结合压缩感知和新混沌映射的图像加密方案

周明伟[1],阚忠良[1*],蒋东华[2]
(1. 黑龙江大学 计算机科学与技术学院,黑龙江 哈尔滨 150080;
2. 长安大学 信息工程学院,陕西 西安 710064)

摘 要:为了解决密文图像在公用信道传输过程中容易遭到基于深度神经网络模型攻击的问题,提出一种结合二维压缩感知、新设计的离散分数阶 Chebyshev 混沌映射和空域最低有效位(Least Significant Bit, LSB)嵌入的视觉有意义图像加密算法。首先,在明文信息熵的控制下迭代分数阶混沌映射以产生特定的密码流。其次,采用受控混沌测量矩阵、FAN 变换置乱以及混合扩散策略对明文图像执行二维压缩和加密操作,得到具有统计伪随机性的秘密图像。然后,通过最低有效位嵌入算法将秘密图像随机地嵌入到非涉密传输介质的各个区域中以生成具有视觉意义的密文图像。另外,将明文信息熵隐藏到密文图像的透明度通道以实现所提算法安全性和实用性之间的均衡。最后,仿真结果和理论分析表明,所提加密算法生成的密文图像不但能够抵御多种常见的攻击,还具有不错的视觉安全性。

关键词:图像加密;压缩感知;混沌映射;最低有效位嵌入;安全性分析
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2023)03-0063-08
doi:10.3969/j.issn.1673-629X.2023.03.010

Image Encryption Scheme by Combining Compressive Sensing and New Chaotic Map

ZHOU Ming-wei[1], KAN Zhong-liang[1*], JIANG Dong-hua[2]
(1. School of Computer Science and Technology, Heilongjiang University, Harbin 150080, China;
2. School of Information Engineering, Chang'an University, Xi'an 710064, China)

Abstract: To solve the problem that the cipher images transmitted in public channel are easily attacked by the deep neural network-based model, a visually meaningful image encryption algorithm by combining the 2D compressive sensing, the newly-designed discrete fractional-order Chebyshev chaotic map and spatial least significant bit (LSB) embedding is proposed. Firstly, the proposed algorithm iterates the fractional-order chaotic map under the control of plaintext information entropy to generate the specific secret key stream. Secondly, the key-controlled chaotic measurement matrixes, FAN transform scrambling and hybrid diffusion strategy are employed to perform the compression and encryption operations on plain image, and the secret image with statistical pseudo-randomness is obtained. Then, the secret image is stochastically embedded into various regions of the non-secret-involved transmission medium by means of the least significant bit embedding algorithm to generate the visually meaningful cipher image. Additionally, the plaintext entropy is hidden in the transparency channel of cipher image to achieve the balance between the security and practicability of proposed algorithm. Ultimately, the simulation results and theoretical analyses indicate that the cipher image generated by proposed encryption algorithm has good visual security in addition to withstanding various common attacks.

Key words: image encryption; compressive sensing; chaotic map; least significant bit embedding; security analysis

0 引 言

随着数字多媒体技术和网络技术的革命性发展,作为信息的一种具体表现形式,数字图像被海量制造、传输与存储。而在信息交换便捷化的当下,数字图像在开放共享的平台上进行传输时容易遭到基于深度神经网络模型的攻击[1],造成隐私泄露,进而引起越来越多的个人用户、企业乃至政府部门对于数据隐私安全的担忧。在此社会背景下,图像密码系统应运而生,以解决在国防军事、医学、工业等诸多领域中的隐私保护问题。

收稿日期:2022-05-03 **修回日期**:2022-09-07
基金项目:国家自然科学基金(61972135);黑龙江省自然科学基金(LH2020F043)
作者简介:周明伟(1994-),男,硕士研究生,研究方向为图像加密、网络安全;通信作者:阚忠良(1969-),男,副教授,硕士,研究方向为网络安全、深度学习。

如文献[2]中所述,隐私图像保密技术一般可以分为两大类,一类是图像加密,而另一类则是图像隐写(图像隐藏)。因此可以根据密文图像的视觉纹理是否具有意义来区分它们。图像加密技术指的是在密码流的控制下按照加密规则将具有视觉意义的明文图像转换成类噪声密文图像,与此同时,黑客在没有得到正确密钥的情况下将无法获取密文图像中所携带的敏感信息。

截止到目前,研究人员基于混沌理论[3-4]、DNA 编码技术[5]、细胞自动机[6]、压缩感知[7-8]以及马尔可夫模型[9]等提出了许多有效的加密方案。然而,此类图像加密方案均存在一个弊病,即缺乏隐蔽性。当生成的具有统计伪随机特性的密文图像在公用信道中传输或本地化存储时极易被黑客或基于神经网络的各种攻击模型所侦测到,进而遭到诸多类型的攻击。

图像隐写则指的是以一种不可检测的方式将敏感明文图像隐藏到可公开获取的载体图像中,以创建具有视觉安全性的密文图像。也就是说,通过隐藏通信行为的方式来达到传递敏感信息的目的。近些年来,结合传统加密技术与图像隐写技术,如矩阵编码嵌入[10]、离散提升小波变换嵌入[11]、斜变换嵌入[12]和奇异值分解嵌入[13-14]等,以设计出能够实现对明文图像的同步加密和隐写的视觉有意义图像加密算法被相继提出。然而就现有的视觉安全图像加密算法而言,虽然采用基于频域变换的分块嵌入方式来提升算法的鲁棒性,但却以牺牲其不可感知性和压缩性能为代价,进而导致携带秘密数据的数字载密图像容易被基于统计模型或是深度神经网络模型的隐写分析器所发现。

