E-mail: jig@aircas.ac.cn
Website: www.cjig.cn
Tel: 010-58887035
中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS

中图法分类号:TP309.7　　**文献标识码**:A　　**文章编号**:1006-8961(2023)11-3428-12

论文引用格式:Xiao D H, Yu S M and Wang Q X. 2023. Chaotic image encryption algorithm based on elliptic curve and adaptive DNA coding. Journal of Image and Graphics, 28(11):3428-3439(肖定汉, 禹思敏, 王倩雪. 2023. 椭圆曲线与自适应DNA编码的混沌图像加密算法. 中国图象图形学报, 28(11):3428-3439)[DOI:10.11834/jig.220807]

椭圆曲线与自适应DNA编码的混沌图像加密算法

肖定汉,禹思敏,王倩雪*

广东工业大学自动化学院,广州　510006

摘　要:**目的**　当前大多数的混沌图像加密算法采用与明文相关的对称加密方式,存在密钥冗余以及一次一密模式难以实现的问题,为此,提出一种新的椭圆曲线与自适应DNA(deoxyribonucleic acid)编码结合的混沌图像加密算法。**方法**　算法利用椭圆曲线的公钥密码体制达成密钥共识,结合4维Lorenz超混沌系统产生共识密钥序列用于自适应DNA编码加密,在DNA编解码的扩散过程中内嵌中间密文状态反馈的动态扩散—自适应置换结构以抵抗分割攻击与选择明文攻击,加密过程的密文状态在解密端能够自适应同步,无需额外传输。**结果**　算法的密钥空间为2^{256},足以抵抗穷举攻击。通过对多幅不同尺寸的测试图像进行仿真,比特变化率(number of bit change rate,NBCR)均接近50%,密文各方向上的相邻像素相关性均接近于0,信息熵接近理想值8,并且全部通过NIST SP800-22随机性测试以及抗差分攻击分析。其他混沌图像加密算法进行对比分析,结果表明,本文算法具有极高的实用性和安全性。**结论**　本文算法完善了密钥冗余的问题,提高了算法的可行性,同时通过实验验证了算法的安全性,适合用于对各种尺寸的图像进行加密及相关的信息安全保障。

关键词:图像加密;椭圆曲线;超混沌系统;自适应DNA编码;动态扩散

Chaotic image encryption algorithm based on elliptic curve and adaptive DNA coding

Xiao Dinghan, Yu Simin, Wang Qianxue*

College of Automation, Guangdong University of Technology, Guangzhou　510006, China

Abstract: **Objective** With the rapid development of computer networks, digital images, as an important part of information transmission, are also widely transmitted through the Internet. Digital images used in national administration, military defense, commercial intelligence, and other fields may contain some sensitive private information. Therefore, during its transmission, the security of an image must be considered. Chaotic systems are characterized by ergodicity, sensitivity to initial conditions, and long-term unpredictability. Therefore, many scholars use these systems in designing image encryption algorithms. To resist chosen-plaintext attacks, most traditional image encryption algorithms based on the chaotic system adopt symmetric encryption methods related to plaintext information in the process of key generation or encryption. This kind of algorithm uses the same key to encrypt and decrypt information. Before transmission, the relevant key needs to be transmitted to the receiver through a secret channel. This one-time pad mode means that the number of keys that need to

收稿日期:2022-08-22;**修回日期**:2023-02-20;**预印本日期**:2023-02-27

*通信作者:王倩雪　wangqianxue@gdut.edu.cn

基金项目:国家自然科学基金项目(61901304);广东省自然科学基金项目(2022A1515010005)

Supported by: National Natural Science Foundation of China (61901304); Natural Science Foundation of Guangdong Province, China (2022A1515010005)

be stored and transmitted increases along with the number and frequency of communications. These keys do not contain information and are redundant data that bring unnecessary burden to users. In addition, the high-frequency transmission of these keys can greatly increase the risk of exposing secret channels, thus leading to adverse effects. To solve these problems, this paper proposes a chaotic image encryption algorithm based on elliptic curve and adaptive DNA coding. **Method** The proposed algorithm adopts the public key cryptosystem of an elliptic curve to make the communication parties reach the key consensus without transmitting the secret private key. To reach the goal of the key consensus, the consensus element is transformed into the initial values of the improved four-dimensional hyperchaotic Lorenz system and is then combined with the four-dimensional hyperchaotic Lorenz system to generate the consensus chaotic key sequence for adaptive DNA coding encryption. This encryption process embeds dynamic diffusion and adaptive permutation structures in the diffusion process of DNA coding and decoding. The operation rules of dynamic diffusion are dynamically selected by a chaotic key sequence, and the intermediate ciphertext state is fed back in the process. Adaptive permutation reveals the characteristics of the intermediate ciphertext state, scrambles the chaotic key sequence, and then performs bit-level permutation. Therefore, this algorithm can resist segmentation and chosen-plaintext attacks. At the same time, the intermediate ciphertext state in the encryption process can be adaptively synchronized at the decryption end without additional transmission, thereby avoiding the problem of key redundancy. **Result** Through the simulation of three test images of different sizes, this paper tests and analyzes the security of the proposed algorithm in terms of key space, key sensitivity, adjacent pixel correlation, information entropy, NIST randomness, number of pixels change rate (NPCR), and unified averaged changed intensity (UACI). Analysis results show that the key space of the algorithm reaches 2^{256}, which is sufficient to resist an exhaustive attack. The ciphertext image is extremely sensitive to the key, and a weak correlation is observed among the adjacent pixels of the ciphertext image. The information entropy of the three ciphertexts are 7.997 5, 7.999 3, and 7.999 8, which are very close to the ideal value of 8. The proposed algorithm passes all 15 sub-tests of NIST SP800-22. The test results of NPCR and UACI are also within the 0.05 confidence interval, thereby suggesting that the proposed algorithm can resist statistical and differential attacks. This algorithm is also compared with some latest chaotic image encryption algorithms. The relevant simulation tests and comparative analysis show that the chaotic image encryption algorithm has high practicability and security. **Conclusion** The proposed algorithm combines the public key cryptosystem and the chaotic system of an elliptic curve and improves the symmetric encryption model of the traditional chaotic image encryption algorithm into an asymmetric encryption model. The special design of this algorithm solves the problem of key redundancy, greatly improves its feasibility, and ensures its security. The security of this algorithm is verified by various experimental simulations, and the results are compared with those of other algorithms. This algorithm is suitable for encrypting privacy gray images of various sizes to ensure information and data security in the process of information communication.

Key words: image encryption; elliptic curve; hyperchaotic system; adaptive DNA coding; dynamic diffusion

0 引　言

随着计算机网络的飞速发展，数字图像作为信息传输的重要载体之一也在广泛地通过互联网进行传输。图像应用在国家行政、军事国防和商业情报等领域中可能包含一些敏感的隐私信息，在其传输过程中必须要考虑图像安全保密的问题，因此越来越多的研究人员加入了对图像加密算法的研究（Ghadirli等，2019）。

Fridrich（1998）提出图像加密方案应该由两个过程的迭代组成：置换和扩散。置换具有随机分离相邻图像像素的特性，而扩散可以将图像中的微小变化传递到密文图像的所有像素。混沌系统具有遍历性、对初值的敏感性和长期不可预测性等特点（禹思敏 等，2016），许多学者将之应用到图像加密算法的设计中。例如，在置换算法设计方面，有学者提出可以将混沌映射生成的伪随机序列作为密钥对图像进行行列置换（罗海波 等，2018）、块置换（Khan和Ahmad，2019）与像素级置换（周辉 等，2021）；在扩散算法设计方面，梁锡坤等人（2019）将混沌密钥矩阵与像素矩阵进行多轮非线性变换并应用取整运算来实现灰度加密。Hua等人（2019）使用高效加扰来分离相邻像素，并采用混沌序列随机顺序替换将纯

