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

蒋东华[1]，朱礼亚[2]，沈子懿[1]，王兴元[3]，陈颖频[4]
（1. 长安大学信息工程学院，710064，西安；2. 长安大学电子与控制工程学院，710064，西安；3. 大连海事大学信息科学技术学院，116026，辽宁大连；4. 闽南师范大学物理与信息工程学院，363000，福建漳州）

摘要：为解决图像加密技术在安全性和效率上的均衡问题，提出了一种结合压缩感知和混沌映射的双图像视觉安全加密算法。首先，通过引入非线性反馈项对经典一维 Chebyshev 混沌映射进行改进，用以构造受控测量矩阵和密码流；然后利用测量矩阵分别对两幅明文图像的整数小波系数进行二维压缩感知，并在密码流的控制下通过 Fan 变换和双向扩散过程生成秘密图像；最后，采用最低有效位嵌入算法将秘密图像信息嵌入到载体图像的像素值通道和 alpha 通道中，实现了两幅明文图像的同步压缩和视觉安全加密。实验结果表明：与采用复杂超混沌系统的单图像视觉安全加密算法相比，该算法在保证安全性的前提下，秘密信息嵌入容量扩大了一倍，加密时间开销减少 40%以上，解密图像的峰值信噪比提升了 1～7 dB。

关键词：图像加密；双向扩散；混沌映射；压缩感知
中图分类号：TP391 **文献标志码**：A
DOI：10.7652/xjtuxb202202015 **文章编号**：0253-987X(2022)02-0139-10

OSID 码

A Double Image Visual Security Encryption Algorithm Combining 2D Compressive Sensing and Chaotic Mapping

JIANG Donghua[1], ZHU Liya[2], SHEN Ziyi[1], WANG Xingyuan[3], CHEN Yingpin[4]
(1. School of Information Engineering, Chang'an University, Xi'an 710064, China;
2. School of Electronics and Control Engineering, Chang'an University, Xi'an 710064, China;
3. School of Information Science and Technology, Dalian Maritime University, Dalian, Liaoning 116026, China;
4. School of Physics and Information Engineering, Minnan Normal University, Zhangzhou, Fujian 363000, China)

Abstract: A double image visual security encryption algorithm combining compressive sensing and chaotic mapping is proposed to balance the security and efficiency of image encryption technology. Firstly, the classical one-dimensional Chebyshev chaotic map is improved by introducing a nonlinear feedback term to construct the key-controlled measurement matrixes and secret code streams. Then, the measurement matrixes are employed to compress the integer wavelet coefficients of two plain images from two directions, respectively, and under the control of the secret code streams, the compressed images are encrypted through Fan transform and bidirectional diffusion operation to generate secret images. Finally, the least significant bit embedding method is applied to randomly embed the encrypted image information into the pixel value channel and the alpha channel of any carrier image to realize the synchronization compression and visual security encryption of the two plaintext images. Simulation results show

收稿日期：2021-06-28。 作者简介：蒋东华(1996—)，男，硕士生；朱礼亚(通信作者)，男，高级工程师。 基金项目：陕西省科技计划资助项目(2021SF-483)；福建省自然科学基金资助项目(2020J05169，2020J01816)。
网络出版时间：2021-11-09 网络出版地址：http://kns.cnki.net/kcms/detail/61.1069.T.20211108.1655.010.html

that under the premise of security, the proposed algorithm could double the payload capacity of secret information, reduce the encryption time by more than 40%, and improve the peak signal-to-noise ratio of decryte image around 1～7 dB, compared with the visually secure single-image encryption scheme based on complicated hyper-chaotic system.

Keywords: image encryption; bidirectional diffusion; chaotic map; compressive sensing

随着网络、通信和多媒体技术的日益发展,数字图像以其承载信息量大、形象直观等特点,被广泛地应用于国防、经济、医学及民生等各个领域。然而,在信息共享便捷化、智能化的当下,图像在传输和存储过程中也存在着诸多安全隐患,如黑客利用网络漏洞非法窃用用户信息,窃取商业和国家机密等。因此,如何对图像的信息进行有效保护,对于个人、企业乃至国家的信息安全都具有重大的意义和研究价值。

在图像加密的实际应用场景中,往往存在信道传输带宽和存储空间受限等客观条件制约。鉴于此,将压缩感知模型与经典混沌加密技术相结合,可实现对明文图像的同步压缩和加密,以有效减少数据传输、存储和处理的压力[1-2],已成为当前信息安全领域的研究热点。例如:龚黎华等基于混沌理论、并行压缩感知和 Arnold 变换构建一种有效的图像压缩加密算法[3],以降低密文图像中相邻像素点之间的相关性;周南润等结合共稀疏表示和随机数置乱设计一种高效的双图像压缩加密算法,并采用二维 Logistic 映射来构建测量矩阵以减轻传输密钥的负担[4]。此外,通过结合混沌控制的二维压缩感知和信息熵,甘志华等提出了具有高安全性的彩色图像加密算法[5]。然而,以上加密算法均是将明文图像转换为无视觉意义的类噪声密文图像,此类具有特殊视觉特征的数字图像更容易引起攻击者的注意,从而受到诸如暴力破解,统计分析以及选择明文分析等攻击[6]。

为此,研究者们利用先加密后嵌入的方式,生成具有视觉安全的密文图像,对明文图像的数据和外在表现形式进行双重保护。Bao 等将图像加密之后嵌入到载体图像之中[7],但由于缺少压缩环节,生成的密文图像的尺寸是明文图像的 4 倍,需消耗额外的存储空间和传输带宽。为了解决该问题,文献[8-9]在 Bao 的框架中引入压缩感知模型,分别提出了两种具有视觉意义的图像加密算法。文献[8]首先通过三维离散 Cat 混沌映射构建测量矩阵,对明文图像的小波系数进行压缩测量,再在空间域上将秘密信息随机地嵌入到载体图像中;文献[9]设计了一种结合并行压缩感知和整数小波域嵌入的图像视觉安全加密算法,在频域上实现了秘密信息的嵌入。以上两种算法均在保持密文图像尺寸不变的前提下,实现了单幅明文图像的视觉安全加密。

通过以上分析可知,在基于压缩感知和混沌系统的图像加密算法中,混沌系统主要用于生成加密密码流和构建满足有限等距性质的测量矩阵[10-11],其特性将直接影响到加密算法的安全性和计算复杂度。现有的研究中多数采用高维的超混沌系统,以获得可观的安全性能增益,但同时也伴随着更大的计算开销,因此需要对混沌系统的构造进行优化,力求在算法的安全性和效率之间实现更好的均衡。另一方面,受压缩率和嵌入信息容量等因素的制约,现有的单图像视觉安全加密算法已无法满足大批量数据的高效处理需求。