针对上述图像加密算法中所存在的问题,该文利用新设计的离散分数阶 Chebyshev 混沌映射、二维压缩感知模型以及空域最低有效位嵌入设计出一种高安全性的视觉有意义图像加密算法。首先,在文献[15]的启发下,对经典一维 Chebyshev 混沌映射进行改进得到其离散分数阶形式的混沌映射。并通过分析其分岔图和李雅普诺夫指数谱验证了该改进型映射具有良好的混沌动力学特性。其次,在明文信息熵的控制下,利用该混沌映射构建出密码流和受控测量矩阵,并用以对明文图像执行二维压缩和加密。最后,再通过无损的空域嵌入方式将秘密图像隐藏到某一可公开获取的载体图像中。实验结果表明:所设计的基于压缩-加密-嵌入框架的图像加密算法不仅能降低密文图像被侦测到和被攻击的概率,同时凭借着明文信息熵和混合扩散策略提升其明文敏感性和密文扩散能力,增强了所提算法在抵御基于明文分析安全攻击模型方面的能力。

1 理论知识

1.1 二维压缩感知模型

在采用传统压缩感知模型处理二维数字图像时,常见做法是先将二维图像堆叠成一维度很大的列向量,然后再对其进行线性测量。但这种处理方式需要占用大量的存储空间和计算资源,因此一些研究者们提出将其扩展到二维正交平面中[16]。

首先,假设一维度为 $N \times N$ 的明文图像 $\boldsymbol{P}$ 在 $\boldsymbol{\Psi}$ 域中是稀疏的。则其可以被稀疏表示为:

$$\boldsymbol{D} = \boldsymbol{\Psi P \Psi}^{\mathrm{T}} \tag{1}$$

式中,变量 $\boldsymbol{\Psi} \in \mathbb{R}^{N\times N}$ 和 $\boldsymbol{D} \in \mathbb{R}^{N\times N}$ 分别表示为稀疏表示基矩阵和明文图像 $\boldsymbol{P}$ 在 $\boldsymbol{\Psi}$ 域中的系数矩阵,而符号 T 记为转置操作。

其次,在二维压缩感知模型中,可以通过将图像 $\boldsymbol{P}$ 的稀疏系数矩阵 $\boldsymbol{D}$ 线性投影到两个相互正交的测量矩阵 $\boldsymbol{\Phi}_1 \in \mathbb{R}^{M\times N}$ 和 $\boldsymbol{\Phi}_2 \in \mathbb{R}^{M\times N}$ 上来实现对明文图像的二维压缩,其中符号 M 与 N 表示矩阵的行数与列数。此过程的数学表述为:

$$\boldsymbol{Z} = \boldsymbol{\Phi}_1 \boldsymbol{D} \boldsymbol{\Phi}_2^{\mathrm{T}} = \boldsymbol{\Phi}_1 \boldsymbol{\Psi P \Psi}^{\mathrm{T}} \boldsymbol{\Phi}_2^{\mathrm{T}} \tag{2}$$

式中,$\boldsymbol{Z}$ 是一个 $M \times M$ 维的测量值矩阵。事实上,矩阵 $\boldsymbol{\Phi}_1$ 对明文图像 $\boldsymbol{P}$ 的行进行操作,而矩阵 $\boldsymbol{\Phi}_2$ 则是对其列进行操作。另外,为了能够从矩阵 $\boldsymbol{Z}$ 中精准重构出图像 $\boldsymbol{P}$,需要解决以下优化问题。

$$\min \ \| \boldsymbol{D} \|_0 \quad \text{s.t. } \boldsymbol{Z} = \boldsymbol{\Phi}_1 \boldsymbol{D} \boldsymbol{\Phi}_2^{\mathrm{T}} \tag{3}$$

1.2 测量矩阵的构建

在对图像进行二维压缩时,测量矩阵的性能对于解密过程中重建图像的视觉质量有所影响。随机型测量矩阵虽然具有普适性,但其性能难以控制。因此,该文依据混沌映射所具有的伪随机性和统计独立性来构建两个确定型混沌测量矩阵。

具体的构建步骤如下:

步骤 1:在给定初始状态和控制参数的情况下,迭代某一维性能优良的混沌映射 $\lfloor d \cdot C_R \cdot N^2 \rfloor$ 次,生成序列 $\boldsymbol{Q}$。其中变量 d 和 C_R 表示抽样距离和预设的压缩率,而符号 $\lfloor \ \sim \ \rfloor$ 表示向负无穷方向取整。

步骤 2:对上一步迭代得到的混沌序列 $\boldsymbol{Q}$ 进行如下处理。

$$\boldsymbol{W} = 1 - 2 \cdot \mathrm{mod}(\boldsymbol{Q}(1:d:d \cdot C_R \cdot N^2), 1) \tag{4}$$

步骤 3:将新生成的伪随机序列 $\boldsymbol{W}$ 按列重排成二维矩阵,并执行归一化操作,从而得到测量矩阵 $\boldsymbol{\Phi}_1$。此过程可以由式(5)表述,其中行数 $M = \lfloor C_R \cdot N \rfloor$。

$$\boldsymbol{\Phi}_1 = \sqrt{\frac{2}{M}} \begin{bmatrix} W_1 & W_{M+1} & \cdots & W_{M(N-1)+1} \\ W_2 & W_{M+2} & \cdots & W_{M(N-1)+2} \\ \vdots & \vdots & \vdots & \vdots \\ W_M & W_{2M} & \cdots & W_{MN} \end{bmatrix} \tag{5}$$

步骤 4:根据不同的初始状态重新执行步骤 1 至步骤 3,得到另一个测量矩阵 $\boldsymbol{\Phi}_2$。

2　所设计的新混沌映射

2.1　新映射的数学定义

针对经典一维 Chebyshev 混沌映射的分岔图存在空白窗口及稳定吸引子等缺陷,该文通过文献[15]中介绍的方法对其进行改进,得到一维分数阶 Chebyshev 混沌映射(Fractional-order Chebyshev Chaotic Map, FCCM)。该改进型混沌映射的数学模型如式(6)所示。

$$x(n)=\mathrm{mod}\left(x(n-1)+\frac{h^{v}}{\Gamma(1+v)}\cos(\mu\cdot \operatorname{acos}(x(n-1))),2\right) \tag{6}$$

