文章编号:1671-4598(2020)12-0191-06 DOI:10.16526/j.cnki.11—4762/tp.2020.12.040 中图分类号:TP277 文献标识码:A

基于混合混沌系统和 ECG 信号的图像加密算法

周闰昌，黄一平，张柯翔，孙健华
(广西师范大学 电子工程学院，广西 桂林 541004)

摘要：为提高明文图像和密钥在加密算法的敏感性和不可预测性，设计了一种基于混合混沌系统和 ECG 信号相结合的图像加密算法；ECG 信号因人而异且难以模仿和复制；首先利用 wolf 算法计算出随机性强的 ECG 信号特征值，以及生成明文图像的 SHA—256 哈希值，用于计算混合混沌系统和 ZigZag 变换的初始条件；其次利用改善的 ZigZag 变换对明文图像进行动态置乱，并进行 DNA 动态编码；最后对置乱的图像按照一定的方法完成扩散过程；通过理论分析和实验结果表明，该加密算法对明文图像和 ECG 信号高度敏感，具有密钥空间大的优点，能够有效地抵抗已知明文、选择明文攻击、抗穷举攻击和差分攻击。

关键词：混沌系统；SHA—256 函数；ECG 信号；ZigZag 变换；DNA 编码

Image Encryption Algorithm Based on Mixed Chaotic System and ECG Signal

Zhou Runchang, Huang Yiping, Zhang Kexiang, Sun Jianhua
(College of Electronic Engineering, Guangxi Normal University, Guilin 541004, China)

Abstract: In order to improve the sensitivity and unpredictability of plaint image and key in encryption algorithm. In the paper, an image encryption algorithm based on mixed chaotic system and electrocardiogram (ECG) signal is proposed. ECG signal vary from person to person, making it difficult to be imitated and duplicated. Firstly, characteristic value of the ECG signal with strong randomness was calculated by Wolf algorithm, and secure hash algorithm—256 (SHA—256) hash function of the plain image is combined to comput the initial conditions for mixed chaotic system and ZigZag transformation. Then, the improved ZigZag transformation was used to image dynamic scrambling pixel position of the plain image, and dynamic deoxyribonucleic acid (DNA) standard rule coding was selected. Finally, getting the scrambling according to certain method or process which is encrypted exclusive image. The experimental and security analysis indicate that the encryption algorithm is highly sensitive to plain image and ECG signal, and has the advantages of large key space and can effectively risist known—plaintext and chosen—plaintext attacks、statistical attack and differential attack.

Keywords: chaotic system; SHA—256 system; ECG signal; ZigZag transformation; DNA coding

0 引言

数字图像具有直观、生动的特点，是多媒体信息的重要形式之一，随着物联网和多媒体技术的发展，数字图像在互联网上广泛传播。因此，对各种通信网络中安全图像和传输的研究越来越受人们的关注[1]。研究人员研发了不同类型的技术，如数据隐藏[2]、数字水印[3]和图像加密[4-6]，而最有效、最直接的方法就是图像加密，将可视化的图像转化为无法识别的噪声类图像。因为图像相邻元素具备高度相关性，传统的加密方案如数据加密标准（DES，data encryption standard）和高级加密标准（AES，advanced Encryption Standard）不适合多媒体加密[4]。混沌系统具有伪随机性、不可预测性、遍历性和对初始值和参数高度敏感性等基本特点[5-6]，利用混沌特点进行图像加密是在密码学和计算机研究的热点。在生成密钥方面，混沌系统分为低维和高维，且两者具有不同的优缺点。高维混沌系统具有较好的随机性，数据分布更均匀，参数空间更大，但计算复杂度高。低维混沌系统具有明显的计算开销优势，但它也降低了混沌性能。

人的心脏是极其复杂的生物系统，而心电图是检测心率的常用方法，心电信号（ECG，electrocardiogram）在医学领域运用较多，特别是诊断病情和预防疾病[7]，受到很多研究者的欢迎。由于 ECG 信号很难被复制和模拟，故近年来，也有研究者将 ECG 信号用于数据加密和传输[8]，文献［9］设计了一种基于自阻塞和 ECG 信号相结合的图像加密算法，ECG 信号使用 wolf 算法生成混沌映射的初始条件，该算法被文献［10］中使用已知明文攻击所破译。

研究者近年来有使用 ZigZag 标准变换对图像进行像素的置换[11-13]，文献［14］提出了选择明文攻击方法对文献［12］进行了破译。有研究者对标准的 ZigZag 变换方式进行改进，文献［15］提出从矩阵的主对角线元素进行扫描，进而遍历整个矩阵；文献［16］提出从选择矩阵的任意位置作为起始元素，以 Z 型方向遍历整个矩阵，因只是简单变换在文献［17］被选择密文攻击。以上方法都存在周期短、部分矩阵元素位置始终不变、变换规则易被破解的缺点。

