doi:10.3969/j.issn.1672-1292.2021.01.002

基于压缩感知和 DNA 编码的图像加密算法

宫　帅,霍　橙,谢　冬

(安徽师范大学计算机与信息学院,安徽 芜湖 241002)

[摘要]　采用后稀疏化方案对待加密的明文图像做压缩感知处理,利用 DNA 编码规则与帐篷映射产生的混沌矩阵做规则运算,将单一编码多元化,对图像进行像素扩散,最后将扩散矩阵进行分割合并处理形成密文图像. 实验结果表明,提出的图像加密方案具备强的抗攻击特性和较好的重构效果.

[关键词]　压缩感知,DNA 编码,帐篷映射,图像加密

[中图分类号]TP309　[文献标志码]A　[文章编号]1672-1292(2021)01-0008-07

Image Encryption Algorithm Based on Compressed Sensing and DNA Coding

Gong Shuai, Huo Cheng, Xie Dong

(School of Computer and Information, Anhui Normal University, Wuhu 241002, China)

Abstract: In the paper, the plaintext images are firstly compressed by compressed sensing with post sparsing scheme, and then the DNA encoding rules and the chaotic matrix generated by the tent map are used to conduct regular operations to pluralize the singular encoding and diffuse the pixels of the images. Finally, the diffusion matrix is divided and merged to form a ciphertext image. The experimental results show that the proposed image encryption scheme has a stronger anti-attacking character and a better reconstructing effect.

Key words: compressed sensing, DNA coding, tent map, image encryption

压缩感知(compressed sensing,CS)理论是一种新的信号处理框架. CS 指出将信号从高维空间投影到低维空间,可同时完成采样与压缩过程. 根据投影得到的测量值求解最优化问题,便可从极少数的采样值里高概率地重构原始信号[1-3]. CS 的研究主要分为 3 类:(1)使原始信号满足某种表示方式下的稀疏性;(2)设计合适的测量矩阵使观测值能被正确恢复;(3)设计恢复算法从观测值中恢复出原始信号. CS 不局限于奈奎斯特采样定理的限制,在同样的采样值情况下,可传输更多的信号,故能更好地重构原始图像. 近些年来,基于 CS 的图像加密方案构造是图像加密领域的一大研究热点[4-7].

DNA 编码规则[8-9]是 DNA 计算应用于密码学领域的一种新思维. DNA 计算的基本原理是以 DNA 序列为载体,将要处理的信息转换为 DNA 分子序列,利用 DNA 的碱基互补配对性质与运算法则进行信息处理,具有大规模并行计算和低能耗的特点. 1994 年 Adleman 利用 DNA 碱基互补配对的思想,解决了 NP 问题的有向哈密顿问题[10],DNA 计算自此诞生. 之后,Enayatifar 等提出了基于遗传算法和 DNA 序列的图像算法[11],通过 Logistic 混沌映射与 DNA 编码得到 DNA 掩码初始值,再通过遗传算法得到最佳的掩码. 李红凯等改进了 DNA 编码的真彩图像加密算法[12],利用混沌序列为映射,对图像进行 DNA 编解码及 DNA 加操作时融入了混沌系统的随机性. 李孝东等[13]提出由图像的 SHA-256 哈希值来生成算法密钥,结合 DNA 编码、运算规则与混沌映射对图像进行逐行随机编码加密.

传统单一的加密算法密钥空间较小且加密后的密文图像相关性较高,在安全方面仍有很大的改进空间. 本文将 CS 与 DNA 编码相结合,提出了一种更加安全、高效的图像加密算法. 首先将明文图像进行 CS 压缩处理;其次,将处理后的矩阵转换并拆分为多个 2 bit 二进制矩阵;最后,根据 DNA 编码规则和 DNA 运算规则,将转换后的序列与帐篷映射产生的序列进行二次扩散,将加密后的序列先分割后合并形成矩

收稿日期:2020-05-15.

基金项目:安徽师范大学博士科研启动基金项目(751869)、安徽省自然科学青年基金项目(1808085QF211).

通讯作者:谢冬,博士,讲师,研究方向:密码学、压缩感知. E-mail:xiedong@ ahnu.edu.cn

阵,即可得到密文图像.