为解决以上问题,本文设计了一种新颖的双图像视觉安全加密算法。首先,从算法安全性和计算复杂度之间的均衡性出发,对一维 Chebyshev 混沌映射进行了改进,即在原有映射中引入一非线性项,可在保证算法安全性的同时有效地减少计算开销;利用二维压缩感知和最低有效位嵌入技术,对两幅明文图像在两个方向上依次进行压缩,并分别嵌入到载体图像的像素值通道和 alpha 通道中,有效提升了算法的压缩性能和嵌入容量,最终实现两幅明文图像的视觉安全加密。仿真结果和性能分析表明,本文所提算法具有良好的视觉安全性、压缩性能和较高的执行效率,可为资源约束环境下的多图像信息保护提供有效的解决方案。

1 混沌理论

1.1 Chebyshev 混沌映射

Chebyshev 映射是一种以阶数为控制参数的一维混沌映射[12],其数学迭代式为

$$x_{n+1} = \cos(k\arccos(x_n)) \tag{1}$$

式中:x_{n+1}为状态变量,是该映射的迭代输出值;k为控制参数,其取值范围为[0,4]。图 1 给出了 Chebyshev 混沌映射的分岔图。从图中可以看出,该映射存在以下问题:①部分区域内存在不动点;②

存在空白窗口；③在参数 k 的整个取值范围内，满映射状态分布不均匀。

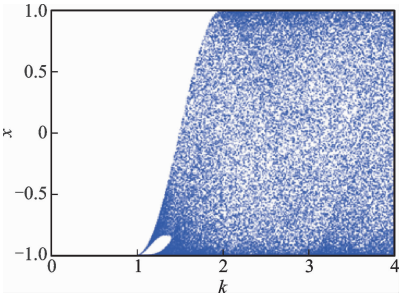


图 1　Chebyshev 混沌映射的分岔图

Fig. 1　The bifurcation diagram of Chebyshev chaotic map

1.2　改进型混沌映射

针对 Chebyshev 混沌映射存在的缺陷，本文对其系统方程进行改进，即在式(1)的基础上引入一个非线性项。改进的 Chebyshev 映射(improved Chebyshev map，ICM)系统方程

$$x_{n+1} = \cos(((4+u)\pi - u\sin(\pi x_n))\arccos(x_n)) \tag{2}$$

式中：$u \in [0,4]$ 为该改进型混沌映射的控制参数。

改进型 Chebyshev 混沌映射的分岔图如图 2 所示。由图 2 可见，在参数 u 的整个取值区间内，改进后的 Chebyshev 映射均处于满映射状态，同时不动点以及空白窗口等问题均得到解决。此外，在对应的硬件电路设计中，将 Chebyshev 混沌电路[13]中的控制项替换为带正弦函数的非线性电路，即可得到改进型 Chebyshev 混沌映射的电路。

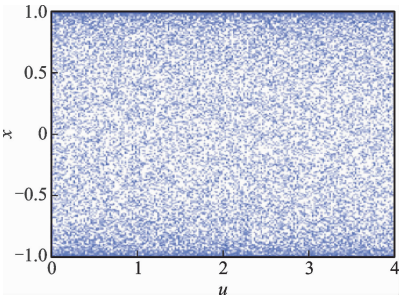


图 2　改进型 Chebyshev 混沌映射的分岔图

Fig. 2　The bifurcation diagram of ICM map

1.3　改进型混沌映射的性能分析

1.3.1　李雅普诺夫指数

对于一维混沌映射 $f(x_n)$，其李雅普诺夫指数(Lyapunov exponent，LE)可由式(3)计算得到[14]。若一个非线性动力系统的 LE 值大于 0，则该系统存在着混沌现象，表达式如下

$$L = \lim_{N\to\infty} \frac{1}{N}\sum_{n=0}^{N} \ln | f'(x_n) | \tag{3}$$

将本文改进型 Chebyshev 混沌映射的李雅普诺夫指数与文献[15-17]所提一维混沌映射的李雅普诺夫指数进行对比，实验结果如图 3 所示。

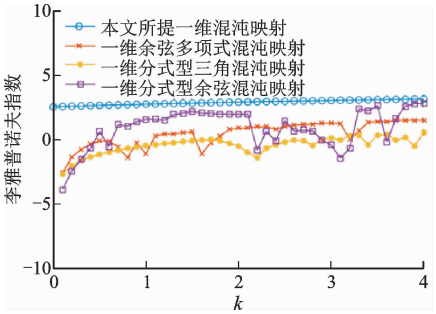


图 3　一维混沌映射的李雅普诺夫指数谱

Fig. 3　Lyapunov exponent spectrum of 1D-chaotic map

可以看出，当控制参数 $u \in [0,4]$ 时，改进型 Chebyshev 混沌映射的 LE 均大于 0，说明该映射始终处于混沌状态。相比与其他的一维混沌映射具有更大的 LE 值，表现出更为复杂的混沌特性。

1.3.2　香农熵

香农熵(SE)表征的是非线性动力系统所产生的时间序列的混乱程度[18]。对于一维混沌映射而言，如果其产生的混沌序列越有序，则相应 SE 的值越低；反之，SE 的值则越高。

对比本文改进型 Chebyshev 混沌映射和文献[15-17]所提出的一维混沌映射的香农熵，实验结果如图 4 所示。由图 4 可见，在整个区间上，改进的混沌映射的 SE 值均大于 0，说明该映射所产生的混沌序列始终处于无序的状态。同时，与其他一维混沌映射相比，改进混沌映射的 SE 值波动的范围更小，表现出更为稳定的混乱程度。

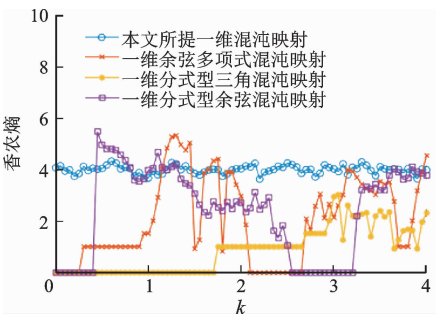


图 4　一维混沌映射的香农熵谱

Fig. 4　Shannon entropy spectrum of 1D-chaotic map

1.3.3　NIST SP800-22 测试

本小节采用美国国家标准技术研究所发布的

SP800-22 测试套件[19-20]来对改进的混沌映射的伪随机性进行测试。假设显著性水平 $\alpha=0.01$，各子项测试的实验数据见表 1。由表中数据可知，本文所提出的改进型 Chebyshev 混沌映射产生的混沌序列通过所有的随机性检验测试，说明其具有良好的伪随机特性。

表 1 NIST 随机性测试的实验数据

Table 1 Experimental data of NIST randomness test

测试项目	P 值	结果
频数检验	0.477 64	通过
分块频数检验	0.523 61	通过
前向累积和检验	0.398 29	通过
后向累积和检验	0.576 12	通过
游程检验	0.545 93	通过
最长游程检验	0.668 36	通过
二元矩阵秩检验	0.652 62	通过
离散傅里叶变换检验	0.673 25	通过
非重叠模板检验	0.775 66	通过
重叠模板检验	0.390 86	通过
通用统计检验	0.327 13	通过
近似熵检验	0.554 24	通过
随机游动检验	0.306 05	通过
随机游动状态频数检验	0.453 74	通过
序列检验	0.598 58	通过
线性复杂度检验	0.675 67	通过