收稿日期:2020-05-08； **修回日期**:2020-05-26。
基金项目:广西师范大学重大科技成果转化培育项目(2019PY005);2019 年广西第四批创新驱动发展专项资金项目(桂科 AA19254001)。
作者简介:周闰昌(1995-),男,湖北随州人,硕士,主要从事图像加密方向的研究。

根据以上分析，提出了基于 ECG 信号和混合混沌系统相结合的数字图像加密方案。使用安全散列算法－256（secure hash algorithm－256，SHA－256）函数以及随机性强的 ECG 信号，加大了密钥空间。该方案采用置乱和扩散技术，通过用 3D 逻辑映射产生的随机序列值，进行动态脱氧核糖核酸（DNA，deoxyribonucleic acid）编码、改进的 ZigZag 变换进行图像置乱以及运算，对图像进行实时动态加密。本文方案经过安全性能测试和分析，实验结果表明，本文算法具有良好的加密性能，并提高了抗常见的攻击能力。

1 基本理论

1.1 混沌系统

3D 逻辑映射的混沌性能要比 1D 或者 2D 逻辑映射有着更好的混沌性能特性，且控制参数多。采用 3D 逻辑映射系统，定义如公式（1）所示：

$$\begin{cases} x_{i+1} = \alpha x_i(1-x_i) + \beta y_i^2 x_i + \gamma z_i^3 \\ y_{i+1} = \alpha y_i(1-y_i) + \beta z_i^2 y_i + \gamma x_i^3 \\ z_{i+1} = \alpha z_i(1-z_i) + \beta x_i^2 z_i + \gamma y_i^3 \end{cases} \tag{1}$$

当设置参数 $3.53<\alpha<3.81$，$0<\beta<0.022$，$0<\gamma<0.015$。x_i，y_i，$z_i\in$（0，1），3D 逻辑映射可产生复杂的混沌行为。而分段线性混沌映射（PWLCM），定义如式（2）所示：

$$x_{i+1} = F_p(x_i)\begin{cases} \dfrac{x_i}{p}, 0 \leqslant x_i < p \\ \dfrac{x_i - p}{0.5 - p}, p \leqslant x_i < 0.5 \\ F_p(1-x_i), 0.5 \leqslant x_i < 1 \end{cases} \tag{2}$$

其中：$x_i\in$［0，1）和控制参数 $p_i\in$（0，0.5）。PWLCM 系统具有良好的遍历性、混淆性以及均匀的不变性分布，可以为加密系统生成随机序列。

1.2 心电信号

人体内最特殊的信号就是 ECG 信号，同一个人在两个不同的时刻与不同人在同一时刻，ECG 信号都有很大的差异，如图 1 所示。ECG 信号采用 wolf 算法提取特征值，记为$\in$［－1，1］[18]。

1.3 DNA 编码

DNA 全称为脱氧核苷酸，是由核苷酸组成的，不同的 DNA 可组成不同的核苷酸。核苷酸包括腺嘌呤（adenine，A）、鸟嘌呤（guanine，G）、胞嘧啶（cytosine，C）和胸腺嘧啶（thymine，T）。参照 Watson－Crick 碱基配对规则[19]，A 总是与 T 配对，C 和 G 也是如此。则 A 和 T、G 与 C 形成碱基互补。二进制中 0 和 1 是互补的，因此 00 和 11 互补以及 01 和 10 互补，而满足沃森－克里克互补规则的只有 8 种。如表 1 所示。图像的像素范围为 0～255，将像素值的十进制转化为二进制，得到 8 位有效像素值，可以表示为一个长度为 4 的 DNA 序列。假设像素值为 198，则二进制为 $(11000110)_2$，根据表中的规则 3，其编码为 ATGC。

