,4(4):336-341.
XING Y H,LI M. Image encryption scheme of chaotic sequence based on LFSR state sequence[J]. Information Security Research,2018,4(4):336-341.

[12] 朱从旭,孙克辉.密钥与明文相关联的混沌图像加密算法[J].中国通信,2012,9(1):73-79.
ZHU C X,SUN K H. Chaos image encryption algorithm[J]. China Communications,2012,9(1):73-79.

[13] 吴新华,刘同佩.基于混沌的图像加密算法研究[J].微电子学与计算机,2010,27(9):73-75.
WU X H,LIU T P. A chaos-based image encryption algorithm research [J]. Microelectronics and Computers,2010,27(9):73-75.

[14] 孙鑫,易开祥,孙优贤.基于混沌系统的图像加密算法[J].计算机辅助设计与图形学学报,2002,14(2):136-139.
SUN X,YI K X,SUN Y X. Image enption algorithm based on chaos systems[J]. Journal of Computer Aided Design and Graphics,2002,14(2):136-139.

[15] 彭军,廖晓峰,张伟,等.基于复合混沌系统的图像加密[J].计算机工程,2006,32(2):34-36.
PENG J,LIAO X F,ZHANG W,et al. Image encryption based on a composite chaos system[J]. Computer Engineering,2006,32(2):34-36.

[16] 石航,王丽丹.一种基于压缩感知和多维混沌系统的多过程图像加密方案[J].物理学报,2019,68(20):39-52.
SHI H,WANG L D. A multi-process image encryption scheme based on compressed sensing and multi-dimensional chaotic system [J]. Journal of Physics,2019,68(20):39-52.

[17] 陈炜,郭媛,敬世伟.基于深度学习压缩感知与复合混沌系统的通用图像加密算法[J].物理学报,2020,69(24):99-111.
CHEN W,GUO Y,JING S W. General image encryption algorithm based on deep learning compression sensing and composite chaos system[J]. Journal of Physics,2020,69(24):99-111.

[18] 段黎力,廖晓峰,向涛.基于Markov性质的一阶安全算术编码及应用[J].物理学报,2010,59(10):6744-6751.
DUAN L L,LIAO X F,XIANG T. First-order security arithmetic coding and application based on Markov properties [J]. Journal of Physics,2010,59(10):6744-6751.

[19] 胡裴龙.基于混沌理论与DNA编码的图像加密方案研究[D].合肥:安徽大学,2018.
HU P L. Image enption algorithm based on chaos theory and DNA coding [D]. Hefei:Anhui University,2018.

[20] HE D,CHEN H,JIANG L G,et al. Chaotic characteristics of a one-dimensional iterative map with infinite collapses[J]. IEEE

Transactions on Circuits & Systems I Fundamental Theory & Applications,2001,48(7):900-906.

[21] 郭柏灵,蒲学科.随机无穷维动力系统[M].北京:北京航空航天大学出版社,2009.
GUO B L,PU X K. Stochastic infinite-dimensional dynamical system [M]. Beijing:Beijing Aerospace University Press,2009.

[22] 周洪波,尹文双,刘静漪,等.基于变参超混沌与可逆向量积的图像加密算法[J].重庆师范大学学报(自然科学版),2021,38(5):90-97.
ZHOU H B,YIN W S,LIU J Y,et al. Image encryption algorithm based on variable parameter hyperchaos and reversible vector product [J]. Journal of Chongqing Normal University (Natural Science edition),2021,38(5):90-97.

[23] 马聪,李国东.基于 L-K 双混沌系统的彩色位级图像加密算法[J].计算机应用与软件,2020,37(3):321-326.
MA C,LI G D. Color bit-level image encryption algorithm based on L-K double chaotic system [J]. Computer Applications and Software,2020,37(3):321-326.

An Image Encryption Scheme Based on the Kolmogorov Equation and the ICMIC

GUAN Zhixuan, HU Jintao, TIAN Hongjiong

(Department of Mathematics, School of Mathematics and Science, Shanghai Normal University, Shanghai 200234, China)

Abstract: For the security problem of image transmission, using the Markov property of the solution of Kolmogorov equation and the chaos of infinite folding of Iterative Chaotic Map with Infinite Collapses (ICMIC), a symmetrical encryption scheme is proposed to resist encoding attack. First, the transfer probability matrix is generated by setting the coefficient matrix of the Kolmogorov equation and the initial state as the key parameter. Second, the transfer probability matrix is input into ICMIC, and the key sequence is determined by the obtained results. Finally, the ciphertext images are generated by adding the key sequence and the plaintext images. The encryption scheme was entally simulated by the MATLAB program, with ciphertext image information entropy above 7.99, NPCR over 99%, and UACI over 33%. The experimental results show that the encryption scheme has high security and can effectively resist statistical attacks and differential attacks.

Keywords: image encryption; Markov process; Kolmogorov equation; ICMIC

(责任编辑 黄 颖)