2 双图像视觉安全加密算法

为在资源约束环境下实现多幅明文图像的视觉安全加密，有效提升算法的安全性、压缩性能、嵌入容量和执行效率，本文结合了改进型 Chebyshev 混沌映射和二维压缩感知技术，并利用图像的像素值通道和 alpha 通道同步嵌入多源的秘密信息，提出了一种高效的双图像视觉安全加密算法。主要包括压缩、二次加密和嵌入 3 个过程，对应的加密流程如图 5 所示。

首先，通过两个受控测量矩阵对两幅明文图像的小波系数进行二维测量，完成图像压缩和初次加密。其次，考虑到压缩感知框架的线性测量特性不能抵抗选择明文攻击[21]，再利用 FAN 变换和双向扩散对压缩图像进行二次加密，得到具有噪声形态的秘密图像。最后，利用最低有效位嵌入算法将秘密图像信息分别嵌入到载体图像的像素值通道和 alpha 通道中，以生成具有视觉意义的密文图像。此外，鉴于该嵌入算法不会导致嵌入过程中秘密图像的信息损失[10]，因此载体图像可以任意选择。假设两幅明文图像为 $\boldsymbol{P}_1\in\mathbf{N}^{N\times N}$ 和 $\boldsymbol{P}_2\in\mathbf{N}^{N\times N}$，载体图像为 $\boldsymbol{C}_1\in\mathbf{N}^{N\times N}$。

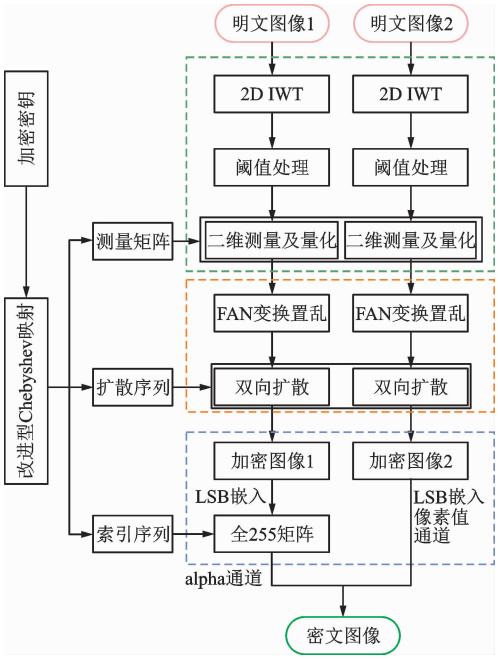


图 5 加密算法的流程图

Fig. 5 Flow chart of proposed encryption algorithm

2.1 二维压缩

步骤 1 分别对两幅明文图像 $\boldsymbol{P}_1$、$\boldsymbol{P}_2$ 进行二维整数小波分解，得到它们对应的稀疏系数矩阵 $\boldsymbol{P}_3$、$\boldsymbol{P}_4$，然后再对其进行阈值处理，相应的数学表达式为

$$\left.\begin{aligned}\boldsymbol{P}_3(\mathrm{abs}(|\boldsymbol{P}_3|)<T_1)=0\\ \boldsymbol{P}_4(\mathrm{abs}(|\boldsymbol{P}_4|)<T_2)=0\end{aligned}\right\}\tag{4}$$

式中：abs(·)表示绝对值函数；T_1 与 T_2 分别为预设的阈值。经过阈值处理后所得到的系数矩阵命名为 $\boldsymbol{P}_5$ 和 $\boldsymbol{P}_6$。

步骤 2 根据密钥 u_0、x_0、u_1、x_1 和 d 分别迭代 ICM 映射 $(N_0+dC_RN^2)$ 次，以获得两条混沌序列 $\boldsymbol{S}_1=\{x^1_{N_0+1},x^1_{N_0+2},\cdots\}$ 和 $\boldsymbol{S}_2=\{x^2_{N_0+1},x^2_{N_0+2},\cdots\}$。其中，$N_0$ 用于消除混沌映射的瞬时效应；C_R 为横向上的压缩率。

步骤 3 分别对混沌序列 $\boldsymbol{S}_1$ 和 $\boldsymbol{S}_2$ 进行抽样，从而得到两条抽样序列 $\boldsymbol{S}_3$ 和 $\boldsymbol{S}_4$。

$$\left.\begin{aligned}\boldsymbol{S}_3&=1-2\bmod(\boldsymbol{S}_1(1:d:\mathrm{end}),1)\\ \boldsymbol{S}_4&=1-2\bmod(\boldsymbol{S}_2(1:d:\mathrm{end}),1)\end{aligned}\right\}\tag{5}$$

式中：mod(·)表示取余数操作。

步骤 4 根据式(6)构建测量矩阵 $\boldsymbol{\Phi}_1$，测量矩阵 $\boldsymbol{\Phi}_2$ 同理可得。

$$\boldsymbol{\Phi}_1 = \sqrt{\frac{2}{M}} \cdot \begin{bmatrix} S_3(1) & S_3(M+1) & \cdots & S_3(M(N-1)+1) \\ S_3(2) & S_3(M+2) & \cdots & S_3(M(N-1)+2) \\ \vdots & \vdots & & \vdots \\ S_3(M) & S_3(2M) & \cdots & S_3(MN) \end{bmatrix} \tag{6}$$

步骤 5　对经过阈值处理后的系数矩阵进行二维压缩测量，其相应的数学公式如下

$$\left.\begin{aligned} \boldsymbol{P}_7 &= \boldsymbol{\Phi}_1 \boldsymbol{P}_5 \boldsymbol{\Phi}_2^{\mathrm{T}} \\ \boldsymbol{P}_8 &= \boldsymbol{\Phi}_1 \boldsymbol{P}_6 \boldsymbol{\Phi}_2^{\mathrm{T}} \end{aligned}\right\} \tag{7}$$

步骤 6　将测量后的实数矩阵 $\boldsymbol{P}_7$ 和 $\boldsymbol{P}_8$ 进行量化，获得两幅压缩图像。

$$\left.\begin{aligned} \boldsymbol{P}_9 &= \mathrm{round}\langle \frac{255(\boldsymbol{P}_7 - \min \boldsymbol{P}_7)}{\max \boldsymbol{P}_7 - \min \boldsymbol{P}_7} \rangle \\ \boldsymbol{P}_{10} &= \mathrm{round}\langle \frac{255(\boldsymbol{P}_8 - \min \boldsymbol{P}_8)}{\max \boldsymbol{P}_8 - \min \boldsymbol{P}_8} \rangle \end{aligned}\right\} \tag{8}$$