1　基础知识

1.1　压缩感知

CS 是在采集信号的同时对数据进行压缩处理,目的是采集尽可能少的信号并以高概率重构出原始信号.

对于一个信号 $\boldsymbol{X}\in\mathbf{R}^N$,$\boldsymbol{X}$ 中包含 k 个非零值,通过测量矩阵 $\boldsymbol{A}$ 获得 M 个线性观测量,可表示为:

$$\boldsymbol{Y}=\boldsymbol{A}\boldsymbol{X}, \tag{1}$$

式中,$\boldsymbol{A}\in\mathbf{R}^{M\times N}$,$\boldsymbol{Y}\in\mathbf{R}^{M\times 1}$.

若将测量矩阵 $\boldsymbol{A}$ 视为对称加密体制的密钥,则 CS 可视为一对称加密系统[5,7]. 如图 1 所示,$\boldsymbol{X}\in\mathbf{R}^{N\times N}$为明文图像预处理后的矩阵,$\boldsymbol{A}\in\mathbf{R}^{M\times N}$为测量矩阵,产生矩阵的初始参数可视作密钥. $\boldsymbol{Y}\in\mathbf{R}^{M\times N}$为观测矩阵,即形成的密文图像.

图 1　压缩感知的压缩(加密)过程

Fig. 1　Compression(encryption) process of compressed sensing

压缩感知的感知部分即利用设计的测量矩阵 $\boldsymbol{A}$ 和测量后的矩阵 $\boldsymbol{Y}$ 来重构原始矩阵 $\boldsymbol{X}$,进而恢复原图像. 压缩感知的重构算法主要分为 3 类:组合算法(傅里叶采样[14]、链式追踪算法[15]等)、贪婪算法(正交匹配追踪算法[16]等)、凸优化算法(基追踪算法[17]、梯度投影算法[18]等). 本文为对比实验,对计算量和精度的要求居中,故选择正交匹配追踪算法(orthogonal matching pursuit,OMP)进行重构原始图像. OMP 算法的基本思想是每次迭代选择一个与测量信号最匹配的、与当前冗余向量最大程度相关的某列进行正交化处理,求得稀疏逼近解,达到一定的阈值条件或迭代次数便可强制终止.

1.2　DNA 编码

DNA 计算以其超大规模和并行运算等特点被广泛应用于密码学中. DNA 序列的 4 种脱氧核苷酸 AGCT 互补,若二进制数据 00、01、10、11 参照 DNA 的编码方式,将会产生 4!=24 种编码方式,再根据 DNA 的碱基互补规则,会有 8 种组合方式符合互补规则[11-13],如表 1 所示.

表 1　DNA 编码规则

Table 1　DNA coding rules

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01

根据编码规则 1 进行编码组合,灰度值 200 二进制表示为 11001000;若根据编码规则 4,其可以解码成一个新的像素值 147,可二进制表示为 10010011. 因此,根据不同的编码规则,可将灰度值解码成不同的像素值. 在图像加密时可将 8 bit 像素值转化为 2 bit 的 DNA 序列进行运算. DNA 序列的加减法运算是源于二进制数据的加减法运算,若采用第一种编码方式对 DNA 进行加减运算,会产生如表 2 和表 3 所示的结果.

表 2　DNA 加法运算

Table 2　DNA addition

+	A	T	C	G
A	A	T	C	G
T	T	G	A	C
C	C	A	G	T
G	G	C	T	A

表 3　DNA 减法运算

Table 3　DNA subtraction

−	A	T	C	G
A	A	C	T	G
T	T	A	G	C
C	C	G	A	T
G	G	T	C	A

8 种不同的编码方式会产生 8 种不同的运算规则,在进行加密时通常会利用参数来进行选择 8 种编码方式的一种或者是几种混叠在一起进行加密,以达到扩散的目的.