式中,x 和 n 为该映射的状态变量和迭代变量,而 μ, v, $h\in\mathbb{R}^{+}$ 则分别表示为其控制参量、分数阶数和离散步长,且伽马函数 $\Gamma(1+v)=\int_0^{+\infty}t^{v}\mathrm{e}^{-t}\mathrm{d}t$。另外,在式(5)中添加取模运算(mod)的目的是限制该映射在相空间中运动轨迹的范围,避免超出计算机的有限字长。

2.2　性能分析与对比

在 $x_0=0.2345$, $v=0.15$, $h=0.45$ 的情况下,图 1 给出了所提一维分数阶 Chebyshev 混沌映射随控制参数 μ 变化的分岔图。从图中可以看出,相比于原始的一维 Chebyshev 混沌映射(其分岔图如图 2 所示),

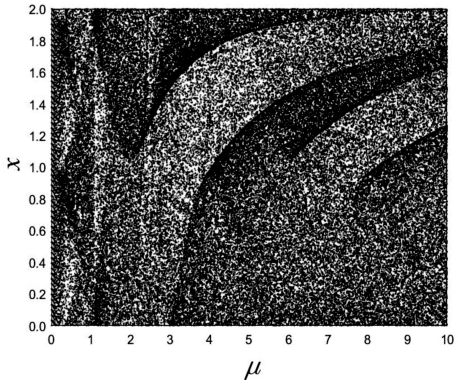


图 1　分数阶 Chebyshev 混沌映射的分岔图

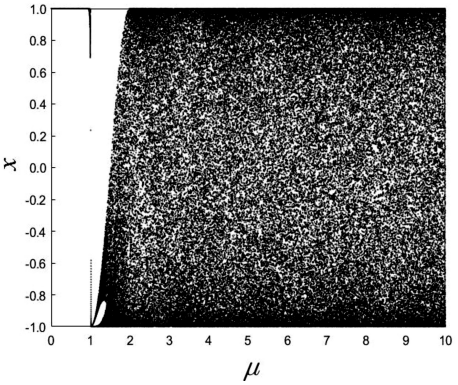


图 2　经典 Chebyshev 混沌映射的分岔图

其空白窗口得以消除、混沌空间范围更大以及输出的混沌序列的遍历性更好。另外,由于向原始混沌映射中引入离散步长和分数阶阶数,因此将其应用于图像保密领域可以显著扩展加密算法的密钥空间。

如果在相空间中非线性系统的轨迹远离其平衡点,则表明该系统不稳定。李雅普诺夫指数(Lyapunov Expone-nt,LE)是一种用于量化描述运动轨迹长期相互排斥和吸引的指标[17]。如果某一系统的 LE 值为正,则表明其相空间中会出现混沌现象。因此判断一个非线性系统是否为混沌系统,仅需检查其 LE 值是否大于 0。对于一维映射 $f(x)$ 而言,其李雅普诺夫指数可以通过式(7)计算得到。

$$L_E=\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N}\ln\left|\frac{\mathrm{d}f(x)}{\mathrm{d}x}\right| \tag{7}$$

所提一维分数阶 Chebyshev 混沌映射随控制参数 μ 变化的 LE 谱如图 3 所示。从图中可以看出,在整个取值区间范围内,所设计的非线性映射的 LE 值均大于 0,且随着 μ 的变化逐渐增大,表明其在整个相空间中均存在混沌行为。除此之外,相比于其他新提出的先进混沌映射而言,其初值敏感性和伪随机性更好。

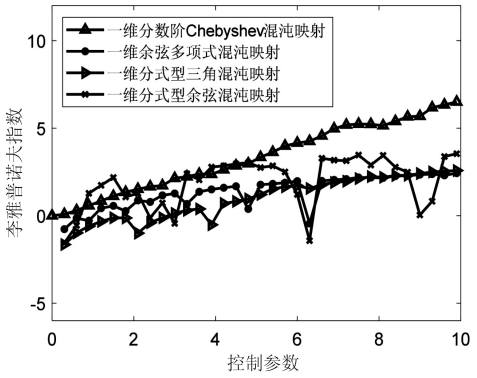


图 3　若干个混沌映射的李雅普诺夫指数谱

3　视觉安全图像加解密算法

所提出的视觉有意义图像加密算法由四个主要步骤组成,即通过分数阶 Chebyshev 混沌映射生成“一图一密”的密码流,采用压缩感知模型在两个正交方向上对明文图像压缩采样,利用 FAN 变换置乱和混合扩散策略二次加密明文像素值以及使用 LSB 嵌入算法将具有统计伪随机性的秘密数据隐藏到非涉密传输介质中。整套加密算法的框架如图 4 所示。