式中：round(·)表示四舍五入操作；min 和 max 分别代表取矩阵中的最小值和最大值。

2.2　二次加密

步骤 1　对压缩图像 $\boldsymbol{P}_9$ 和 $\boldsymbol{P}_{10}$ 进行 FAN 变换置乱，其中置乱过程的数学表述可由式(9)表示。

$$\begin{bmatrix} i_n \\ j_n \end{bmatrix} = \mathrm{mod}\left(\begin{bmatrix} t_{00} & t_{01} \\ t_{10} & t_{11} \end{bmatrix} \begin{bmatrix} i_{n-1} \\ j_{n-1} \end{bmatrix} + q \begin{bmatrix} N \\ N \end{bmatrix}, \begin{bmatrix} N \\ N \end{bmatrix} \right) + 1 \tag{9}$$

$$q = \max[\,|t_{00}|, |t_{01}|, |t_{10}|, |t_{11}|\,] \tag{10}$$

式中：(i_{n-1}, j_{n-1})和(i_n, j_n)分别表示置乱前后像素点的坐标。另外还须满足等式$|t_{00}t_{11} - t_{01}t_{10}| = 1$。将经过 *FAN* 置乱后所得到的矩阵命名为 $\boldsymbol{P}_{11}$ 和 $\boldsymbol{P}_{12}$。

步骤 2　根据密钥 u_2 和 x_2 迭代 ICM 混沌映射($N_0 + C_R N^2$)次，以获得序列 $\boldsymbol{S}_3 = \{x^3_{N_0+1}, \cdots, x^3_{N_0+C_R \cdot N^2}\}$。

步骤 3　根据式(11)计算得到用于双向扩散操作的扩散序列 $\boldsymbol{D}$。

$$\boldsymbol{D} = \mathrm{mod}(\boldsymbol{S}_3 + \boldsymbol{q}_0) \times 10^{10},\ 256 \tag{11}$$

步骤 4　对矩阵 $\boldsymbol{P}_{11}$ 和 $\boldsymbol{P}_{12}$ 进行双向扩散，以获得加密矩阵 $\boldsymbol{E}_3$ 和 $\boldsymbol{E}_4$。其中，式(12)(13)分别为前向扩散和后向扩散；$n = 1, 2, \cdots, 0.5C_R N^2$。

$$\left.\begin{aligned} \boldsymbol{E}_1^{(1)} &= \mathrm{mod}(\boldsymbol{B}_0 + \boldsymbol{P}_{11}^{(1)} + \boldsymbol{D}^{(1)}, 256) \\ \boldsymbol{E}_1^{(n)} &= \mathrm{mod}(\boldsymbol{E}_1^{(n-1)} + \boldsymbol{P}_{11}^{(n)} + \boldsymbol{D}^{(n)}, 256) \\ \boldsymbol{E}_2^{(1)} &= \mathrm{mod}(\boldsymbol{B}_0 + \boldsymbol{P}_{12}^{(1)} + \boldsymbol{D}^{(1)}, 256) \\ \boldsymbol{E}_2^{(n)} &= \mathrm{mod}(\boldsymbol{E}_2^{(n-1)} + \boldsymbol{P}_{12}^{(n)} + \boldsymbol{D}^{(n)}, 256) \end{aligned}\right\} \tag{12}$$

$$\left.\begin{aligned} \boldsymbol{E}_3^{(\mathrm{end})} &= \mathrm{mod}(\boldsymbol{B}_1 + \boldsymbol{E}_1^{(\mathrm{end})} + \boldsymbol{D}^{(\mathrm{end})}, 256) \\ \boldsymbol{E}_3^{(\mathrm{end}-n)} &= \mathrm{mod}(\boldsymbol{E}_3^{(\mathrm{end}-n+1)} + \boldsymbol{E}_1^{(\mathrm{end}-n)} + \boldsymbol{D}^{(\mathrm{end}-n)}, 256) \\ \boldsymbol{E}_4^{(\mathrm{end})} &= \mathrm{mod}(\boldsymbol{B}_1 + \boldsymbol{E}_2^{(\mathrm{end})} + \boldsymbol{D}^{(\mathrm{end})}, 256) \\ \boldsymbol{E}_4^{(\mathrm{end}-n)} &= \mathrm{mod}(\boldsymbol{E}_4^{(\mathrm{end}-n+1)} + \boldsymbol{E}_2^{(\mathrm{end}-n)} + \boldsymbol{D}^{(\mathrm{end}-n)}, 256) \end{aligned}\right\} \tag{13}$$

2.3　嵌入

步骤 1　为防止嵌入过程中可能发生的数据溢出，对载体图像的像素值进行缩放。

$$\boldsymbol{C}_2 = \lfloor A + 255^{-1}(\mu - A)\boldsymbol{C}_1 \rfloor \tag{14}$$

式中：$A = 10$，$\mu = 245$。

步骤 2　根据密钥 u_3 和 x_3 迭代 ICM 混沌映射($N_0 + 0.25N^2$)次，以获得序列 $\boldsymbol{S}_4 = \{x^4_{N_0+1}, \cdots, x^4_{N_0+0.25N^2}\}$。

步骤 3　按升序顺序对混沌序列 $\boldsymbol{S}_4$ 进行排序，以生成索引序列 $\boldsymbol{T}$。

步骤 4　构造元素值均为 255 的 4 个方矩阵 $\boldsymbol{W}_n \in \mathbf{N}^{0.5N \times 0.5N}$($n = 1, 2, 3, 4$)，再将载体图像 $\boldsymbol{C}_2$ 的像素值矩阵进行 4 等分分割以获得矩阵 $\boldsymbol{U}_n \in \mathbf{N}^{0.5N \times 0.5N}$，($n = 1, 2, 3, 4$)。

步骤 5　然后通过最低有效位嵌入算法将 $\boldsymbol{E}_3$ 和 $\boldsymbol{E}_4$ 分别随机地嵌入到矩阵 $\boldsymbol{W}_n$ 和 $\boldsymbol{U}_n$ 中。

$$\left.\begin{aligned} \boldsymbol{W}_1^{T(n)}(1,2) &= \boldsymbol{E}_3^n(1,2), \quad \boldsymbol{W}_2^{T(n)}(3,4) = \boldsymbol{E}_3^n(3,4) \\ \boldsymbol{W}_3^{T(n)}(5,6) &= \boldsymbol{E}_3^n(5,6), \quad \boldsymbol{W}_4^{T(n)}(7,8) = \boldsymbol{E}_3^n(7,8) \end{aligned}\right\} \tag{15}$$

$$\left.\begin{aligned} \boldsymbol{U}_1^{T(n)}(1,2) &= \boldsymbol{E}_4^n(1,2), \quad \boldsymbol{U}_2^{T(n)}(3,4) = \boldsymbol{E}_4^n(3,4) \\ \boldsymbol{U}_3^{T(n)}(5,6) &= \boldsymbol{E}_4^n(5,6), \quad \boldsymbol{U}_4^{T(n)}(7,8) = \boldsymbol{E}_4^n(7,8) \end{aligned}\right\} \tag{16}$$

式中：符号 $\boldsymbol{W}_1^{T(n)}(1,2)$ 表示矩阵 $\boldsymbol{W}_1$ 中的第 $\boldsymbol{T}(n)$ 个元素的第 1 和第 2 个比特位。