1.3　帐篷映射

帐篷映射是一种简单且相对稳定的混沌映射[4],其表达式如下:

$$z(n+1)=\begin{cases}\dfrac{z(n)}{\mu}, & 0\leqslant z(n)<\mu;\\[2ex] \dfrac{1-z(n)}{1-\mu}, & \mu\leqslant z(n)<1.\end{cases} \tag{2}$$

式中,$\mu\in(0,1)$,$z(n)\in(0,1)$,$n=1,2,\cdots$. 系统达到混沌状态,与 Logistic 映射相比,基于混沌映射的系统具有良好的相关性且产生的随机值分布更均匀[4],故本文的混沌部分选取帐篷映射实现.

2　基于压缩感知和 DNA 编码的图像加密算法

为解决压缩感知后产生的小数和负数导致的 DNA 编码过程复杂且精度不够问题,本文采用后稀疏化对图像进行压缩感知处理,即在解密过程中对密文图像和测量矩阵稀疏化后调用 OMP 重构算法进行重构,再做逆稀疏化得到重构图像.

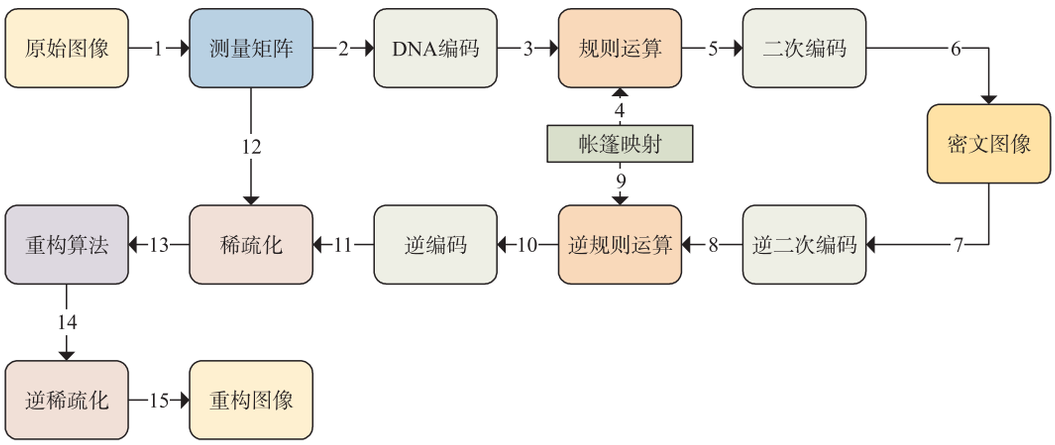


图 2　基于 CS 与 DNA 编码的图像加密方案

Fig. 2　Image encryption scheme based on CS and DNA coding

2.1　加密算法

(1)将大小为 $M\times N$ 的原始图像 I 转换为大小为 $N\times N$ 的矩阵(若 $M>N$,将其分组表示成两个 $N\times N$ 的图像;反之,则将其补成 $N\times N$ 的图像);

(2)调整产生测量矩阵算法中的参数(矩阵的行数 M 与列数 N),产生一个适当的测量矩阵 $\boldsymbol{A}$;

(3)随机选取一种编码规则,将压缩后的二维矩阵 $\boldsymbol{Y}$ 转化为 M 行 N 列 16 bit 的二进制二维矩阵 $\boldsymbol{Y}_1$;

(4)将 $\boldsymbol{Y}_1$ 拆分为 8 个 M 行 N 列 2 bit 的二进制二维矩阵,并将 8 个矩阵分别转化为 8 个 1 行 $M\times N$ 列 2 bit 的二进制序列,然后将 8 个序列合并成一个 M 行 $8\times N$ 列 2 bit 的二进制矩阵 $\boldsymbol{Y}_2$;

(5)利用帐篷映射产生一个 1 行 $8\times M\times N$ 列 2 bit 的二进制序列(产生序列时参数可调)并将其转换为 M 行 $8\times N$ 列的二维矩阵 $\boldsymbol{Z}_1$,利用 DNA 编码规则对矩阵 $\boldsymbol{Y}_2$ 和 $\boldsymbol{Z}_1$ 进行 DNA 配对加法/减法运算得到 DNA 扩散后的矩阵 $\boldsymbol{Z}_2$;

(6)选取一种不同于步骤(3)的编码规则,对矩阵 $\boldsymbol{Z}_2$ 进行二次编码,拆分转置并进行进制转换,得到新的 M 行 N 列的二维矩阵 $\boldsymbol{Z}_3$ 即为加密后的矩阵.