3.1　密码流的生成

鉴于信息熵对消息极度敏感[18],该文采用明文图像的信息熵来构建加密过程中各阶段的密码流以有效抵抗基于选择明文分析的安全攻击模型,其数学定义如式(8)所示。

$$I(\rho_i)=\sum_{i=0}^{255}p(\rho_i)\log_2 p(\rho_i)^{-1} \tag{8}$$

式中,符号 $p(\rho_i)$ 记为消息 ρ_i 的概率。

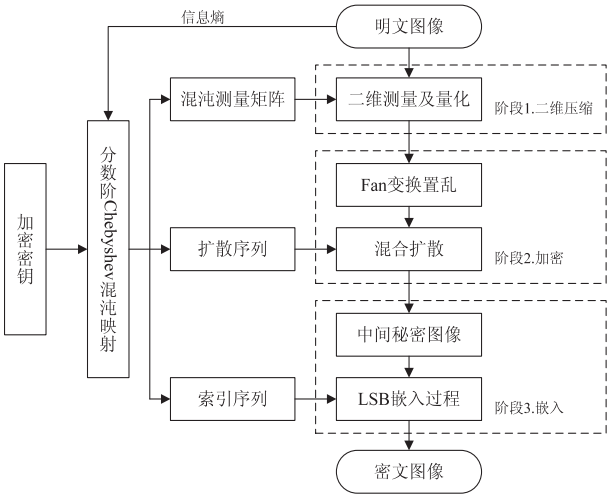


图 4 所提图像加密算法流程

首先,通过式(8)计算出待加密明文图像 $\boldsymbol{P} \in \mathbb{N}^{N\times N}$ 的信息熵,记为 I_P。其次,再将所设计的分数阶混沌映射的初始状态分别设置为 $(\mu_0^1 + I_P - \lfloor I_P \rfloor, x_0^1)$ 和 $(\mu_0^2 + I_P - \lfloor I_P \rfloor, x_0^2)$,并根据第 1.2 节所介绍的方法生成测量矩阵 $\boldsymbol{\Phi}_1$ 和 $\boldsymbol{\Phi}_2$。然后,再将 FCCM 映射的初始状态设为 $(\mu_0^3 + I_P - \lfloor I_P \rfloor, x_0^3)$ 和 $(\mu_0^4 + I_P - \lfloor I_P \rfloor, x_0^4)$,并分别迭代该映射 $(T_0 + C_R \cdot N^2)$ 次以生产两条混沌序列 $\boldsymbol{X} = \{x_{T_0+1}, x_{T_0+2}, \cdots, x_{T_0+C_R\cdot N^2}\}$ 和 $\boldsymbol{Y} = \{y_{T_0+1}, y_{T_0+2}, \cdots, y_{T_0+C_R\cdot N^2}\}$。最后,再根据式(9)分别处理混沌序列 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$,得到扩散序列 $\boldsymbol{D}_x$ 和索引序列 $\boldsymbol{T}_y$。

$$\begin{cases} \boldsymbol{D}_x = \mathrm{mod}(\lfloor \boldsymbol{X} \times 10^{10} \rfloor, 256) \\ \boldsymbol{T}_y = \mathrm{sort}(\boldsymbol{Y}, \text{'ascend'}) \end{cases} \tag{9}$$

3.2 二维压缩阶段

在传统压缩感知模型中,从少量测量值中通过正交匹配追踪、平滑 l_0 范数以及贝叶斯框架等重构算法精准恢复出原始信号的前提是该信号具有可压缩性或在某域中具有稀疏性。但在空域中自然图像普遍不具备此特性,因此通常的做法是采用频域变换将其转换到其他域中进行稀疏表示,从而增加算法的计算和时间复杂度。针对这个问题,该文采用一种对信号稀疏性不敏感的重建算法(2DPG-ED)[19]来提升算法的时间效率。

首先,在二维压缩阶段,第 3.1 节中所构建的两个受控的正交混沌测量矩阵被用于对明文图像进行二维压缩,并再对压缩后的系数进行线性量化。此阶段可以由式(10)表述。

$$\begin{cases} \boldsymbol{P}_1 = \boldsymbol{\Phi}_1 \cdot P \cdot \boldsymbol{\Phi}_2^{\mathrm{T}} \\ \boldsymbol{P}_2 = \lfloor 255 \times (\boldsymbol{P}_1 - \min(\boldsymbol{P}_1)) \cdot \\ \qquad (\max(\boldsymbol{P}_1) - \min(\boldsymbol{P}_1))^{-1} \rfloor \end{cases} \tag{10}$$

式中,函数 max 和 min 分别表示取最大值和最小值操作。

3.3 加密阶段

考虑到压缩感知的本质是线性映射[20],其难以抵抗选择明文攻击。因此,所设计的图像加密算法除了采用“一图一密”策略来提高算法的安全性外,还利用 FAN 变换置乱和混沌扩散策略来掩盖明文图像独有的统计特性并使加密图像具有雪崩效应。具有的操作步骤如下:

FAN 变换置乱:FAN 变换是 Arnold 变换的一般形式,其模型如式(11)所示。

$$\begin{cases} \begin{bmatrix} i_n \\ j_n \end{bmatrix} = \begin{bmatrix} t_{00} & t_{01} \\ t_{10} & t_{11} \end{bmatrix} \times \begin{bmatrix} i_{n-1} \\ j_{n-1} \end{bmatrix} + q \begin{bmatrix} N \\ N \end{bmatrix} \bmod \begin{bmatrix} N \\ N \end{bmatrix} + 1 \\ q = \max(|t_{00}|, |t_{01}|, |t_{10}|, |t_{11}|) \\ t_{00}t_{11} - t_{01}t_{10} = \pm 1 \end{cases} \tag{11}$$

式中,(i_{n-1}, j_{n-1}) 和 (i_n, j_n) 表示变换前后的像素坐标,参数 $t_{00}, t_{01}, t_{10}, t_{11}$ 为该变换的控制参数。根据式(11),对压缩图像 $\boldsymbol{P}_2$ 进行 FAN 变换置乱,得到矩阵 $\boldsymbol{P}_3$。

混合扩散策略:为得到较好的扩散效果,该文结合加模操作和按位异或操作设计出混沌扩散策略,如式(12)所示。

$$\begin{cases} \boldsymbol{P}_4(1) = \mathrm{mod}(\boldsymbol{P}_3(1) + \boldsymbol{D}_x(1) + \\ \qquad \lfloor (I_P - \lfloor I_P \rfloor) \times 10^6 \rfloor, 256) \\ \boldsymbol{P}_4(i) = \boldsymbol{P}_3(i) \otimes \boldsymbol{P}_4(i-1) \otimes \boldsymbol{D}_x(i) \\ \qquad i = 2, 3, 4\cdots \end{cases} \tag{12}$$