图像中的微小变化传播到密码图像的所有像素。

为了进一步提高图像加密系统的有效性和安全性，还有学者提出将混沌图像加密算法与各个领域的新技术相结合。Chai等人(2020)提出一种将压缩感知技术与混沌结合的图像加密算法，将彩色图像三色分量稀疏化，使用混沌序列对密文进行双随机像素扩散。Yang等人(2021)提出了一种将哈希散列算法与DNA(deoxyribonucleic acid)编码序列结合的图像加密方案，用散列值建立明文和密文的耦合关系，再分解明文进行加扰与DNA编解码。

这类算法使用相同的密钥加密和解密信息，为了抵抗选择明文攻击往往需要算法密钥或加密过程与明文信息相关，这种一次一密的加密模式意味着每次通信之前需要先将相关密钥通过秘密信道传输给通信对象，随着通信对象与频率的增加，需要保管与传输的密钥数量也会增加，此外，密钥的高频传输也会增加秘密信道暴露的风险。

针对上述问题，有些学者提出将椭圆曲线密码学(elliptic curve cryptography，ECC)与混沌对称加密相结合。椭圆曲线公钥加密是一种非对称的加密方式，基于离散对数难解问题产生公私密钥对，公钥对外公开使用，私钥由自己妥善保管，由私钥可以计算公钥，而根据公钥不能逆推得到私钥。加密时，使用公钥加密，私钥解密。Sasikaladevi等人(2020)提出一种混合双层超混沌超椭圆曲线的图像加密方案，在第1层中基于超混沌序列进行DNA编码，在第2层中基于Genus-2超椭圆曲线进行加密。Ye等人(2022)提出了一种基于压缩感知和公钥椭圆曲线的双图像加密算法，对明文图像进行离散小波变换(discrete wavelet transform，DWT)处理，然后对量化矩阵进行压缩感知并拼接在一起，最后对新矩阵进行椭圆曲线加密。Liang等人(2021)提出一种公钥图像加密方法，对明文图像导出的用于产生混沌序列的哈希值进行ECC加密，然后根据不同位所包含的信息量将明文图像分为5个平面进行置换—扩散加密后再组合。

基于此，本文提出了一种新的椭圆曲线与自适应DNA编码的混沌图像加密算法。算法通过椭圆曲线公钥加密与混沌系统的结合，使通信双方不需要传输密钥就能达成密钥共识，并通过DNA自适应编码的中间密文状态反馈的方式提升算法的抵抗选择明文攻击的能力，最后，密文状态可以自适应同步无需额外传输。

1 相关知识

1.1 椭圆曲线

定义(Koblitz等，2000) p 是一个素数且 $p>3$，在素数 p 的有限域 $\boldsymbol{GF}(p)$ 上定义的椭圆曲线指的是所有满足Weierstrass标准形式方程的点 (x,y) 再加上一个称为零点或无穷远点的元素 O 构成的集合 $\boldsymbol{E}_p(a,b)$。具体为

$$y^2=\left(x^3+ax+b\right)\bmod p \tag{1}$$

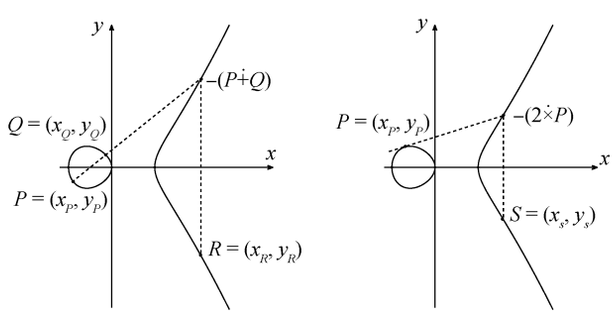
式中，$x,y,a,b\in\boldsymbol{GF}(p)$，$a,b$ 是常数且满足条件 $\Delta=4a^3+27b^2\neq 0$。基于椭圆曲线 $\boldsymbol{E}_p(a,b)$ 定义一个加法运算，用符号“$\dot{+}$”表示，若椭圆曲线的3个点同在一直线上，则它们的和为 O。假设点 $P=\left(x_P,y_P\right)$ 和 $Q=\left(x_Q,y_Q\right)$ 是 $\boldsymbol{E}_p(a,b)$ 中的点，从上面定义出发可以得到椭圆曲线加法的运算规则：

1) O 为加法的单位元，对椭圆曲线上的任一点 P，有 $P\dot{+}O=P$。

2)点 P 的负元为 $\dot{-}P=\left(x_P,\ -y_P\right)$，且 $P\dot{+}(\dot{-}P)=P\dot{-}P=O$。

3)要计算坐标不同且不互为负元的两点 P 和 Q 之和，即 $P\dot{+}Q$，如图1(a)所示，连接 PQ 作延长线与椭圆曲线的新交点的负元 $R=\left(x_R,y_R\right)$ 即为结果。$R(x_R,y_R)=P(x_P,y_P)\dot{+}Q(x_Q,y_Q)$ 的代数计算表达式可由上述定义得到，即

$$\begin{cases}x_R=(\lambda^2-x_P-x_Q)\bmod p\\ y_R=(\lambda(x_P-x_R)-y_P)\bmod p\end{cases} \tag{2}$$



(a) 相加：$P\dot{+}Q$　　(b) 倍加：$2\dot{\times}P$

图1　加法运算规则

Fig. 1　Addition operation rules

((a) add: $P\dot{+}Q$; (b) doubling point: $2\dot{\times}P$)

式中，$\lambda = \left(\frac{y_Q - y_P}{x_Q - x_P}\right) \bmod p$。

4）要计算点P的两倍，即$S = P + P = 2 \times P$，如图1（b）所示，作点P切线与椭圆曲线的新交点的负元$S = (x_S, y_S)$即为结果。$S(x_S, y_S)$的代数计算表达式为

$$\begin{cases} x_S = (\lambda^2 - x_P - x_P) \bmod p \\ y_S = (\lambda(x_P - x_S) - y_P) \bmod p \end{cases} \tag{3}$$

式中，$\lambda = \left(\frac{3x_P^2 + a}{2y_P}\right) \bmod p$。

当椭圆曲线$\boldsymbol{E}_p(a, b)$上存在一点G满足

$$n \times G = \underbrace{G + G + \cdots + G}_{n} = O \tag{4}$$

则所有$k \times G(k = 1, 2, \cdots, n)$构成的集合是$\boldsymbol{E}_p(a, b)$上的一个循环子群$\boldsymbol{F}$，点$G$称为该群的一个生成元，$n$也称为生成元$G$的阶。对循环子群$\boldsymbol{F}$里的任意点$T$，皆满足

$$k \times G = T(1 \leqslant k \leqslant n) \tag{5}$$

已知系数k和生成元G时容易计算得到点T，而已知点G和点T时欲计算得到系数k则非常困难，这个难解问题也称为椭圆曲线离散对数问题（elliptic curve discrete logarithm problem，ECDLP）（Li 等，2012）。

1.2 DNA编码

DNA是一种双链结构的高分子化合物，含有4种碱基：腺嘌呤（A）、鸟嘌呤（G）、胞嘧啶（C）和胸腺嘧啶（T），其中，A与T互补，C与G互补。一幅原始灰度图像的像素值在0～255之间，可由8位二进制数表示，又因为在二进制数中0与1是互补的，所以00和11，01和10也对应是互补的，如果用00、01、10、11分别表示碱基A、G、C、T，那么每一个像素值都对应一条含有4个碱基的DNA序列，根据以上的互补规则，DNA编码规则有8种（周辉 等，2021），如表1所示。

表1 DNA编码规则

Table 1 DNA encoding 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

为了便于DNA计算在密码学中的应用，对DNA碱基引入了加法运算和减法运算，符号表示为“⊞”与“⊟”，规则如表2和表3所示。

表2 DNA加法运算

Table 2 DNA addition operation

⊞	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

表3 DNA减法运算

Table 3 DNA subtraction operation

⊟	A	G	C	T
A	A	G	C	T
G	T	A	G	C
C	C	T	A	G
T	G	C	T	A

1.3 4维Lorenz超混沌系统

在本文加密算法中，对3维Lorenz混沌系统添加并耦合额外的状态变量获得4维超混沌系统用于生成密钥序列（Lin和Li，2021），其方程定义为

$$\begin{cases} \dot{x} = a(y - x) + w \\ \dot{y} = cx - y - xz \\ \dot{z} = xy - bz \\ \dot{w} = -yz + rw \end{cases} \tag{6}$$