2.2　解密算法

(1)选取与加密过程对应的编码规则对密文图像做逆二次编码,并拆分为 8 个 M 行 N 列 2 bit 的二进制二维矩阵,将 8 个矩阵先转置再合并为一个 M 行 $8\times N$ 列 2 bit 的二进制矩阵 $\boldsymbol{Y}_2'$;

(2)将 $\boldsymbol{Y}_2'$与帐篷映射产生的矩阵 $\boldsymbol{Z}_1$ 进行 DNA 配对减法/加法运算;

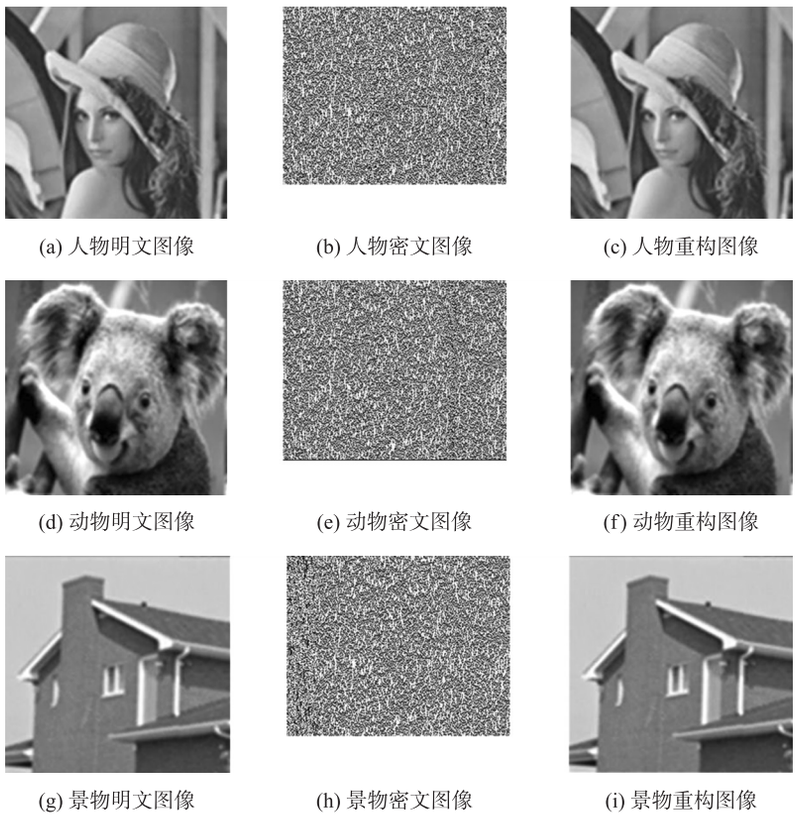
(3)对逆规则后的矩阵做逆编码处理并合并矩阵做十进制转换得到 DNA 解密后的矩阵 $\boldsymbol{Y}_1'$;

(4)对矩阵 $\boldsymbol{Y}_1'$和测量矩阵 $\boldsymbol{A}$ 做稀疏化处理并作为输入调用 OMP 重构算法;

(5)对重构后的矩阵做逆稀疏化处理得到重构图像.

3　实验仿真

为方便分析和对比,本文选取传统的基于 CS 的图像加密方案和基于 DNA 编码的图像加密方案用作对比实验,采用 256×256 的三类灰度图像(人物、动物、景物)作为实验明文图像,以 MATMAB R2013b 作为实验仿真平台对算法进行验证. 在图 3 中,$\boldsymbol{A}\in\mathbf{R}^{200\times256}$,$\boldsymbol{A}$ 中 d(稀疏度)= 160,帐篷映射 $z(0)=0.85$,$\mu=0.3$.