式中,符号 $\otimes$ 记为按位异或操作,且扩散序列 $\boldsymbol{D}_x$ 在第 3.1 节中构建得到。

3.4 嵌入阶段

随着当下深度学习技术的快速发展,基于神经网络的安全攻击模型日益趋于成熟。针对其可以智能地对公用信道中具有类噪声外形的密文图像进行解密分析或恶意破坏等问题,该文利用最低有效位嵌入方式为具有统计伪随机特性的加密数据提供一个非涉密的“视觉标签”以实现对明文图像内容和外形的双重保护。

在嵌入阶段,首先对载体图像 $\boldsymbol{L} \in \mathbb{N}^{N\times N}$ 的像素值执行缩放操作以防止嵌入秘密图像以后数据溢出,如式(13)所示。

$$\boldsymbol{L}_1 = \lfloor \begin{bmatrix} 10 & \cdots & 10 \\ \vdots & \ddots & \vdots \\ 10 & \cdots & 10 \end{bmatrix} + \frac{\tau - 10}{255} \boldsymbol{L} \rfloor \tag{13}$$

式中,常数 τ 取为 245。

其次,将载体图像 $\boldsymbol{L}_1$ 划分为四个部分 $\boldsymbol{L}_1^i (i = 1, 2, 3, 4)$,且每部分的维度均为 $(N/2) \times (N/2)$。然后将中间秘密图像 $\boldsymbol{P}_4$ 中每个像素值的两个比特位为一组

拆分成四部分,并逐个替换掉 $\boldsymbol{L}_1^i$ 中的第 $T_y(j)$ 个像素值的最低两个比特位,直至 $\boldsymbol{P}_4$ 中所有像素值全部嵌入完为止,从而得到最终的具有视觉安全性的密文图像。同时,由此可见,为了不增加额外的传输花销和存储空间,本算法中的变量 C_R 的取值须小于等于 0.5。

另外,为了提高算法的实用性,最后将明文信息熵的小数位分别提取出来,并在密钥和 LSB 嵌入算法的控制下,逐个隐藏到密文图像的透明度通道中。

3.5　解密过程

由于所提出的视觉有意义图像加密算法属于对称加密范畴,因此其相应的解密过程为各加密操作的逆过程的集合。另外,为了保证解密密钥的安全性,建议加密方采用非对称加密的方式通过公用信道将密钥传递给授权的解密方。具体的解密步骤如下所示。

步骤 1:根据协商一致的非对称加密方式解密出共享密钥并提取出密文图像透明度通道中的明文信息熵,再根据密钥生成规则构建得到受控密码流,如第 4.1 节描述所示。

步骤 2:根据索引序列 $\boldsymbol{T}_y$ 从隐写图像中逐个提取出秘密图像的各比特部分,随后再进行拼接操作。

步骤 3:在逆混合扩散操作策略的控制下,如式(14)所示,从秘密图像 $\boldsymbol{P}_4$ 中重构出矩阵 $\boldsymbol{P}_3$,紧接着再执行逆 FAN 置乱操作。

$$\begin{cases} \boldsymbol{P}_3(i) = \boldsymbol{P}_4(i) \otimes \boldsymbol{P}_4(i-1) \otimes D_x(i) \\ \qquad i = (C_R \cdot N)^2, \cdots, 3, 2 \\ \boldsymbol{P}_3(1) = \mathrm{mod}(3 \times 256 + \boldsymbol{P}_4(1) - D_x(1) - \\ \qquad \lfloor (I_P - \lfloor I_P \rfloor) \times 10^6 \rfloor, 256) \end{cases} \tag{14}$$

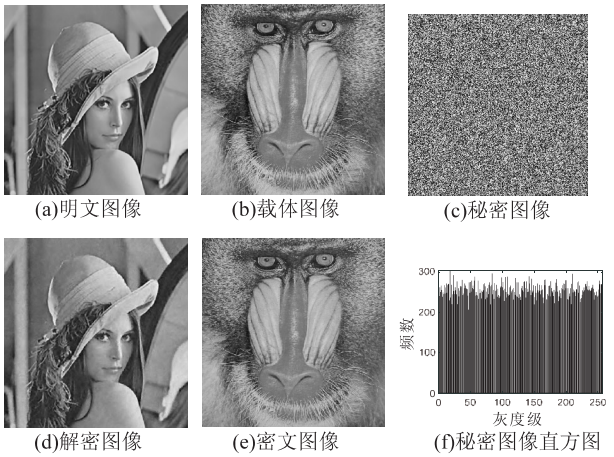
步骤 4:在对矩阵 $\boldsymbol{P}_2$ 进行逆量化操作之后,再根据文献[19]中介绍的重构算法从测量值矩阵 $\boldsymbol{P}_1$ 中恢复出明文图像,至此,解密过程结束。

4　算法仿真与性能分析

4.1　仿真结果

在本章的仿真实验中,仿真平台选为 Matlab 2020b,所设计的一维分数阶 Chebyshev 混沌映射的初始控制参数和初始状态分别为:$(\mu_0^1, \mu_0^2, \mu_0^3, \mu_0^4) = (6.372, 7.687, 5.193, 6.471)$ 和 $(x_0^1, x_0^2, x_0^3, x_0^4) = (0.759, 0.581, 0.652, 0.385)$。其他参数设置如下:$C_R = 0.5$,$d = 25$,$t_{00} = 9$,$t_{01} = 5$,$t_{10} = 11$,$t_{11} = 6$,$T_0 = 500$。另外,明文图像和载体图像分别是分辨率均为 512 × 512 的“Lena”和“Baboon”。