式中，变量上方的“·”表示迭代值。令$a = 10$，$b = 8/3$，$c = 28$，当$-1.52 \leqslant r \leqslant -0.06$时，该系统为超混沌系统。本文选取$r = -1$，系统的4个李雅普诺夫指数分别为$\lambda_{LE1} = 0.3381$、$\lambda_{LE2} = 0.1586$、$\lambda_{LE3} = 0$与$\lambda_{LE4} = -15.1752$。系统的初值范围分别为$x_0 \in (-40, 40)$，$y_0 \in (-40, 40)$，$z_0 \in (1, 81)$与$w_0 \in (-250, 250)$。

2 图像加解密算法

本文加密算法设计如图2所示。首先通信双方分别随机生成自己的私钥并通过椭圆曲线算法产生并对外发布相应公钥，双方取得对方的公钥后与自己的私钥相结合达成密钥共识并生成混沌密钥序列，然后发送者使用共识密钥序列对明文图像进行

DNA自适应编码加密并传输给接收者，接收者接收到密文图像后使用共识密钥进行相应解密操作即可得到解密图像。算法将对称的混沌加密模式转变成非对称形式，通信双方仅需要妥善保存私钥。此算法通过安全的公钥保障保密通信，解决了大量冗余密钥的管理与分发问题。

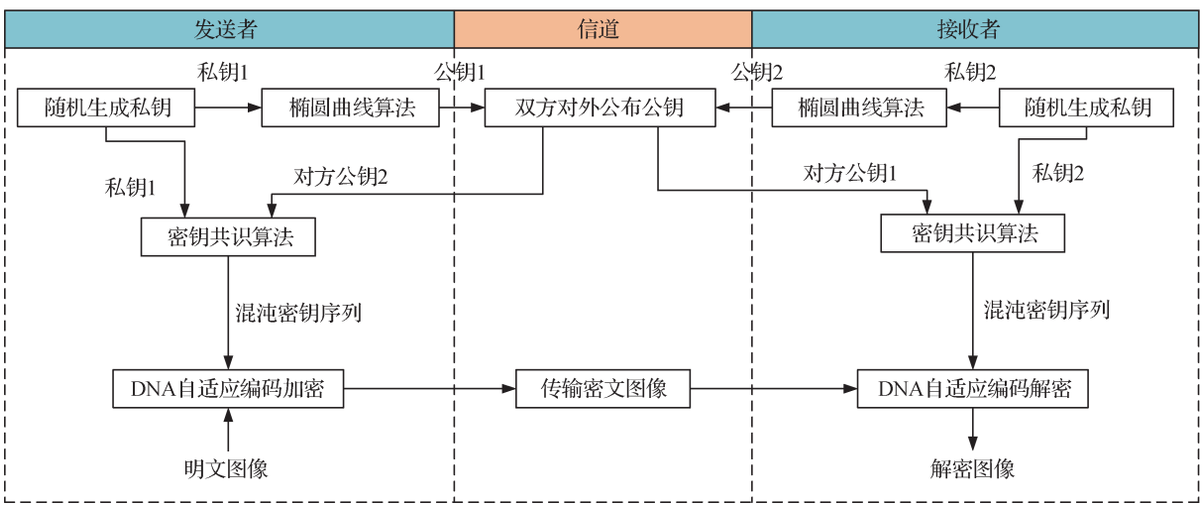


图2　加密算法设计图

Fig. 2　Design of encryption algorithm

2.1　密钥共识算法

密钥共识算法通过椭圆曲线的公钥密码体制产生混沌系统的初始值，再由混沌系统根据图像尺寸生成相应长度的混沌密钥序列用于DNA自适应编码加密。

1）产生公私密钥对。记椭圆曲线上的点G的阶n是使得$n \times G = O$成立的最小正整数。$\boldsymbol{E}_p(a,b)$和G是该密码体制种通信各方均已知的参数。发送者与接收者随机生成的私钥分别为k_a和k_b，应用椭圆曲线算法计算产生相应的公钥T_a和T_b，即

$$\begin{cases} T_a = k_a \dot{\times} G \\ T_b = k_b \dot{\times} G \end{cases} \tag{7}$$

2）公布公钥并达成元点共识。通信双方通过公共信道公布公钥，将对方的公钥与自己的私钥相结合得到共识元点(k_x, k_y)。即

$$(k_x, k_y) = k_a \dot{\times} T_b = k_b \dot{\times} T_a = (k_a \times k_b) \dot{\times} G \tag{8}$$

3）计算混沌系统初值。本算法中的椭圆曲线密钥长度为256 bit，故共识元点(k_x, k_y)的坐标值长度亦为256 bit，将k_x与k_y分割（|）成4块64位二进制数，具体为

$$\begin{cases} k_x = k_{x,1} \| k_{x,2} \| k_{x,3} \| k_{x,4} \\ k_y = k_{y,1} \| k_{y,2} \| k_{y,3} \| k_{y,4} \end{cases} \tag{9}$$

然后，纠缠量化成混沌系统初值，具体为

$$\begin{cases} x_0 = \dfrac{k_{x,1} \oplus k_{y,4}}{2^{64}} \times 80 - 40 \\ y_0 = \dfrac{k_{x,2} \oplus k_{y,3}}{2^{64}} \times 80 - 40 \\ z_0 = \dfrac{k_{x,3} \oplus k_{y,2}}{2^{64}} \times 80 + 1 \\ w_0 = \dfrac{k_{x,4} \oplus k_{y,1}}{2^{64}} \times 500 - 250 \end{cases} \tag{10}$$

式中，符号$\oplus$表示异或运算。

4）生成混沌密钥序列。假定原始明文图像$\boldsymbol{P}_0$的像素数为$m \times n$，将初值代入式（6）的混沌系统中进行迭代，舍去前300个值避免瞬态效应，迭代$4 \times m \times n$次生成4个伪随机序列$\boldsymbol{X}$、$\boldsymbol{Y}$、$\boldsymbol{Z}$和$\boldsymbol{W}$，变换生成密钥序列$\boldsymbol{X}'$、$\boldsymbol{Y}'$、$\boldsymbol{Z}'$和$\boldsymbol{W}'$，具体为

$$\begin{cases} \boldsymbol{X}'(i) = \lfloor \boldsymbol{X}(i) \times 10^{14} \rfloor \bmod 8 + 1 \\ \quad i = 1, 2, \cdots, 4 \times m \times n \\ \boldsymbol{Y}'(i) = \lfloor \boldsymbol{Y}(i) \times 10^{14} \rfloor \bmod 4 + 1 \\ \quad i = 1, 2, \cdots, 4 \times m \times n \\ \boldsymbol{Z}' = sort(\boldsymbol{Z}) \\ \boldsymbol{W}'(i) = \lfloor \boldsymbol{W}(i) \times 10^{14} \rfloor \bmod 8 + 1 \\ \quad i = 1, 2, \cdots, 4 \times m \times n \end{cases} \tag{11}$$

式中，符号$\lfloor \cdot \rfloor$表示向下取整运算，$sort(\cdot)$表示对矩阵进行排序并输出索引值序列。

2.2　DNA自适应编码

DNA自适应编码流程如图3所示，共识混沌密

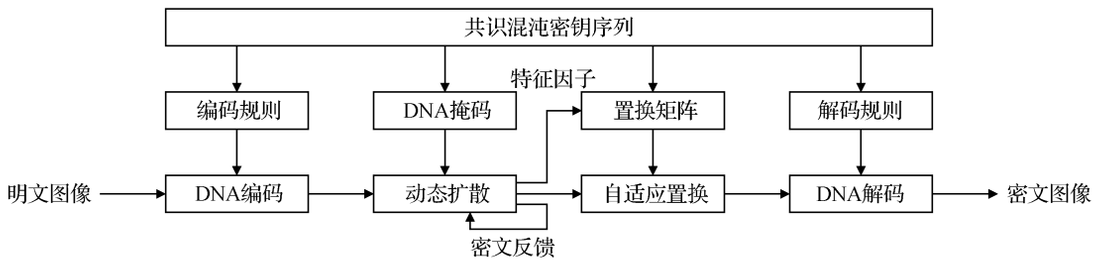


图 3　DNA 自适应编码流程图

Fig. 3　Flow chart of DNA adaptive coding

钥序列作为加密密钥，在 DNA 编码与解码的扩散过程中嵌入动态扩散—自适应置换环节，其中动态扩散环节具有密文反馈与掩码动态选择扩散规则的特点，自适应置换环节通过提取扩散密文特征因子来对密钥进行自适应加扰。