(a) 人物明文图像　(b) 人物密文图像　(c) 人物重构图像

(d) 动物明文图像　(e) 动物密文图像　(f) 动物重构图像

(g) 景物明文图像　(h) 景物密文图像　(i) 景物重构图像

图 3　混合加密的加密解密效果示意图

Fig. 3　Schematic diagram of the encryption and decryption effects of mixed encryption

3.1　重构图像正确性验证

从图 3 可以看出,本文所用加密算法对不同种类图像(人物、动物、景物)的加密和解密没有影响,图像加密后完全类似于噪声,视觉无法辨认,隐藏了原始信息. 加密后的图像在外界无干扰的情况下可完全恢复原始图像.

一般地,用峰值信噪比(peak signal to noise ratio,PSNR)通过量化的方法来衡量恢复的图像品质. PSNR 值是原图像与被处理图像之间的均方误差相对于$(2^n-1)^2$的对数值,单位为 dB:

$$N_{\mathrm{PSNR}}=10\log_2\left(\frac{P_{\max}^2}{V_{\mathrm{MSE}_{I,I'}}}\right), \tag{3}$$

式中,$P_{\max}$为图像的最大像素值;I 为原始图像;I'为重构图像;V_{MSE}为 I 和 I'的均方差. PSNR 值高于 40 dB,说明图像重构质量非常接近原图像;在 30~40 dB,表示图像失真但可接受;在 20~30 dB,表示图像重构质量差;低于 20 dB,表示图像不可接受. 从表 4 数据看,两种单独加密方案重构图像的 PSNR 值均在 30~40 dB,混合加密方案重构图像 PSNR 值均高于 40 dB,可知混合加密方案重构效果较好,重构图像非常接近原图像.

表 4　重构图像的 PSNR 值

Table 4　PSNR values of reconstructed images

方案	PSNR 值		
	人物	动物	景物
基于 CS	34.448 2	33.514 9	35.920 5
基于 DNA 编码	32.996 8	33.578 5	35.881 2
基于 CS 和 DNA 编码	46.098 2	44.560 0	44.194 0

3.2　密文图像相关性分析

在图像加密方案中,要求产生的密文图像具有良好的统计特性. 相关性是衡量密文图像抵抗统计学攻击的标准,好的加密效果要求相邻像素点的相关性尽可能地低. 相关性系数定义如下:

$$C=\frac{\sum_{i=1}^{K}\left(x_i-\frac{1}{K}\sum_{i=1}^{K}x_i\right)\left(y_i-\frac{1}{K}\sum_{i=1}^{K}y_i\right)}{\sqrt{\sum_{i=1}^{K}\left(x_i-\frac{1}{K}\sum_{i=1}^{K}x_i\right)^2\times\sum_{i=1}^{K}\left(y_i-\frac{1}{K}\sum_{i=1}^{K}y_i\right)^2}},\tag{4}$$

式中,K 为随机抽取的 K 对相邻像素点,本实验 $K=1\ 000$;x_i 和 y_i 是随机选择的相邻像素值. 表 5 提供了原始图像在 3 个方向上的相关性系数,表 6、表 7 和表 8 分别提供了 3 种密码方案的密文图像在 3 个方向上的相关性系数. 数据表明,混合加密方案的密文图像在 3 个方向上的相关性均较低,即密文图像具有良好的统计特性.

表 5　原始图像相关性

Table 5　Correlation of original images

图像种类	相关性系数		
	对角线	水平	垂直
人物	0.979 9	0.980 5	0.989 4
动物	0.982 0	0.989 5	0.992 3
景物	0.978 3	0.990 6	0.988 2

表 6　密文图像对角线相关性

Table 6　Diagonal correlation of ciphertext images

方案	相关性系数		
	人物	动物	景物
基于 CS	0.955 9	0.946 6	0.924 5
基于 DNA 编码	0.462 9	0.445 7	0.378 8
CS 和 DNA 编码	0.002 7	0.027 9	0.012 1

表 7　密文图像水平相关性

Table 7　Horizontal correlation of ciphertext images

方案	相关性系数		
	人物	动物	景物
基于 CS	0.990 9	0.993 8	0.994 3
基于 DNA 编码	0.460 9	0.440 0	0.383 4
CS 和 DNA 编码	0.040 3	0.007 0	0.021 1