图 5 给出了提出的视觉有意义图像加密算法的仿真结果。由此可以看出,明文图像在经过二维压缩加密以后所生成的秘密图像的分辨率是原始的四分之一。同时,其直方图的分布近似均匀分布,表明明文图像所具有的独特统计特性被有效掩盖。其次从视觉上看,最终产生的密文图像与对应的载体图像近似,且重建得到的解密图像与明文图像相差不大。然后,通过峰值信噪比(Peak Signal-to-Noise Ratio,PSNR)和平均结构相似度(Mean Structural Similarity,MSSIM)指标来量化两幅图像之间的视觉差异(它们的数学定义请参考文献[12])。最后经过计算得出密文图像与载体图像之间的 PSNR 值和 MSSIM 值分别为 39.985 7 dB 和 0.995 3,而解密图像与明文图像之间的 PSNR 值和 MSSIM 值分别为 35.028 7 dB 和 0.910 6。从仿真实验的数值结果可以看出,在不受外界或人为干扰的情况下,所提加密算法具有不错的不可感知性和重建质量。

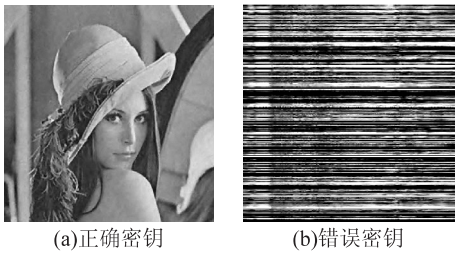


(a)明文图像　(b)载体图像　(c)秘密图像
(d)解密图像　(e)密文图像　(f)秘密图像直方图

图 5　所提加密方案的仿真结果

4.2　密钥分析

针对加密算法而言,其密钥空间和密钥敏感性共同决定其抵抗暴力攻击的级别。所提算法是在明文信息熵的控制下采用具有初值敏感性的混沌映射来构建密码流,从而保证本算法的密钥敏感性。图 6 给出了一组密钥敏感性分析的结果。其中图 6(a)是通过正确密钥从密文图像“Ba-boon”中解密得到的重建图像,而图 6(b)则是将其中的一个密钥 μ_0^1 添加一个极小的扰动(10^{-14})后所解密得到的重建图像。



(a)正确密钥　(b)错误密钥

图 6　密钥敏感性分析结果

在所设计的图像加密算法中,最主要的密钥是分数阶 Chebyshev 混沌映射的四组初始控制参数和状态。假设仿真平台的数据精度为 10^{-14},则本算法总的密钥空间为 10^{672},远大于文献[16]提出的最低密钥空

间 2^{100}。除此之外,构建混沌测量矩阵时的抽样距离 d,FAN 置乱的参数(t_{00},t_{01},t_{10},t_{11})以及量化参数均可以作为密钥。综上可知,所提出的视觉有意图像加密算法具有足够的抵抗力以抵御暴力攻击。

4.3 香农信息熵分析

信息熵是反映信息源随机性的最重要指标。它的数学定义如式(8)所示。对具有 256 位灰度级的数字图像而言,其理论值为 8。当横纵向压缩率 C_R 均为 0.75 时,且将嵌入层移除后,计算出分辨率为 512 × 512 的若干明文图像和其相应秘密图像的信息熵,数值结果如表 1 所示。从实验结果可以看出,秘密图像的信息熵均大于 7.99。另外,表 2 列出不同算法加密 Lena512 图像后生成的秘密图像的信息熵对比结果。从表中可以得知,相比于文献[13,21-23],所设计的图像加密算法具有更好的密文伪随机性。

表 1 明文图像和秘密图像的信息熵

实验用图	香农信息熵	
	明文图像	秘密图像
Lena	7.506 1	7.997 3
Girlface	7.081 8	7.997 2
Cameraman	7.091 1	7.996 9
Peppers	7.571 5	7.997 5
Coldhill	4.502 8	7.997 1

表 2 不同算法之间的信息熵对比

指标	文中算法	文献[21]的算法	文献[22]的算法	文献[23]的算法
香农信息熵	7.997 3	7.996 8	7.997 2	7.898 6

4.4 NPCR 与 UACI 分析

像素变化率(Number of Pixels Change Rate,NPCR)和归一化平均变化强度(Unified Average Change Intensity,UACI)[3]常被用来定量评估加密算法抵御差分攻击的能力。它们的数学定义可由式(15)推导出。

$$\begin{cases} V_{\mathrm{NPCR}} = \dfrac{1}{W \times H}\sum_{i,j} \mathrm{sign}(\boldsymbol{I}_1(i,j) - \boldsymbol{I}_2(i,j)) \times 100\% \\ V_{\mathrm{UACI}} = \dfrac{1}{W \times H}\left[\sum_{i,j} \dfrac{|\boldsymbol{I}_1(i,j) - \boldsymbol{I}_2(i,j)|}{255}\right] \times 100\% \end{cases} \tag{15}$$

式中,符号 $\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 记作分辨率为 $W \times H$ 的待测试图像。

实验选取四幅维度为 512 × 512 的明文图像(Lena,Baboon,Boat 和 Peppers)进行分析,并且仅将它们的第一个像素点的值加一或减一以生成相应的测试用图。最后在移除嵌入阶段的情况下根据式(15)计算得到不同明文图像所对应的 NPCR 和 UACI 值,如表 3 所示。