步骤 6　最后再将组合后的矩阵 $\boldsymbol{W}$ 作为 alpha 通道与组合后的矩阵 $\boldsymbol{U}$ 一起生成具有视觉意义的密文图像 $\boldsymbol{Q}$。

3　解密算法

解密方可根据密钥生成的密码流和受控测量矩阵对密文图像 $\boldsymbol{Q}$ 分别进行提取、解密及重建等逆操作，从而获得两幅解密图像，具体步骤如下。

(1)根据接收到的密钥值迭代 ICM 混沌映射以产生索引序列 $\boldsymbol{T}$、双向扩散序列 $\boldsymbol{D}$ 以及受控测量矩阵 $\boldsymbol{\Phi}_1$ 和 $\boldsymbol{\Phi}_2$。

(2)利用索引序列 $\boldsymbol{T}$ 和最低有效位提取算法从密文图像 $\boldsymbol{Q}$ 的像素值通道和 alpha 通道中提取出加密数据 $\boldsymbol{E}_3$ 和 $\boldsymbol{E}_4$。

(3)通过式(17)(18)从加密数据中求解出置乱后的矩阵 $\boldsymbol{P}_{11}$ 和 $\boldsymbol{P}_{12}$。

$$\left.\begin{aligned}
&\boldsymbol{E}_1^{(\mathrm{end})}=\mathrm{mod}(\boldsymbol{E}_3^{(\mathrm{end})}-\boldsymbol{B}_1-\boldsymbol{D}^{(\mathrm{end})},256)\\
&\boldsymbol{E}_1^{(\mathrm{end}-n)}=\mathrm{mod}(\boldsymbol{E}_3^{(\mathrm{end}-n)}-\boldsymbol{E}_3^{(\mathrm{end}-n+1)}-\boldsymbol{D}^{(\mathrm{end}-n)},256)\\
&\boldsymbol{E}_2^{(\mathrm{end})}=\mathrm{mod}(\boldsymbol{E}_4^{(\mathrm{end})}-B_1-\boldsymbol{D}^{(\mathrm{end})},256)\\
&\boldsymbol{E}_2^{(\mathrm{end}-n)}=\mathrm{mod}(\boldsymbol{E}_4^{(\mathrm{end}-n)}-E_4^{(\mathrm{end}-n+1)}-\boldsymbol{D}^{(\mathrm{end}-n)},256)
\end{aligned}\right\} \tag{17}$$

$$\left.\begin{aligned}
&\boldsymbol{P}_{11}^{(1)}=\mathrm{mod}(\boldsymbol{E}_1^{(1)}-\boldsymbol{B}_0-\boldsymbol{D}^{(1)},256)\\
&\boldsymbol{P}_{11}^{(n)}=\mathrm{mod}(\boldsymbol{E}_1^{(n)}-\boldsymbol{E}_1^{(n-1)}-\boldsymbol{D}^{(n)},256)\\
&\boldsymbol{P}_{12}^{(1)}=\mathrm{mod}(\boldsymbol{E}_2^{(1)}-\boldsymbol{B}_0-\boldsymbol{D}^{(1)},256)\\
&\boldsymbol{P}_{12}^{(n)}=\mathrm{mod}(\boldsymbol{E}_2^{(n)}-\boldsymbol{E}_2^{(n-1)}-\boldsymbol{D}^{(n)},256)
\end{aligned}\right\} \tag{18}$$

(4)对由从 FAN 变换逆置乱中得到的矩阵 $\boldsymbol{P}_9$ 和 $\boldsymbol{P}_{10}$ 进行逆量化操作。

(5)通过 2DPG-ED 重建算法[22]从压缩矩阵 $\boldsymbol{P}_7$,$\boldsymbol{P}_8$ 中恢复出稀疏系数矩阵 $\boldsymbol{P}_5$ 和 $\boldsymbol{P}_6$。

(6)对系数矩阵 $\boldsymbol{P}_5$ 和 $\boldsymbol{P}_6$ 进行二维整数小波逆变换即可得到两幅解密图像。

4 算法性能分析

4.1 仿真结果

本节的性能测试均在装有 Matlab 2018b 的笔记本电脑上运行。加密密钥和其他参数设置如下:$[u_0,u_1,u_2,u_3]=[3.799,3.987,1.293,2.471]$,$[x_0,x_1,x_2,x_3]=[0.759,0.381,-0.652,0.385]$,$[t_{00},t_{01},t_{10},t_{11}]=[9,5,11,6]$,$T_1=30$,$T_2=2$,$d=25$,$C_R=0.5$,$B_0=20$,$B_1=107$。

为了检验本文提出的双图像视觉安全加密算法的视觉安全性和压缩性能,本小节对其进行仿真实验,结果如图 6 所示。

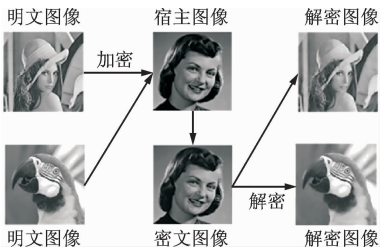


图 6 所提算法对图像 Lena 和 Parrots 的加解密结果

Fig. 6 The encryption and decryption results of proposed algorithm on images "Lena" and "Parrots"

可以看出,经过压缩-加密操作的明文图像被成功嵌入到载体图像中,加密得到的密文图像与载体图像之间无显著视觉差异。因此本文所提的加密算法可以有效保证密文图像的视觉安全性。同时解密图像可以较为清晰的显示明文图像的绝大部分信息。为定量表示本文加密算法的视觉安全性和压缩性能,分别计算出密文图像与相应载体图像之间,以及解密图像和明文图像之间的峰值信噪比(peak signal to noise ratio,PSNR)[23]。前者为 43.45 dB,后者为 33.46 dB 和 37.19 dB。定性和定量实验结果表明,本文双图像视觉安全加密算法具有良好的视觉安全性和压缩性能。

4.2 性能提升分析

在本文所提出的加密算法中,可通过设置阈值使得明文的小波系数更加稀疏从而进一步提升压缩性能。本文选用 Lena 和 Parrots 作为明文图像,Girlface 作为载体体图像,考察阈值对仿真实验结果的影响,如图 7 所示。可以看出:①阈值对解密图像质量的影响并不是单一的,当阈值的取值小于最优阈值时,随着阈值取值的增大,解密图像的质量也随之增大,反之,则随着阈值的增大而减小;②阈值对密文图像不可见性的影响可以忽略。基于此,文中的阈值设置分别为 $T_1=30$ 和 $T_2=2$。

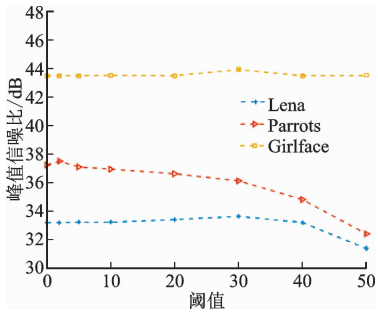


图 7 阈值对仿真结果的影响

Fig. 7 The impacts of thresholds T_1 T_2 on simulation results

混沌映射对于受控测量矩阵的有限等距性质和算法的压缩性能均有一定的影响。图 8 为 Chebyshev 混沌映射和其改进型对于压缩性能影响的走势图。从图 8 可见,在整个参数取值范围内,利用改进型混沌映射得到解密图像的视觉质量更高且变化范围更小。因此,算法的压缩性能在提升的同时更