表 8　密文图像垂直相关性

Table 8　Vertical correlation of ciphertext images

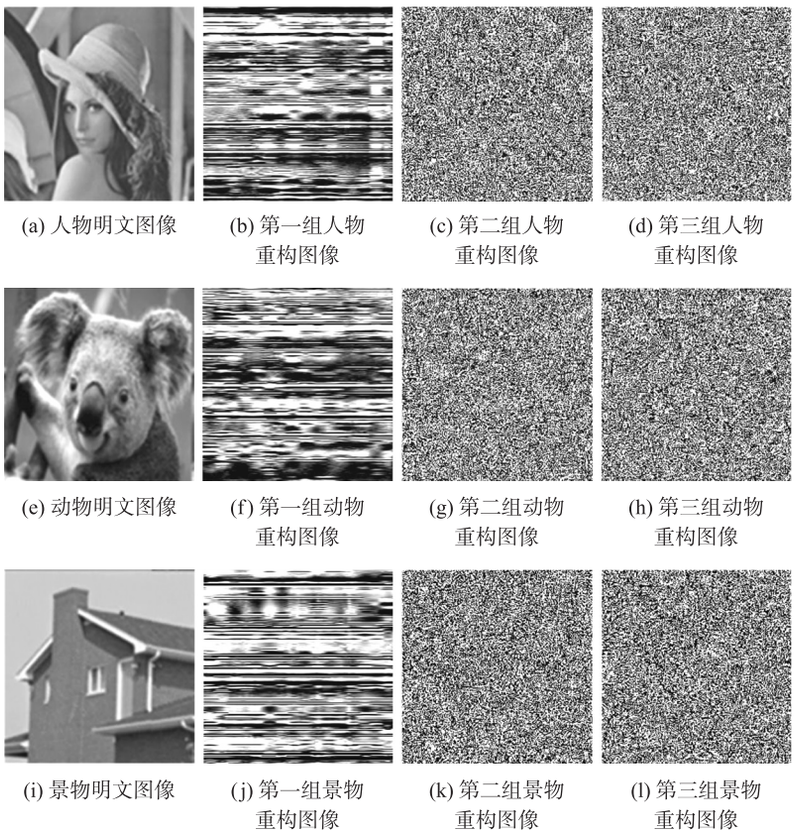
方案	相关性系数		
	人物	动物	景物
基于 CS	0.968 2	0.956 2	0.927 3
基于 DNA 编码	0.433 5	0.433 4	0.376 6
CS 和 DNA 编码	0.016 3	0.027 9	0.038 9

3.3　密文图像抗猜测攻击性分析

方案的抗猜测攻击性是指攻击者猜测的密钥与真实密钥存在一定的误差,即密钥的敏感性. 本文的抗攻击性分析分为 3 个不同的条件进行:第一组将密钥 1(测量矩阵)中的系数 d 进行细微改变,由原来的 $d=160$ 改为 $d=159$ 来重构图像,其他因素不变;第二组将密钥 2(帐篷映射产生的序列)中的初值由原来的 $z(0)=0.85$ 改为 $z(0)=0.850\ 000\ 000\ 001$ 来重构图像,其他因素不变;第三组将第一组和第二组的组合联立,即密钥 1 和密钥 2 同时改变,其他因素不变.

本文在分析时结合主观的肉眼观察和客观的 PSNR 值来区分差距,如图 4 所示,微调密钥后的重构图像与原始图像差别极大. 由表 9 中的数据可知,第一组的 PSNR 值均低于 20dB,说明重构图像效果极差,已不能接受;第二组和第三组的 PSNR 值相差极小,且均小于第一组的 PSNR 值,说明图像重构的效果更差. 实验数据表明,本文的密钥 1 和密钥 2 均具有较好的敏感性,文中的加密算法能够较好地抵抗来自密

钥的敏感性攻击,即加密算法的抗猜测攻击性强.