1）DNA 编码。将密钥序列 $\boldsymbol{X}'$ 作为编码规则密钥，每 4 个密钥对应将 1 个明文像素值编码生成 4 个 DNA 碱基，像素数为 $m \times n$ 的明文图像 $\boldsymbol{P}_0$ 经过 DNA 编码后得到像素数为 $m \times 4n$ 的编码矩阵 $\boldsymbol{E}_{\text{code}}$，即

$$\boldsymbol{E}_{\text{code}} = encode(\boldsymbol{P}_0, \boldsymbol{X}') \tag{12}$$

式中，$encode(\cdot)$ 表示 DNA 编码运算。

2）生成掩码矩阵 $\boldsymbol{M}_{\text{code}}$。按式（12）将密钥序列 $\boldsymbol{Y}'$ 按光栅扫描顺序变换成 $m \times 4n$ 的 DNA 掩码矩阵 $\boldsymbol{M}_{\text{code}}$，即

$$\boldsymbol{M}_{\text{code}}(i) = \begin{cases} \text{A} & \boldsymbol{Y}'(i) = 1 \\ \text{G} & \boldsymbol{Y}'(i) = 2 \\ \text{C} & \boldsymbol{Y}'(i) = 3 \\ \text{T} & \boldsymbol{Y}'(i) = 4 \end{cases}$$

$$i = 1,2,\cdots,4 \times m \times n \tag{13}$$

3）动态扩散。将掩码矩阵 $\boldsymbol{M}_{\text{code}}$ 元素作为扩散因子与规则动态选择因子，同时将前一个像素加密的结果反馈到下一个像素的加密过程中。对编码矩阵 $\boldsymbol{E}_{\text{code}}$ 进行动态扩散得到扩散密文 $\boldsymbol{E}_{\text{diff}}$，具体为

$$\boldsymbol{E}_{\text{diff}}(i) = \begin{cases} \boldsymbol{E}_{\text{code}}(i) \boxplus \boldsymbol{E}_{\text{diff}}(i-1) \boxplus \boldsymbol{M}_{\text{code}}(i) & \boldsymbol{M}_{\text{code}}(i) = \text{A} \\ \boldsymbol{E}_{\text{code}}(i) \boxplus \boldsymbol{E}_{\text{diff}}(i-1) \boxminus \boldsymbol{M}_{\text{code}}(i) & \boldsymbol{M}_{\text{code}}(i) = \text{G} \\ \boldsymbol{E}_{\text{code}}(i) \boxminus \boldsymbol{E}_{\text{diff}}(i-1) \boxplus \boldsymbol{M}_{\text{code}}(i) & \boldsymbol{M}_{\text{code}}(i) = \text{C} \\ \boldsymbol{E}_{\text{code}}(i) \boxminus \boldsymbol{E}_{\text{diff}}(i-1) \boxminus \boldsymbol{M}_{\text{code}}(i) & \boldsymbol{M}_{\text{code}}(i) = \text{T} \end{cases} \tag{14}$$

式中，$i = 1, 2, \cdots, 4 \times m \times n$，“$\boxplus$”和“$\boxminus$”运算为表 2 和表 3 所示的 DNA 碱基加减法运算。且当 $i = 0$ 时，$\boldsymbol{E}_{\text{diff}}(0) = \boldsymbol{E}_{\text{code}}(4 \times m \times n)$。

4）自适应置换。统计扩散密文 $\boldsymbol{E}_{\text{diff}}$ 中 4 种 DNA 碱基的个数 $n_{\text{A}}, n_{\text{G}}, n_{\text{C}}, n_{\text{T}}$，并量化为特征密钥因子。具体为

$$\begin{aligned} r_1 &= n_{\text{A}} \bmod m, \quad t_1 = n_{\text{A}} \bmod 4n \\ r_2 &= n_{\text{G}} \bmod m, \quad t_2 = n_{\text{G}} \bmod 4n \\ c_1 &= n_{\text{C}} \bmod 4n, \quad t_3 = n_{\text{C}} \bmod m \\ c_2 &= n_{\text{T}} \bmod 4n, \quad t_4 = n_{\text{T}} \bmod m \end{aligned} \tag{15}$$

然后，应用特征密钥因子对密钥序列 $\boldsymbol{Z}'$ 进行自适应加扰：将密钥序列 $\boldsymbol{Z}'$ 重排成 $m \times 4n$ 的矩阵，将第 1 行到第 r_1 行元素每行循环左移 t_1 位；将第 r_2 行到最后一行元素每行循环右移 t_2 位；将第 1 列到第 c_1 列元素每列循环上移 t_3 位；将第 c_2 列到最后一列元素每行循环下移 t_4 位。将加扰后的密钥矩阵 $\boldsymbol{Z}''$ 元素作为置换因子对扩散密文 $\boldsymbol{E}_{\text{diff}}$ 进行自适应置换得到置换密文 $\boldsymbol{E}_{\text{scra}}$，具体为

$$\boldsymbol{E}_{\text{scra}}(i) = \boldsymbol{E}_{\text{diff}}(Z''(i)), \quad i = 1,2,\cdots,4 \times m \times n \tag{16}$$

此置换过程仅改变了扩散密文中各元素的位置而不改变其值，在解密时可以从密文中获得同样的特征密钥因子，故称为自适应置换。

5）DNA 解码。将密钥序列 $\boldsymbol{W}'$ 作为解码规则密钥，对置换密文 $\boldsymbol{E}_{\text{scra}}$ 进行 DNA 解码得到密文图像 $\boldsymbol{C}$，尺寸恢复为 $m \times n$，具体为

$$\boldsymbol{C} = decode(\boldsymbol{E}_{\text{scra}}, \boldsymbol{W}') \tag{17}$$

式中，$decode(\cdot, \cdot)$ 表示 DNA 解码运算。

DNA 自适应编码加密过程具有对称性，它的解密过程就是加密的逆过程。首先，将加密过程中的解码密钥序列 $\boldsymbol{W}'$ 作为编码规则密钥对密文图像进行 DNA 编码。统计各碱基个数获得特征密钥因子对密钥序列 $\boldsymbol{Z}'$ 加扰并进行逆置换。然后使用密钥序列 $\boldsymbol{Y}'$ 同样地生成掩码矩阵 $\boldsymbol{M}_{\text{code}}$ 进行逆扩散，逆扩散过程为

$$\boldsymbol{E}_{\text{code}}(i) = \begin{cases} \boldsymbol{E}_{\text{diff}}(i) \boxminus \boldsymbol{E}_{\text{diff}}(i-1) \boxminus \boldsymbol{M}_{\text{code}}(i) & \boldsymbol{M}_{\text{code}}(i) = \text{A} \\ \boldsymbol{E}_{\text{diff}}(i) \boxminus \boldsymbol{E}_{\text{diff}}(i-1) \boxplus \boldsymbol{M}_{\text{code}}(i) & \boldsymbol{M}_{\text{code}}(i) = \text{G} \\ \boldsymbol{E}_{\text{diff}}(i) \boxplus \boldsymbol{E}_{\text{diff}}(i-1) \boxminus \boldsymbol{M}_{\text{code}}(i) & \boldsymbol{M}_{\text{code}}(i) = \text{C} \\ \boldsymbol{E}_{\text{diff}}(i) \boxplus \boldsymbol{E}_{\text{diff}}(i-1) \boxplus \boldsymbol{M}_{\text{code}}(i) & \boldsymbol{M}_{\text{code}}(i) = \text{T} \end{cases} \tag{18}$$