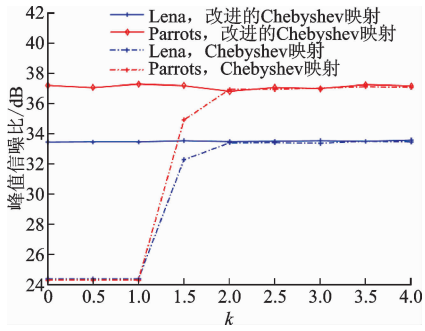


图 8 混沌映射对压缩性能的影响

Fig. 8 The impacts of chaotic map on compressive property

趋于稳定。

4.3　安全性分析

4.3.1　密钥分析

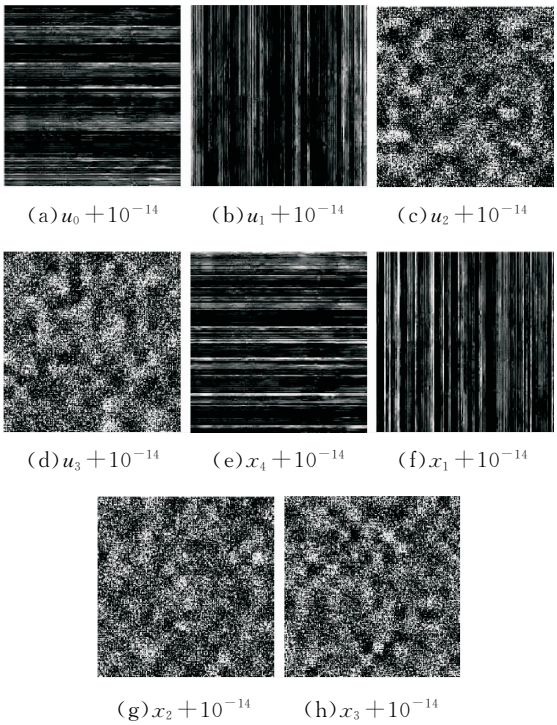
密钥空间以及密钥敏感度可表明加密算法抵抗暴力攻击的能力。本文算法的密钥主要由混沌映射的控制参数$[u_0,u_1,u_2,u_3]$与初始状态$[x_0,x_1,x_2,x_3]$组成。假设双精度数据的计算精度为10^{-14}，则本文总的密钥空间为$(10^{14})^{4\times4}\times(10^{14})^{2\times4}=10^{336}$。同时，由表 2 给出的比较结果可见，本文提出的加密算法具有更大的密钥空间。

表 2　不同加密算法中密钥空间的对比结果

Table 2　Comparison results of key space in different encryption algorithms

加密算法来源	本文	文献[10]	文献[24]	文献[25]
密钥空间/bit	10^{336}	10^{75}	2.6×10^{59}	10^{224}

对明文图像 Lena 和 Parrots 进行二维压缩、加密后随机地嵌入到载体图像 Girlface 中。分别对某一解密密钥添加一个极小的扰动，并保持其余相关密钥不变。最后使用八组错误的密钥对密文图像进行解密，结果如图 9 所示。



(a)u_0+10^{-14}　(b)u_1+10^{-14}　(c)u_2+10^{-14}

(d)u_3+10^{-14}　(e)x_4+10^{-14}　(f)x_1+10^{-14}

(g)x_2+10^{-14}　(h)x_3+10^{-14}

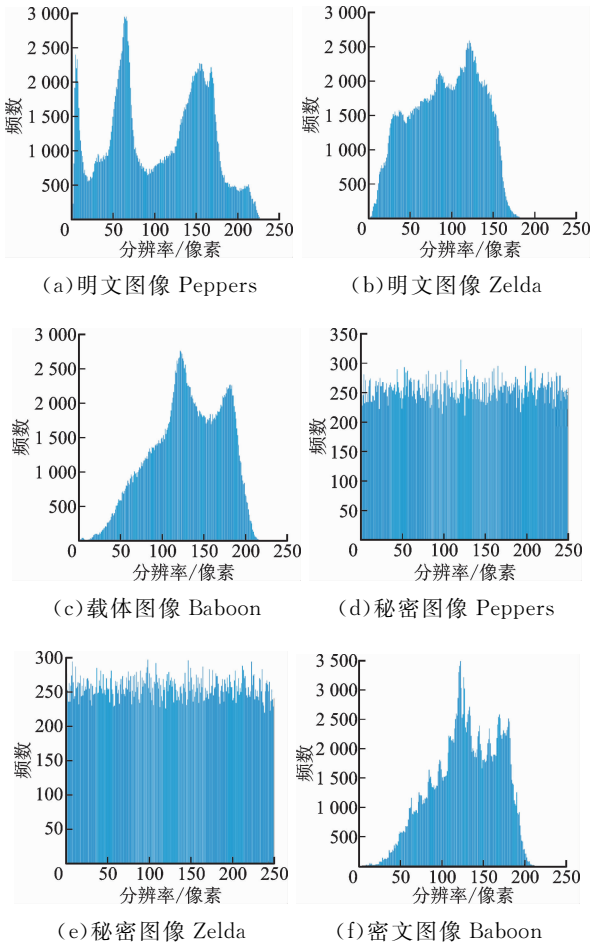
图 9　使用错误密钥所得到的解密图像

Fig. 9　Decrypted images obtained by using wrong keys

由图 9 可以看出，解密密钥的微小变化都会导致解密图像与其对应的明文图像之间存在巨大差异，无法从中提取任何有视觉意义的信息。通过上述分析，本文提出的加密算法具有较大的密钥空间和强的密钥敏感性，足以抵抗暴力攻击。

4.3.2　直方图分析

为抵抗统计攻击，一个有效的加密算法所得到的秘密图像应具有均匀的直方图分布。本小节采用分辨率为 512×512 像素的明文图像 Peppers、Zelda 和载体图像 Baboon 进行测试。实验结果如图 10 所示。可以看出，本文中加密算法生成的秘密图像的像素值趋于均匀分布。在另一方面，密文图像与载体图像的直方图高度近似，表明嵌入算法可有效保留载体图像大部分的像素值分布。



(a)明文图像 Peppers　(b)明文图像 Zelda

(c)载体图像 Baboon　(d)秘密图像 Peppers

(e)秘密图像 Zelda　(f)密文图像 Baboon

图 10　不同图像的直方图分析结果

Fig. 10　Histogram analysis results for different images

4.3.3　抗差分攻击分析

本文设计的加密算法所产生的密文图像具有视觉安全特性，因此明文图像的微小变化主要体现在秘密图像的差异上。假设 $\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$ 是两幅仅有一个比特位差异的明文图像，则其相应的抗差分攻击性能指标可以由像素变化率(I_{NPCR})和归一化平均变化强度(I_{UACI})[26]计算得到。表 3 为加密算法在抵