表 3 不同算法之间的 NPCR 和 UACI 值对比 %

明文图像	文中算法		文献[16]的算法		文献[13]的算法	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
Lena	99.649 0	33.614 8	99.620 1	34.098 5	99.569 9	33.455 8
Baboon	99.635 3	33.498 9	99.620 1	34.092 0	99.607 4	33.471 8
Boat	99.661 3	33.628 5	99.655 2	33.899 8	99.628 8	33.451 3
Peppers	99.636 8	33.621 2	99.687 2	33.029 0	99.599 8	33.496 7

从实验结果可以看出,明文图像的微小变换必将导致其所对应秘密图像发生巨大的改变,同时也说明所提算法具有足够抵御差分攻击的能力。另外,通过对比其他加密算法的实验数据可以得知,该算法的抗差分性能可以与文献[16]的媲美,且优于文献[13]。

4.5 不可感知性分析

就具有视觉安全性的图像加密算法而言,其密文图像与相应载体图像之间的视觉差异越小,则所提算法的不可感知性越强,则秘密图像被侦测到的概率越小。接下来,采用不同的加密算法分别加密若干个分辨率为 512 × 512 的明文图像并随机地嵌入到非涉密信息传输介质(载体图像)中。随后计算出不同组实验的 PSNR 值和 MSSIM 值,结果如表 4 所示。

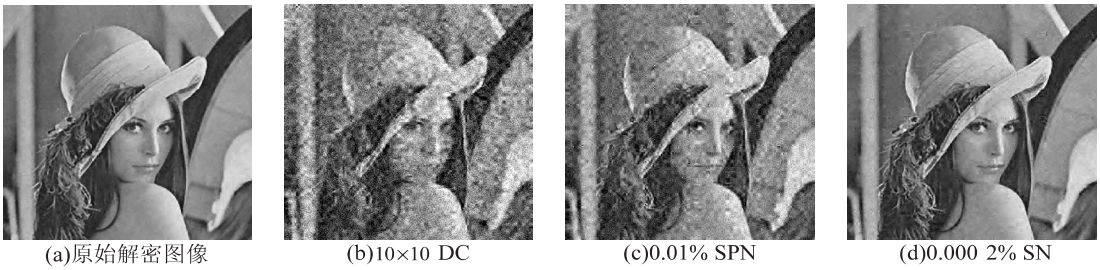
表 4 不可感知性分析的实验结果

明文图像	载体图像	峰值信噪比/dB			平均结构相似性		
		文中算法	文献[24]的算法	文献[13]的算法	文中算法	文献[24]的算法	文献[13]的算法
Lena	Girlface	45.960 7	31.048 0	31.058 2	0.932 6	0.935 6	0.892 9
Brain	Cameraman	39.445 9	31.064 8	30.896 9	0.969 0	0.972 6	0.907 6
Parrots	Bridge	39.159 7	31.755 9	31.457 0	0.994 1	0.994 5	0.978 2
Zelda	Woman	38.283 5	31.150 9	31.264 0	0.982 7	0.990 7	0.919 6
平均值		40.712 5	31.254 9	31.169 0	0.969 6	0.973 4	0.924 6

从得到的实验数据来看,相比于文献[13]所提出的基于变换域有损嵌入方法的视觉有意义图像加密算法,该文所设计的加密算法能明显得到 9 dB 左右的峰值信噪比提升。总的来说,采用最低有效位替换的嵌入方式可以有效提高所提加密算法的不可感知性。

4.6　鲁棒性分析

由于目前几乎所有的公用传输信道都是具有噪声的信道,因此密文图像须具有较强抗噪声或数据丢失的能力。也就是说当密文图像被噪声弄模糊或存在数据丢失之后,通过解密算法仍然可以从中恢复出原始图像的大部分纹理信息。另外,以分辨率为 512 × 512 的“Lena”图像作为明文图像,“Baboon”图像用作载体图像。首先,对明文图像进行加密并随机地嵌入到载体图像中的各个区域。然后,对具有视觉安全性的密文图像进行不同百分比强度的数据裁剪(Data Cropping,DC)、椒盐噪声(Salt & Pepper Noise,SPN)和斑点噪声(Speckle Noise,SN)攻击。最后,图 7 给出了使用正确密钥解密受攻击后的密文图像的实验结果。可以从图中看到,重建后的图像在视觉上仍然是有意义且可读的。这表明即使密文图像的数据发生一定程度的变化,所提出的解密算法仍然可以恢复出原始明文图像中的大部分信息。因此,所提出的算法对噪声污染和裁剪攻击具有一定的鲁棒性。



(a)原始解密图像　(b)10×10 DC　(c)0.01% SPN　(d)0.000 2% SN

图 7　鲁棒性分析的实验结果

4.7　时间复杂度分析

除了评估算法的安全性之外,加密效率对于图像加密算法来说也是一个极重要的指标。从第 3 节中可以看出,所设计的算法主要由四个部分组成。它们分别是密码流生成阶段、二维压缩阶段、图像加密阶段以及 LSB 嵌入阶段,且占用的时间复杂度分别为 $\Theta(2\cdot C_R\cdot N^2(d+C_R))$,$\Theta(2C_R\cdot N^2)$,$\Theta(C_R^2\cdot N^2)$ 和 $\Theta(C_R^2\cdot N^2)$。因此,所提的视觉有意义图像加密算法的总时间复杂度为 $\Theta(c\cdot N^2)$,其中符号 c 为某一常数。而对于相应的解密算法,其时间复杂度取决于所采用的重构算法以及是否采用并行处理架构。

表 5　不同算法的加密用时对比结果

操作阶段	加密用时/s		
	文中算法	文献[25]的算法	文献[13]的算法
压缩-加密阶段	1.246 0	0.547 1	1.281 6
LSB 嵌入阶段	1.049 4	2.018 4	0.178 2
总计	2.295 4	2.565 5	1.459 8