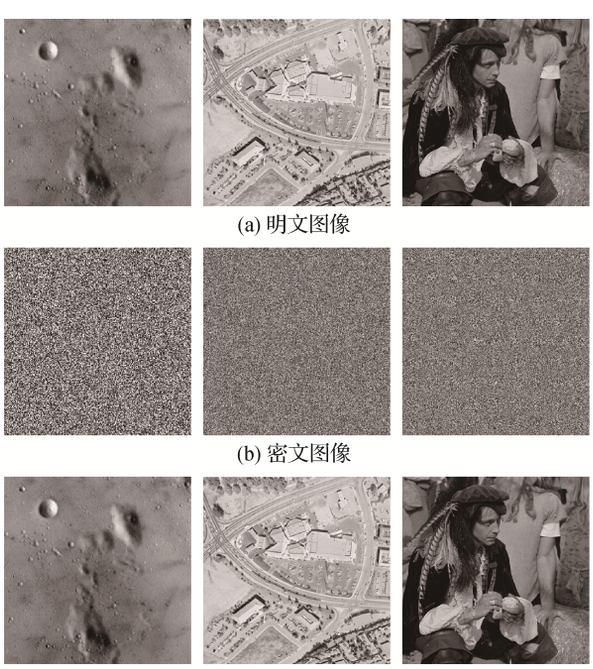
式中，$i = 4 \times m \times n, 4 \times m \times n - 1, \cdots, 1$，当 $i = 0$ 时，$\boldsymbol{E}_{\text{diff}}(0) = \boldsymbol{E}_{\text{code}}(4 \times m \times n)$。最后将加密过程中的编码密钥序列 $\boldsymbol{X}'$ 作为解码规则密钥进行DNA解码即可获得解密图像。

3 仿真结果及安全性分析

使用算法对USC-SIPI“Miscellaneous”图像数据集中的3幅像素数分别为256 × 256、512 × 512和1 024 × 1 024的灰度图像“5.1.09”、“5.2.09”与“5.3.01”进行加密仿真，仿真实验在MATLAB R2018b软件中进行实现，仿真环境为Intel Core i7-7700 @ 3.60 GHz CPU、8 GB内存和Windows 10操作系统。椭圆曲线参数 $\{p, a, b, G(G_x, G_y)\}$ 与双方私钥 s_a 和 s_b 设定如下：

$$
\begin{aligned}
p &= \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF} \\
&\quad\ \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFC2F} \\
a &= \text{00000000 00000000 00000000 00000000} \\
&\quad\ \text{00000000 00000000 00000000 00000000} \\
b &= \text{00000000 00000000 00000000 00000000} \\
&\quad\ \text{00000000 00000000 00000000 00000007} \\
G_x &= \text{79BE667E F9DCBBAC 55A06295 CE870B07} \\
&\quad\ \text{029BFCDB 2DCE28D9 59F2815B 16F81798} \\
G_y &= \text{483ADA77 26A3C465 5DA4FBFC 0E1108A8} \\
&\quad\ \text{FD17B448 A6855419 9C47D08F FB10D4B8} \\
s_a &= \text{DE2EA148 FF2FF7C2 6ECFA0DE ACB6A2B0} \\
&\quad\ \text{401DB5F0 76CC277A BC4AA217 F593C48B} \\
s_b &= \text{EF8224D4 D3E53497 5D98E4CC 69108CE2} \\
&\quad\ \text{97052C48 294ABB71 3E2D8F17 1F0CDD16}
\end{aligned}
$$

加密效果如图4所示，可以观察到3幅图像均被加密为杂乱无章的密码图像，又由于算法的每一步都是完全可逆的，可以从相应的密文图像中完全解密恢复原始图像。



(a) 明文图像　(b) 密文图像　(c) 解密图像

图4　加密效果图

Fig. 4　Encryption effect diagram ((a) plaintext images; (b) ciphertext images; (c) decrypt images)

实验仿真的算法运行时间如表4所示，算法的实际运行效率受计算机硬件、仿真环境与编程代码等因素影响。

为了评估该算法的总体性能，下面分别从密钥空间、抗统计攻击和抗差分攻击等方面进行分析。

3.1 密钥空间

一般情况下，一个好的加密算法的密钥空间应该大于 2^{100}，才能抵御穷举攻击（杨宇光和裴帅康，2022）。本算法的密钥为通信双方的长度为256 bit的私钥，攻击者只有破解出通信两端之一的完整私钥才可以从信道中获取到有效信息，故算法密钥空间为 2^{256}，显然本文算法的密钥空间足够大，完全能够抵抗穷举攻击。此外，加密算法应该对其密钥极其敏感。否则，具有微小差异的不正确密钥也可能正确解密原始图像的信息，这可能使实际密钥空间小于理论密钥空间。

比特变化率数（number of bit change rate, NBCR）可用于测试算法的密钥敏感性（Castro等，2005）。对于两个尺寸一样的图像的像素以光栅扫描顺序二进制编码 $\boldsymbol{X}_1$ 和 $\boldsymbol{X}_2$，NBCR定义为

表 4　算法运行时间

Table 4　Algorithm running time

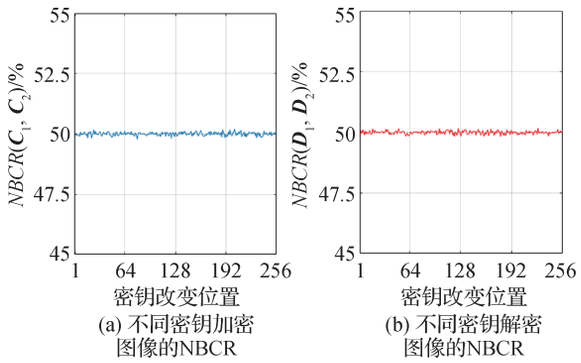
图像(尺寸/像素)	加密时间/s	解密时间/s
5.1.09(256×256)	0.251 8	0.330 5
5.2.09(512×512)	1.019 2	0.986 5
5.3.01(1 024×1 024)	4.275 7	4.179 5

$$NBCR(\boldsymbol{X}_1,\boldsymbol{X}_2)=\frac{Ham(\boldsymbol{X}_1,\boldsymbol{X}_2)}{Len} \tag{19}$$

式中，$Ham(\boldsymbol{X}_1,\boldsymbol{X}_2)$表示$\boldsymbol{X}_1$和$\boldsymbol{X}_2$的汉明距离，$Len$表示图像的位长度，当NBCR接近50%时可以认为图像$\boldsymbol{X}_1$和$\boldsymbol{X}_2$完全不一样。

加密算法的密钥敏感性测试步骤如下：

先设定一个原始密钥K_1，改变其256位数据中的一位得到差异密钥K_2，在加密端分别使用K_1和K_2对测试图像“5.1.09”进行加密，得到两幅密文图像$\boldsymbol{C}_1$和$\boldsymbol{C}_2$，计算$\boldsymbol{C}_1$和$\boldsymbol{C}_2$的NBCR；在解密端分别使用K_1和K_2对同一密文图像$\boldsymbol{C}_1$进行解密得到两幅解密图像$\boldsymbol{D}_1$和$\boldsymbol{D}_2$，计算$\boldsymbol{D}_1$和$\boldsymbol{D}_2$的NBCR。依次单一改变密钥256位数据进行测试，得到密钥敏感性分析结果，如图5所示，当密钥的任何一位发生变化时，得到的两个密文图像和解密图像是完全不同的，这意味着本算法对密钥极其敏感。