抗差分攻击方面的实验结果。从表中可知，本文中的密文图像的 I_{NPCR} 和 I_{UACI} 值接近于理论值 99.609 4%和 33.463 5%[24]，即明文图像的细微变化将会导致密文图像产生显著差异，这意味着加密算法对差分攻击具有很强的抵抗能力。

表 3 本文加密算法对 4 种明文图像抵抗差分攻击的实验结果

Table 3 Experimental results of proposed encryption scheme against differential attacks

抵抗差分攻击指标	Lena	Baboon	Boat	Peppers
I_{NPCR}/%	99.620 1	99.620 1	99.655 2	99.687 2
I_{UACI}/%	34.098 5	34.092 0	33.899 8	33.029 0

4.3.4 视觉安全性分析

对于视觉安全加密算法而言，密文图像与载体图像的相似度越高，算法的视觉安全性也越强。本小节将采用峰值信噪比和平均结构相似度(mean structural similarity，MSSIM)[23]来定量评估载体图像和密文图像之间的相似度。应用本文和文献[24-25]中的加密算法分别对 4 幅 512×512 像素的明文图像进行加密(其中，本文算法同时加密两幅相同的明文图像)，并计算密文图像与对应载体图像之间的 PSNR 和 MSSIM 的值，实验结果如表 4 所示。表中数据显示，与文献[24-25]相比，本文提出的加密算法在嵌入容量提升一倍的情况下，所生成的密文图像依然具有较好的视觉安全性。

表 4 视觉安全性分析的实验结果

Table 4 Experimental results of visual security analysis

分辨率/像素	明文图像	载体图像	峰值信噪比/dB			平均结构相似度		
			本文	文献[24]	文献[25]	本文	文献[24]	文献[25]
512×512	Lena	Girlface	43.446 1	31.048 0	31.058 2	0.931 9	0.935 6	0.892 9
512×512	Brain	Cameraman	37.396 2	31.064 8	30.896 9	0.968 0	0.972 6	0.907 6
512×512	Parrots	Bridge	37.419 5	31.755 9	31.457 0	0.993 5	0.994 5	0.978 2
512×512	Zelda	Woman	36.637 2	31.150 9	31.264 0	0.982 0	0.990 7	0.919 6

4.4 压缩性能分析

考虑到本文加密算法采用了有损压缩及线性量化操作，为此对多幅 512×512 像素的明文图像进行仿真实验，以定量评估加密算法的压缩性能。仿真测试所得到的实验数据如表 5 所示。此外，对比文献[24-25]的实验数据，可以看出本文提出的双图像视觉安全加密算法具有良好的压缩性能。这得益于所采用的完全可逆的嵌入和提取算法，而导致文献[24-25]压缩性能损失的因素不仅包括因量化操作而带来的截断误差，同时还有嵌入操作而带来的能量损失。

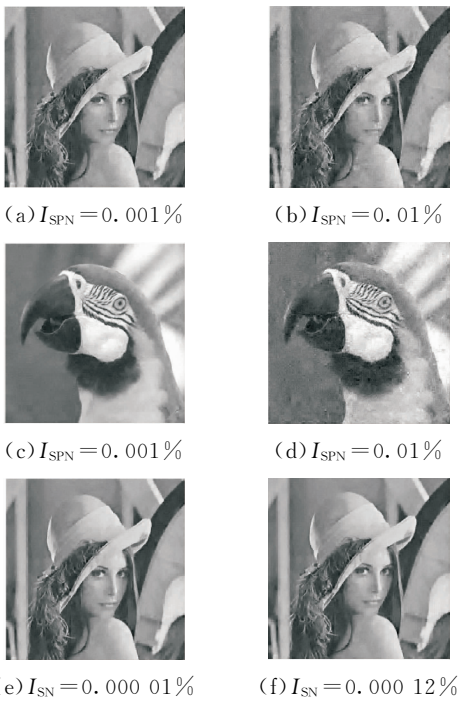
表 5 解密质量分析的实验结果

Table 5 Experimental results of decryption quality analysis

明文图像	载体图像	解密质量/dB		
		本文	文献[24]	文献[25]
Lena	Girlface	33.456 8	29.528 3	34.066 9
Brain	Cameraman	37.744 9	33.347 6	26.448 5
Parrots	Bridge	37.186 1	30.896 9	28.805 1
Zelda	Woman	34.55 67	31.869 7	34.453 2

4.5 鲁棒性分析

在信道中传输时，密文数据有可能会受到噪声的污染，为了定性评估本文算法抵抗噪声攻击的能力，对密文图像分别添加不同强度的椒盐噪声(I_{SPN})和斑点噪声(I_{SN})，实验结果如图 11 所示(明文图像 Lena 和 Parrots 分别加密并嵌入到载体图像的像素值通道和 alpha 通道中)。可以看出，本文所提出的双图像视觉安全加密算法具有一定的抗噪声干扰的能力。相比于椒盐噪声，斑点噪声对加密算法的影响更大。另外，随着噪声强度的增加，从



(a) $I_{SPN}=0.001\%$ (b) $I_{SPN}=0.01\%$

(c) $I_{SPN}=0.001\%$ (d) $I_{SPN}=0.01\%$

(e) $I_{SN}=0.000\ 01\%$ (f) $I_{SN}=0.000\ 12\%$


(g) $I_{SN}=0.000\ 01\%$


(h) $I_{SN}=0.001\ 29\%$

图 11　鲁棒性分析的实验结果

Fig. 11 Experimental results of robustness analysis

alpha 通道中提取出并解密得到的图像的视觉质量衰减的更快。

4.6　加密用时分析

本文所提双图像加密算法的时间开销主要由压缩、二次加密及嵌入用时构成。其中，二维压缩环节的时间复杂度为 $O(dC_RN^2)$；二次加密中，FAN 变换置乱和双向扩散的时间复杂度为 $O(6+C_R)N^2)$，嵌入部分对应的时间复杂度为 $O(0.75N^2)$。因此本文算法总的时间复杂度为 $O((6+C_R)N^2)$。

为定量评价本文算法的时间效率，表 6 给出了不同算法处理 512×512 像素明文图像所需时间的对比结果。可以看出，相比文献[8]、文献[24]中采用的三维和四维混沌系统，本文算法的加密用时分别减少 42%和 75%。同时，在秘密信息嵌入容量扩大一倍的情况下，嵌入用时相比文献[8]也减少了 49%。最短的总用时表明本文算法具有较高的时间效率。

表 6　加密用时对比的实验结果

Table 6 Comparison experiment results of encryption time

操作阶段	加密用时/s		
	本文	文献[8]	文献[24]
压缩-加密阶段	0.316 9	0.547 1	1.281 6
双通道嵌入阶段	1.033 9	2.018 4	0.178 2
总计	1.350 8	2.565 5	1.459 8