(a) 人物明文图像　(b) 第一组人物重构图像　(c) 第二组人物重构图像　(d) 第三组人物重构图像

(e) 动物明文图像　(f) 第一组动物重构图像　(g) 第二组动物重构图像　(h) 第三组动物重构图像

(i) 景物明文图像　(j) 第一组景物重构图像　(k) 第二组景物重构图像　(l) 第三组景物重构图像

图 4　不同类型图像的加密解密效果示意图

Fig. 4　Schematic diagram of the encryption and decryption effects of different types of images

表 9　3 组实验 PSNR 值

Table 9　The PSNR of three experiments

图像种类	PSNR 值		
	第一组	第二组	第三组
人物	16.202 5	10.926 8	10.890 3
动物	16.308 6	10.929 7	10.950 2
景物	15.766 6	10.910 6	10.924 9

4　结论

本文基于压缩感知理论与 DNA 编码运算规则,提出了一种图像加密方案,先对图像进行后稀疏化的压缩感知处理,再将压缩后的矩阵转换并拆分为多个 2 bit 二进制矩阵,使用 DNA 编码运算规则和二次编码实现对多个二进制矩阵的单独加密,从而达到对图像的像素扩散. 实验结果表明,提出的加密方案重构效果较好,且能够抵抗一些常见的攻击.

[参考文献](References)

[1] CANDES E J,ROMBERG J. Sparsity and incoherence in compressive sampling[J]. Inverse Problems,2007,23(3):969-985.

[2] CANDES E J,TAO T. Near-optional signal recovery from random projections:universal encoding strategies[J]. IEEE Transactions on Information Theory,2006,52(12):5406-5425.

[3] CANDES E J,TAO T. Decoding by linear programming[J]. IEEE Transaction on Information Theory,2005,51(12):4203-4215.

[4] XIE D,PENG H,LI L,et al. A secure and efficient scalable secret image sharing scheme with flexible shadow sizes[J]. Plos

one,2017,12(1):0168674.
[5] ZHOU N,ZHANG A,WU J,et al. Novel hybrid image compression-encryption algorithm based on compressive sensing[J]. Optik,2014,125(18):5075-5080.
[6] CAMBARERI V,MANGIA M,PARESCH F,et al. Low-complexity multiclass encryption by compressed sensing[J]. IEEE Transactions on Signal Processing,2015,63(9):2183-2195.
[7] CHAI X,GAN Z,CHEN Y,et al. A visually secure image encryption scheme based on compressive sensing[J]. Signal Processing,2017,134:35-51.
[8] ZHANG Y Q,WANG X Y,LIU J,et al. An image encryption scheme based on the MLNCML system using DNA sequences[J]. Optics and Lasers in Engineering,2016,82:95-103.
[9] 王光义,任国瑞,崔明章,等. 基于混沌占空置乱和DNA编码的图像加密算法[J]. 计算机应用与软件,2016,33(6):298-302.
[10] ADLEMAN L. Molecular computation of solution to combinatorial problems[J]. Science,1994,66(11):1021-1024.
[11] ENAYATIFAR R,ABDULLAH A H,IANIN I F. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence[J]. Optics and Lasers in Engineering,2014,56(5):83-93.
[12] 李红凯,裘国永,王涛. 基于DNA编码的随机真彩图加密算法[J]. 计算机应用研究,2016,49(1):1132-1136.
[13] 李孝东,周彩兰,黄林荃. 基于DNA编码的安全高效的图像加密算法[J]. 计算机应用与软件,2018,35(1):318-324.
[14] GILBERT A C,STRAUKRISHNAN M,STRAUSS M. Improved time bounds for near-optimal sparse Fourier representations[C]// Proceedings of SPIE Wavelets XI. San Diego,USA,2005:398-412.
[15] GILBERT A C,STRAUSS M J,TROOP J A,et al. Algorithmic linear dimension reduction in the ℓ-1 norm for sparse vectors[C]// Proceedings of the 44th Annual Allerton Conference on Communication,Control and Computing. Monticello,USA,2006.
[16] TROOP J A,GILBERT A C. Signal recovery from random measurements via orthogonal matching pursuit[J]. IEEE Transactions on Information Theory,2007,53(12):4655-4666.
[17] MALLAT S G,ZHANG Z. Matching pursuits with time-frequency dictionaries[J]. IEEE Transactions on Signal Processing,1993,41(2):3397-3415.
[18] NESTEROV Y. Gradient methods for minimizing composite objective function[J]. Mathematical Programming,2013,140(1):125-161.

[责任编辑:严海琳]