(a) 不同密钥加密图像的NBCR　(b) 不同密钥解密图像的NBCR

图5　密钥敏感性分析

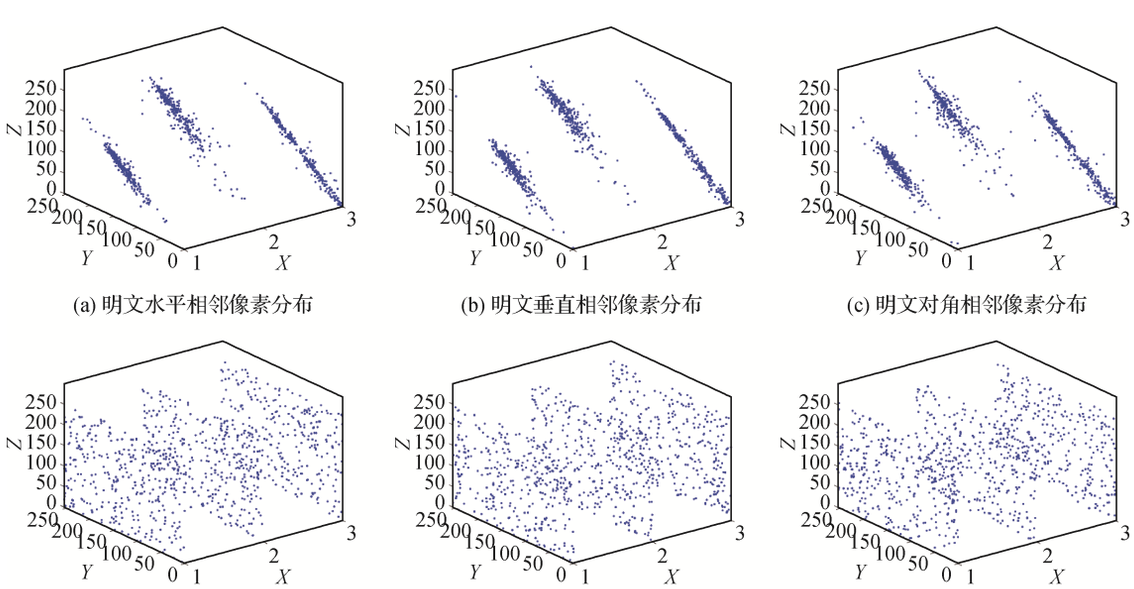
Fig. 5　Key sensitivity analysis

((a) NBCR of images encrypted with different keys; (b) NBCR of images decrypted with different keys)

3.2　抗统计攻击分析

3.2.1　相关性分析

相邻像素相关性描述图像中相邻像素之间的相关性程度，对于有视觉感知意义的图像，相邻像素之间的相关性通常非常高，因为它们的值彼此接近，而通过图像加密算法处理获得的加密图像应当呈现弱相关性。如图6所示，随X轴分别表示3幅测试图像的明密文，在Y–Z平面绘制相应方向上的相邻像素值的分布情况。可以看到，明文图像在各个方向上的相邻像素分布均集中在对角线附近，表现出强相关性。而密文图像在各个方向上的相邻像素都均匀



(a) 明文水平相邻像素分布　(b) 明文垂直相邻像素分布　(c) 明文对角相邻像素分布

(d) 密文水平相邻像素分布　(e) 密文垂直相邻像素分布　(f) 密文对角相邻像素分布

图6　相邻像素值分布情况

Fig. 6　Distribution of adjacent pixel values ((a) horizontal adjacent pixel distribution of plaintext; (b) vertical adjacent pixel distribution of plaintext; (c) diagonal adjacent pixel distribution of plaintext; (d) horizontal adjacent pixel distribution of ciphertext; (e) vertical adjacent pixel distribution of ciphertext; (f) diagonal adjacent pixel distribution of ciphertext)

分布在整个区间,表现出弱相关性。

通常,还通过计算不同方向上的相关系数来评价图像相邻像素相关性,具体为

$$r_{xy}=\frac{E((x-E(x))(y-E(y)))}{\sqrt{D(x)}\sqrt{D(y)}}$$
$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{20}$$
$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2$$

式中,x_i与y_i表示水平、垂直与对角方向上的相邻像素采样点的像素值,$E(x)$表示样本的期望值,$D(x)$表示样本的方差,N为样本总数。

表5列出了3幅测试图像加密前后的相关性系数,可以看到,密文图像各个方向上的相关系数均接近于零,与明文图像相比显著降低,说明加密算法很好地破坏了相邻像素的相关性。

表5　相邻像素相关性分析

Table 5　Correlation analysis of adjacent pixels

图像(尺寸/像素)		水平方向	垂直方向	对角方向
5.1.09(256×256)	明文	0.937 1	0.899 7	0.906 9
	密文	−0.009 8	0.006 7	0.002 3
5.2.09(512×512)	明文	0.870 3	0.903 9	0.802 0
	密文	−0.001 6	0.003 7	−0.002 5
5.3.01(1 024×1 024)	明文	0.981 4	0.977 0	0.966 4
	密文	−0.001 1	−0.008 7	0.003 7

3.2.2　直方图分析

直方图表示的是图像所有可能像素值的频率分布。对于正常图像,某些像素值的频率分布会较高,而另一些像素值的频率会较低,因此,直方图是不规则的,反映图像的某些特征。而加密图像的直方图应该是平坦均匀的,攻击者无法从中获取任何有效信息。图7给出了3幅测试图像的直方图分析结果。可以看出,密文图像的直方图是均匀分布的,与明文图像截然不同,可以抵抗直方图攻击。

3.2.3　信息熵

信息熵是检验图像随机性的重要指标,若图像的信息熵接近理想值8,则表示图像具有优异的随机性,能抵抗统计攻击,图像信息熵的计算式为

$$H(s)=-\sum_{i=0}^{255}P(s_i)\log_2 P(s_i) \tag{21}$$

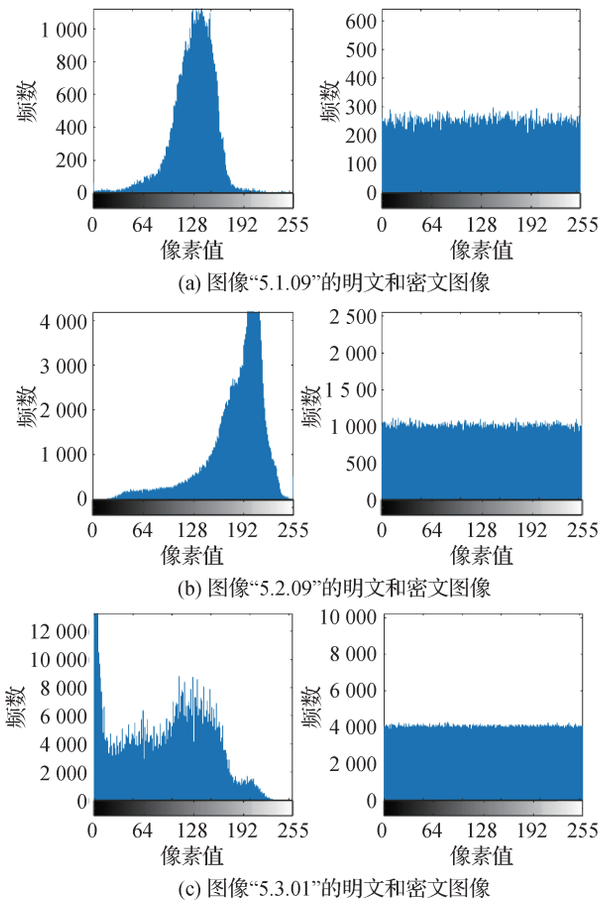


图7　直方图分析

Fig. 7　Histogram analysis

((a) plaintext and ciphertext of image 5. 1. 09; (b) plaintext and ciphertext of image 5. 2. 09; (c) plaintext and ciphertext of image 5. 3. 01)

式中,s_i表示0～255的像素值,$P(s_i)$表示像素值s_i在图像中出现的概率。表6列出了3幅测试图像加密前后对应的信息熵的值。可以看出,所有明文图像的信息熵都相对较小,而密文图像信息熵非常接近理想值。

表6　信息熵分析

Table 6　Information entropy analysis

图像(尺寸/像素)	明文信息熵	密文信息熵
5.1.09(256×256)	6.709 3	7.997 5
5.2.09(512×512)	6.994 0	7.999 3
5.3.01(1 024×1 024)	7.523 7	7.999 8