5　结　论

针对资源约束环境下的图像信息保护问题，本文从加密算法的安全性、压缩性能和执行效率入手，利用改进的混沌映射和二维压缩感知提出了一种高效的双图像视觉安全加密算法。与现有的单图像视觉安全加密算法相比，在加密效率、压缩性能和嵌入容量方面均有不同程度的提升。

(1)对经典的一维 Chebyshev 混沌映射进行改进，进一步提升了其混沌特性，在保证算法的安全性的同时，加密用时减少了 40%以上，加密效率明显提升。

(2)利用二维压缩感知技术对明文图像进行压缩，并结合改进混沌映射所构建的测量矩阵和阈值设置，可获得约 1～7 dB 的压缩性能增益。

(3)在载体图像像素值通道和 alpha 通道中同步嵌入两幅明文图像的秘密信息，嵌入容量扩大了一倍，同时密文图像的视觉安全性没有发生退化。

综上，本文所提出的算法具有良好的安全性、压缩性能和较高的执行效率，可在资源约束环境下实现两幅图像的同步压缩和视觉安全加密。

参考文献：

[1] 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)：200501.
SHI Hang，WANG Lidan. Multi-process image encryption scheme based on compressed sensing and multi-dimensional chaotic system [J]. Acta Physica Sinica，2019，68(20)：200501.

[2] 宫帅，霍橙，谢冬. 基于压缩感知和 DNA 编码的图像加密算法 [J]. 南京师范大学学报(工程技术版)，2021，21(1)：8-14.
GONG Shuai，HUO Cheng，XIE Dong. Image encryption algorithm based on compressed sensing and DNA coding [J]. Journal of Nanjing Normal University(Engineering and Technology Edition)，2021，21(1)：8-14.

[3] GONG Lihua，QIU Kaide，DENG Chengzhi，et al. An image compression and encryption algorithm based on chaotic system and compressive sensing [J]. Optics & Laser Technology，2019，115：257-267.

[4] ZHOU Nanrun，JIANG Hao，GONG Lihua，et al. Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging [J]. Optics and Lasers in Engineering，2018，110：72-79.

[5] GAN Zhihua，BI Jianqiang，DING Wenke，et al. Exploiting 2D compressed sensing and information entropy for secure color image compression and encryption [J]. Neural Computing and Applications，2021，33(19)：12845-12867.

[6] CHAI Xiuli，GAN Zhihua，CHEN Yiran，et al. A visually secure image encryption scheme based on compressive sensing [J]. Signal Processing，2017，134：35-51.

[7] BAO Long，ZHOU Yicong. Image encryption：generating visually meaningful encrypted images [J]. Infor-

mation Sciences, 2015, 324:197-207.

[8] CHAI Xiuli, WU Haiyang, GAN Zhihua, 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, 124:105837.

[9] WANG Hui, XIAO Di, LI Min, et al. A visually secure image encryption scheme based on parallel compressive sensing [J]. Signal Processing, 2019, 155: 218-232.

[10] CHAI Xiuli, WU Haiyang, GAN Zhihua, et al. Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy [J]. Signal Processing, 2020, 171:107525.

[11] ZHOU Nanrun, ZHANG Aidi, ZHENG Fen, et al. Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing [J]. Optics & Laser Technology, 2014, 62:152-160.

[12] 蓝婷婷, 游林, 翁昕耀. 基于 Chebyshev 混沌映射与模糊金库的指静脉安全认证方案 [J]. 通信技术, 2019, 52(6):1469-1476.
LAN Tingting, YOU Lin, WENG Xinyao. Finger vein secure authentication scheme based on Chebyshev map and fuzzy vault [J]. Communications Technology, 2019, 52(6):1469-1476.

[13] YI Renjie, CUI Chen, MIAO Yingjie, et al. A method of constructing measurement matrix for compressed sensing by Chebyshev chaotic sequence [J]. Entropy, 2020, 22(10):1085.

[14] 赵洪祥, 谢淑翠, 张建中, 等. 基于改进型 Henon 映射的快速图像加密算法 [J]. 计算机应用研究, 2020, 37(12):3726-3730.
ZHAO Hongxiang, XIE Shucui, ZHANG Jianzhong, et al. Fast image encryption algorithm based on improved Henon map [J]. Application Research of Computers, 2020, 37(12):3726-3730.

[15] TALHAOUI M Z, WANG Xingyuan, MIDOUN M A. A new one-dimensional cosine polynomial chaotic map and its use in image encryption [J]. The Visual Computer, 2021, 37(3):541-551.

[16] MIDOUN M A, WANG Xingyuan, TALHAOUI M Z. A sensitive dynamic mutual encryption system based on a new 1D chaotic map [J]. Optics and Lasers in Engineering, 2021, 139:106485.

[17] TALHAOUI M Z, WANG Xingyuan, TALHAOUI A. A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme [J]. The Visual Computer, 2021, 37(7): 1757-1768.

[18] ALAWIDA M, SAMSUDIN A, TEH J S, et al. A new hybrid digital chaotic system with applications in image encryption [J]. Signal Processing, 2019, 160: 45-58.

[19] LIU Lidong, JIANG Donghua, WANG Xingyuan, et al. 2D logistic-adjusted-Chebyshev map for visual color image encryption [J]. Journal of Information Security and Applications, 2021, 60:102854.

[20] GONG Lihua, WU Rouqing, ZHOU Nanrun. A new 4D chaotic system with coexisting hidden chaotic attractors [J]. International Journal of Bifurcation and Chaos, 2020, 30(10):2050142.

[21] ZHANG Yushu, ZHOU Jiantao, CHEN Fei, et al. Embedding cryptographic features in compressive sensing [J]. Neurocomputing, 2016, 205:472-480.

[22] ZHANG Bo, XIAO Di, XIANG Yong. Robust coding of encrypted images via 2D compressed sensing [J]. IEEE Transactions on Multimedia, 2021, 23: 2656-2671.

[23] 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/OL]. 图学学报, 2021:1-9[2021-04-26]. https://kns.cnki.net/kcms/detail/detail.aspx?FileName=GCTX20210521001&DbName=CAPJ2021.
JIANG Donghua, LIU Lidong, WANG Xingyuan, et al. Image encryption algorithm based on cellular neural network and parallel compressed sensing [J/OL]. Journal of Graphics, 2021:1-9[2021-04-26]. https://kns.cnki.net/kcms/detail/detail.aspx?FileName=GCTX20210521001&DbName=CAPJ2021.

[24] ZHU Liya, SONG Huansheng, ZHANG Xi, et al. A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding [J]. Signal Processing, 2020, 175:107629.

[25] JIANG Donghua, LIU Lidong, WANG Xingyuan, 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.

[26] 毛彦斌, 张选平, 杨晓刚. 伪 DNA 密码图像加密算法研究 [J]. 西安交通大学学报, 2015, 49(9):91-98.
MAO Yanbin, ZHANG Xuanping, YANG Xiaogang. A novel image encryption algorithm based on pseudo DNA coding [J]. Journal of Xi'an Jiaotong University, 2015, 49(9):91-98.

(编辑 刘杨)