表 5 列出不同算法加密分辨率为 512 × 512 的“Lena”明文图像时各个阶段所消耗的时间。从得到的实验数值结果可以看出,所提加密算法的加密速度低于文献[13]中所介绍的算法,但高于文献[25]所提出的算法。因此,建议将大规模的明文图像进行分块处理之后再进行压缩加密和 LSB 嵌入以提高该算法的加密效率。一方面,可以通过降低图像块的维度来减少分数阶 Chebyshev 混沌映射的迭代次数。另一方面,图像块维度的降低可以大大节约重建过程中求解凸优化过程的耗时。

5　结束语

首先提出一种新的分数阶形式的 Chebyshev 混沌映射,并通过分岔图和李雅普诺夫指数对其性能进行评估。实验结果表明,与新提出的其他一维混沌映射相比,所设计的 FCCM 映射具有更大的混沌范围和更复杂的混沌性能。另外,在此基础上,结合二维压缩感知模型和 LSB 嵌入提出了一种基于压缩-加密-嵌入架构的视觉安全图像加密算法。该方案中,在分数阶混沌映射的控制下,通过测量矩阵、FAN 变换置乱、混沌扩散策略以及最低有效位替换嵌入完成对明文图像的双重加密。最后通过从密钥、抗差分攻击、不可感知性和加密效率等方面进行实验仿真和分析,证实所提算法在保证足够安全之外,还降低了密文图像遭到攻击的可能性。在后续的研究中,将对多幅隐私图像的安全通信进行研究以提升现有保密方案的传输效率。

参考文献:

[1] 徐　昭,周　昕,白　星,等. 基于深度学习的混沌加密灰度图像重建方法[J]. 光学与光电技术,2021,19(3):75-81.

[2] KADHIM I J,PREMARATNE P,VIAL P J,et al. Comprehensive survey of image steganography:techniques,evaluations,and trends in future research[J]. Neurocomputing,2019,335:299-326.

[3] 徐子同,高　涛,于正同,等. 基于离散型 Hopfield 神经网

络的图像加密算法[J]. 计算机技术与发展,2021,31(6):106-111.
[4] 沈子懿,王卫亚,蒋东华,等. 基于 Hopfield 混沌神经网络和压缩感知的可视化图像加密算法[J]. 计算机应用,2021,41(10):2893-2899.
[5] CHEN J X,ZHU Z L,ZHANG L B,et al. Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption[J]. Signal Processing,2018,142:340-353.
[6] YANG Y G,TIAN J,LEI H,et al. Novel quantum image encryption using one-dimensional quantum cellular automata [J]. Information Sciences,2016,345:257-270.
[7] 朱礼亚,张 曦,张 亮. 基于并行压缩感知与混沌映射的图像加密方案设计[J]. 微电子学与计算机,2019,36(10):96-102.
[8] 蒋东华,刘立东,王兴元,等. 基于细胞神经网络和并行压缩感知的图像加密算法[J]. 图学学报,2021,42(6):891-898.
[9] SHI Y D,HU Y N,WANG B. Image encryption scheme based on multiscale block compressed sensing and Markov model[J]. Entropy,2021,23:1-33.
[10] HUA Z Y,ZHANG K Y,LI Y M,et al. Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing[J]. Signal Processing,2021,183:107998.
[11] CHAI X L,GAN Z H,CHEN Y R,et al. A visually secure image encryption scheme based on compressive sensing[J]. Signal Processing,2017,134:35-51.
[12] JIANG D H,LIU L D,ZHU L Y,et al. Adaptive embedding:a novel meaningful image encryption scheme based on parallel compressive sensing and slant transform[J]. Signal Processing,2021,188:108220.
[13] ZHU L Y,SONG H S,ZHANG X,et al. A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding[J]. Signal Processing,2020,175:107629.
[14] YE G D,PAN C,DONG Y X,et al. Image encryption and hiding algorithm based on compressive sensing and random numbers insertion[J]. Signal Processing,2020,172:107563.
[15] RAHEEM Z F,SALMAN S M. On a discretization process of fractional-order Logistic differential equation[J]. Journal of the Egyptian Mathematical Society,2014,22:407-412.
[16] 蒋东华,朱礼亚,沈子懿,等. 结合二维压缩感知和混沌映射的双图像视觉安全加密算法[J]. 西安交通大学学报,2022,56(2):139-148.
[17] HUA Z Y,JIN F,XU B X,et al. 2D logistic-sine-coupling map for image encryption[J]. Signal Processing,2018,149:148-161.
[18] YEG D,PAN C,HUANG X L. A chaotic image encryption algorithm based on information entropy[J]. International Journal of Bifurcation and Chaos,2018,28(1):1-11.
[19] ZHANG B,XIAO D,XIANG Y. Robust coding of encrypted images via 2D compressed sensing[J]. IEEE Transactions on Multimedia,2021,23:2656-2671.
[20] WANG H,XIAO D,LI M,et al. A visually secure image encryption scheme based on parallel compressive sensing[J]. Signal Processing,2019,155:218-232.
[21] 李珊珊,赵 莉,张红丽. 基于猫映射的图像灰度值加密[J]. 计算机应用,2021,41(4):1148-1152.
[22] XU L,LI Z,LI J,et al. A novel bit-level image encryption algorithm based on chaotic maps[J]. Optics and Lasers in Engineering,2016,78:17-25.
[23] CHEN T H,ZHANG M,WU J H,et al. Image encryption and compression based on kronecker compressed sensing and elementary cellular automata scrambling[J]. Optics and Laser Technology,2016,84:118-133.
[24] JIANG D H,LIU L D,WANG X Y,et al. Image encryption algorithm for crowd data based on a new hyperchaotic system and Bernstein polynomial[J]. IET Image Processing,2021,15(14):3698-3717.
[25] CHAI X L,WU H Y,GAN Z H,et al. An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding[J]. Optics and Lasers in Engineering,2020,124:1-19.