3.3　抗差分攻击分析

差分攻击是一种常用且有效的攻击方式,通过研究明文图像中的差异对密文的影响,建立明文与

密文之间的关系。像素变化率(number of pixels change rate,NPCR)和统一平均变化强度(unified average changing intensity,UACI)是测试加密算法是否能够抵抗差分攻击的两个重要指标。假设$\boldsymbol{C}_1$和$\boldsymbol{C}_2$是由两个只有一个位差的明文图像使用同一密钥加密得到的密文,它们的NPCR和UACI值的计算式为

$$NPCR(\boldsymbol{C}_1,\boldsymbol{C}_2)=\frac{\sum_{i=1}^{N}D(i)}{N}\times 100\%$$
$$D(i)=\begin{cases}1 & C_1(i)=C_2(i)\\ 0 & C_1(i)\neq C_2(i)\end{cases} \tag{22}$$

而

$$UACI=\frac{\sum_{i=1}^{N}\left|C_1(i)-C_2(i)\right|}{255\times N}\times 100\% \tag{23}$$

式中,N表示图像的像素数,$\boldsymbol{C}(i)$表示图像第i个像素的像素值,$D(i)$表示两幅图像的第i个像素是否一样。根据定义可知NPCR与UACI分别统计了明文的微小差异所导致的密文的像素变化概率以及变化程度,反映了加密算法对明文的敏感性。根据Hua等人(2019)给出的显著性水平为0.05时的不同大小图像的NPCR与UACI的置信区间,表7与表8列出的3幅测试图像的NPCR与UACI测试结果均在置信区间内,意味着本文算法能够有效的抵抗差分攻击。

表7　NPCR测试结果

Table 7　NPCR test results

图像(尺寸/像素)	NPCR/%	置信区间/%
5.1.09(256×256)	99.612 4	[99.569 3,100]
5.2.09(512×512)	99.615 5	[99.589 3,100]
5.3.01(1 024×1 024)	99.621	[99.599 4,100]

表8　UACI测试结果

Table 8　UACI test results

图像(尺寸/像素)	UACI/%	置信区间/%
5.1.09(256×256)	33.452 8	[33.282 4,33.644 7]
5.2.09(512×512)	33.473 9	[33.373 0,33.554 1]
5.3.01(1 024×1 024)	33.458 3	[33.418 3,33.508 8]

3.4　NIST随机性测试

NIST SP800-22是测量数据序列随机性的既定标准。使用本文算法对USC-SIPI“Miscellaneous”与“Aerials”图像数据集进行加密,然后将多个密文图像用做二进制序列输入进行随机性测试。实验中,NIST测试了100个1 000 000位的二级制序列。如果任何测试的值P-value小于0.000 1,则认为序列随机性不够好(Wang等,2015)。表9列出了测试结果。本文算法通过了所有的子测试,这表明本文算法加密得到的密文图像具有高度的随机性。

表9　NIST随机性测试

Table 9　NIST randomness test

随机性测试	P-value	结果
Frequency (Monobit) Test	0.719 747	Pass
Frequency Tesr within a Block	0.122 325	Pass
Cumulative Sums (Cusum) Test*	0.606 177	Pass
Runs Test	0.935 716	Pass
Long Runs of Ones in a Block Test	0.867 692	Pass
Binary Matrix Rank Test	0.289 667	Pass
Discrete Fourier Transform (Spectral) Test	0.419 021	Pass
Non-overlapping Templates Matching Test*	0.517 279 4	Pass
Overlapping Templates Matching Test	0.202 268	Pass
Maurers Universal Statisitcal Test	0.202 268	Pass
Approximate Entropy Test(m=10)	0.991 468	Pass
Random Excursions Test*	0.538 184	Pass
Random Excursions Variant Test*	0.455 294 667	Pass
Serial Test* (m=10)	0.352 261 5	Pass
Linear Complexity Test	0.911 413	Pass

注:*表示该测试中至少有两个统计值,P-value由平均统计值表征。pass表示通过测试,m表示该子测试的取数长度。

3.5　对比与分析

使用本文算法对图像Lena进行加密与性能测试,并与其他加密算法进行对比,其他算法的测试结果直接从相应的论文中引用,对比结果如表10所示,其中。可以观察到,各算法相邻像素相关性分析的性能差异较小,而在信息熵与抗差分攻击分析方面,本文算法性能更优异,表明本文算法具有更好的安全性。

本文算法采用非对称的密钥生成与分发方式,暴露的公钥基于椭圆曲线离散对数的难解问题使攻击者无法逆向推导私钥,同时足够大的私钥空间可以抵抗穷举攻击,解决了冗余密钥的管理与分发问题的同时密钥安全性足以得到保障。对图像的

表10　与其他算法性能对比结果

Table 10　Results comparison with other algorithms

算法	相邻像素相关性			信息熵	NPCR/%	UACI/%
	水平	垂直	对角			
本文	−0.005 9	−0.005 6	**−0.000 4**	**7.997 5**	99.617 0	33.472 6
Wang等人(2019)	−0.003 1	0.008 4	−0.000 7	7.997 1	99.601 6	33.473 5
Xu等人(2019)	−0.001 5	0.004 1	0.006 9	7.993 5	99.609 8	33.469 7
Ge和Ye(2019)	0.002 0	−0.002 9	−0.008 3	7.997 2	99.610 0	**33.490 0**
陶珊等人(2020)	0.001 8	0.001 0	0.001 4	/	99.609 3	33.463 4
Kaur等人(2020)	**−0.000 6**	−0.005 7	0.000 9	7.993 8	99.600 6	34.637 9
He等人(2021)	0.001 3	**0.000 2**	0.003 3	7.997 2	99.610 0	33.460 0
Roy等人(2021)	−0.001 7	−0.000 9	−0.001 9	/	96.594 0	32.886 0
邓文博等人(2022)	0.003 4	−0.009 0	−0.009 2	7.996 6	99.606 6	33.442 5
刘海峰等人(2022)	0.004 8	0.003 3	0.001 6	7.997 3	**99.650 0**	33.490 0

注：加粗字体表示各列最优结果，“/”表示文献未记录图像Lena的此项测试结果。

DNA自适应编码加密过程通过DNA编解码内嵌动态扩散—自适应置换结构将扩散与置换环节互相紧密联系，使得攻击者无法通过分割攻击逐一破解，同时动态扩散过程与自适应置换过程都与中间密文相关，当采用不同的明文进行加密时，中间密文也会随之变化，杜绝了选择明文攻击的可能性。

4　结　论

针对当前大多数一次一密模式的混沌图像加密算法存在的密钥冗余的问题，本文提出了椭圆曲线与自适应DNA编码的混沌图像加密算法。算法由密钥共识算法与自适应DNA编码加密两个部分组成，前者让使用者无需传输私钥便可达成密钥共识，后者将具有中间密文状态反馈的动态扩散—自适应置换结构嵌入DNA编码的扩散过程中，使置换与扩散过程相互紧密联系以抵抗分割攻击和选择明文攻击，同时，加密过程的密文状态可以在解密端自适应同步，避免了密钥冗余的问题。对测试图像的实验仿真与安全性分析的结果表明，本文算法在对各种尺寸的图像的加密中都表现出优异的性能，对主流的几种攻击方式都有较高的抵御能力，并且通过与近年的其他算法的对比体现了本文的优越性。由于密钥共识算法是基于椭圆曲线上的离散对数难解问题而设计，具有高复杂度，低加密效率的特点，产生共识密钥序列的计算速度需要进一步优化，这将成为下一步研究的核心问题。

参考文献(References)

Castro J C H, Sierra J M, Seznec A, Izquierdo A and Ribagorda A. 2005. The strict avalanche criterion randomness test. Mathematics and Computers in Simulation, 68(1): 1-7 [DOI: 10.1016/j.matcom.2004.09.001]

Chai X L, Bi J Q, Gan Z H, Liu X X, Zhang Y S and Chen Y R. 2020. Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. Signal Processing, 176: #107684 [DOI: 10.1016/j.sigpro.2020.107684]

Deng W B, Liu S, Liu F C and Huang R N. 2022. An image encryption algorithm based on compressed sensing and DNA coding. Computer Engineering and Science, 44(9): 1574-1582 (邓文博, 刘帅, 刘福才, 黄茹楠. 2022. 基于压缩感知和DNA编码的图像加密算法. 计算机工程与科学, 44(9): 1574-1582) [DOI: 10.3969/j.issn.1007-130X.2022.09.007]

Fridrich J. 1998. Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos, 8(6): 1259-1284 [DOI: 10.1142/S021812749800098X]

Ge M and Ye R S. 2019. A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties. Egyptian Informatics Journal, 20(1): 45-54 [DOI: 10.1016/j.eij.2018.10.001]

Ghadirli H M, Nodehi A and Enayatifar R. 2019. An overview of encryption algorithms in color images. Signal Processing, 164: 163-185 [DOI: 10.1016/j.sigpro.2019.06.010]

He P C, Sun K H and Zhu C X. 2021. A novel image encryption algorithm based on the delayed maps and permutation-confusion-diffusion architecture. Security and Communication Networks, 2021: #6679288 [DOI: 10.1155/2021/6679288]

Hua Z Y, Zhou Y C and Huang H J. 2019. Cosine-transform-based cha-

otic system for image encryption. Information Sciences, 480: 403-419 [DOI: 10.1016/j.ins.2018.12.048]

Kaur G, Agarwal R and Patidar V. 2020. Chaos based multiple order optical transform for 2D image encryption. Engineering Science and Technology, an International Journal, 23(5): 998-1014 [DOI: 10.1016/j.jestch.2020.02.007]

Khan J S and Ahmad J. 2019. Chaos based efficient selective image encryption. Multidimensional Systems and Signal Processing, 30(2): 943-961 [DOI: 10.1007/s11045-018-0589-x]

Koblitz N, Menezes A and Vanstone S. 2000. The state of elliptic curve cryptography. Designs, Codes and Cryptography, 19 (2/3): 173-193 [DOI: 10.1023/A:1008354106356]

Li L, Abd El-Latif A A and Niu X M. 2012. Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images. Signal Processing, 92(4): 1069-1078 [DOI: 10.1016/j.sigpro.2011.10.020]

Liang H T, Zhang G D, Hou W J, Huang P Y, Liu B and Li S L. 2021. A novel asymmetric hyperchaotic image encryption scheme based on elliptic curve cryptography. Applied Sciences, 11(12): #5691 [DOI: 10.3390/app11125691]

Liang X K, Tao L M and Hu B. 2019. Image hybrid encryption based on a generalized chaotic mapping and matrix nonlinear transformation. Journal of Image and Graphics, 24(3): 325-333 (梁锡坤, 陶利民, 胡斌. 2019. 一类广义混沌映射和矩阵非线性变换的图像混合加密. 中国图象图形学报, 24(3): 325-33) [DOI: 10.11834/jig.180349]

Lin R G and Li S. 2021. An image encryption scheme based on Lorenz hyperchaotic system and RSA algorithm. Security and Communication Networks, 2021: #5586959 [DOI: 10.1155/2021/5586959]

Liu H F, Zhou X F, Liang X L and Wang L H. 2022. Image encryption algorithm based on multiple chaotic systems. Journal of Shaanxi University of Science and Technology, 40(1): 188-195 (刘海峰, 周雪飞, 梁星亮, 汪丽华. 2022. 基于多混沌系统的图像加密算法. 陕西科技大学学报, 40(1): 188-195) [DOI: 10.3969/j.issn.1000-5811.2022.01.028]

Luo H B, Ge B, Wang J and Wu B. 2018. Dynamic self-feedback chaotic system image encryption based on neural network scrambling image. Journal of Image and Graphics, 23(3): 346-361 (罗海波, 葛斌, 王杰, 吴波. 2018. 整合神经网络置乱图像的动态自反馈混沌系统图像加密. 中国图象图形学报, 23(3): 346-361) [DOI: 10.11834/jig.170464]

Roy M, Chakraborty S, Mali K, Roy D and Chatterjee S. 2021. A robust image encryption framework based on DNA computing and chaotic environment. Microsystem Technologies, 27 (10): 3617-3627 [DOI: 10.1007/s00542-020-05120-0]

Sasikaladevi N, Geetha K, Sriharshini K and Aruna M D. 2020. H^3-hybrid multilayered hyper chaotic hyper elliptic curve based image encryption system. Optics and Laser Technology, 127: #106173 [DOI: 10.1016/j.optlastec.2020.106173]

Tao S, Tang C and Lei Z K. 2020. Image encryption based on vector decomposition and chaotic random phase mask. Laser and Optoelectronics Progress, 57(4): #041002 (陶珊, 唐晨, 雷振坤. 2020. 基于矢量分解和混沌随机相位掩模的图像加密. 激光与光电子学进展, 57(4): #041002 [DOI: 10.3788/LOP57.041002]

Wang Q X, Yu S M, Guyeux C, Bahi J and Fang X L. 2015. Study on a new chaotic bitwise dynamical system and its FPGA implementation. Chinese Physics B, 24(6): #060503 [DOI: 10.1088/1674-1056/24/6/060503]

Wang X Y, Zhang J J, Zhang F C and Cao G H. 2019. New chaotical image encryption algorithm based on Fisher-Yatess scrambling and DNA coding. Chinese Physics B, 28(4): #040504 [DOI: 10.1088/1674-1056/28/4/040504]

Xu Q Y, Sun K H, Cao C and Zhu C X. 2019. A fast image encryption algorithm based on compressive sensing and hyperchaotic map. Optics and Lasers in Engineering, 121: 203-214 [DOI: 10.1016/j.optlaseng.2019.04.011]

Yang Y, Wang L D, Duan S K and Luo L. 2021. Dynamical analysis and image encryption application of a novel memristive hyperchaotic system. Optics and Laser Technology, 133: #106553 [DOI: 10.1016/j.optlastec.2020.106553]

Yang Y G and Pei S K. 2022. Image encryption algorithm based on double chaotic system and DNA encoding. Journal of Anhui University (Natural Science Edition), 46(5): 37-49 (杨宇光, 裴帅康. 2022. 基于双混沌系统和DNA编码的图像加密算法. 安徽大学学报(自然科学版), 46(5): 37-49) [DOI: 10.3969/j.issn.1000-2162.2022.05.006]

Ye G D, Liu M and Wu M F. 2022. Double image encryption algorithm based on compressive sensing and elliptic curve. Alexandria Engineering Journal, 61(9): 6785-6795 [DOI: 10.1016/j.aej.2021.12.023]

Yu S M, Lü J H and Li C Q. 2016. Some progresses of chaotic cipher and its applications in multimedia secure communications. Journal of Electronics and Information Technology, 38(3): 735-752 (禹思敏, 吕金虎, 李澄清. 2016. 混沌密码及其在多媒体保密通信中应用的进展. 电子与信息学报, 38(3): 735-752) [DOI: 10.11999/JEIT151356]

Zhou H, Xie H W, Zhang H and Zhang H T. 2021. Parallel remote sensing image encryption algorithm based on chaotic map and DNA encoding. Journal of Image and Graphics, 26(5): 1081-1094 (周辉, 谢红薇, 张昊, 张慧婷. 2021. 混沌系统和DNA编码的并行遥感图像加密算法. 中国图象图形学报, 26(5): 1081-1094) [DOI: 10.11834/jig.200344]

作者简介

肖定汉，男，硕士研究生，主要研究方向为密码学和图像处理。E-mail: xiao_dinghan@163.com

王倩雪，通信作者，女，副教授，硕士生导师，主要研究方向为数字域混沌系统和混沌密码学。

E-mail: wangqianxue@gdut.edu.cn

禹思敏，男，教授，博士生导师，主要研究方向为混沌理论与应用、混沌密码分析与设计。E-mail: siminyu@163.com