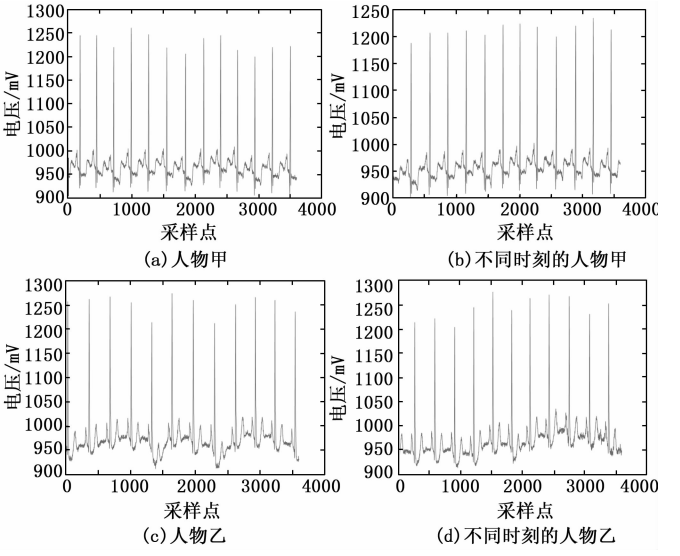

图 1 心电信号

表 1 DNA 编码规则

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

在 DNA 计算中，DNA 的加、减和异或都是根据二进制编码来的，如表 2～表 4 所示。

表 2 采用 DNA 编码规则 1 的加法运算

＋＋	A＝00	T＝11	C＝10	G＝01
A＝00	A	T	C	G
T＝11	T	C	G	A
C＝10	C	G	A	T
G＝01	G	A	T	C

表 3 采用 DNA 编码规则 1 的减法运算

－－	A＝00	T＝11	C＝10	G＝01
A＝00	A	G	C	T
T＝11	T	A	G	C
C＝10	C	G	A	T
G＝01	G	C	T	A

1.4 改进的 ZigZag 变换系统

ZigZag 变换是一种像素置乱的方法，可以通过选择矩阵任意位置作为起始元素，然后以 Z 形路径遍历矩阵来实现像素的置乱[16]。假设选取矩阵的（3，2）位置数，经过 Z 型遍历整个矩阵，得到新的矩阵，如图 2 所示。ZigZag 变

表 4　采用 DNA 编码规则 1 的异或运算

XOR	A=00	T=11	C=10	G=01
A=00	A	T	C	G
T=11	T	A	G	C
C=10	C	G	A	T
G=01	G	C	T	A

换系统是将经过 Z 型变换生成的一维矩阵 $\boldsymbol{L}$ 分成 4 个等长的矩阵，矩阵内部排序分为顺序和逆序，共有 16 种方式，排序如表 5 所示。而矩阵间的排序为 4 个等长矩阵的排序组合，再转换为二维矩阵。

表 5　4 个等长矩阵的排序

	L_1	L_2	L_3	L_4
1	正	正	正	正
2	正	正	正	逆
3	正	正	逆	正
4	正	正	逆	逆
5	正	逆	正	正
6	正	逆	正	逆
7	正	逆	逆	正
8	正	逆	逆	逆
9	逆	正	正	正
10	逆	正	正	逆
11	逆	正	逆	正
12	逆	正	逆	逆
13	逆	逆	正	正
14	逆	逆	正	逆
15	逆	逆	逆	正
16	逆	逆	逆	逆

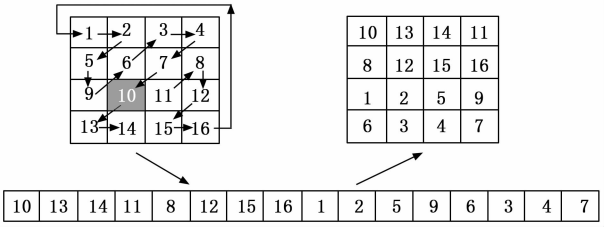

图 2　ZigZag 变换

为了提高加密算法对明文图像和 ECG 信号的依赖性，利用 SHA－256 函数和由 3D 混沌映射的一个混沌序列 $\{X_i\}$ 来计算 ZigZag 置乱的起始位置、矩阵内部排序以及矩阵间排序，改进的 ZigZag 变换如图 3 所示。不同明文图像和 ECG 信号可得到不同的初始位置，置乱效果也不一样，具有很高的置乱率，可提高抵抗选择明文攻击和已知明文攻击的能力。

2　加密算法

图像加密算法流程如图 4 所示。

图像加密算法具体过程如下。

1）假设明文图像为 I，其大小为 $M*N$，为加强算法

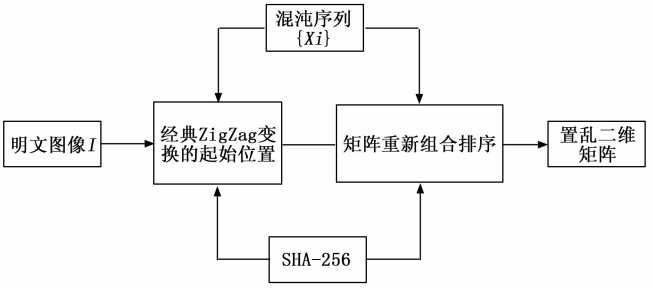

图 3　ZigZag 变换系统

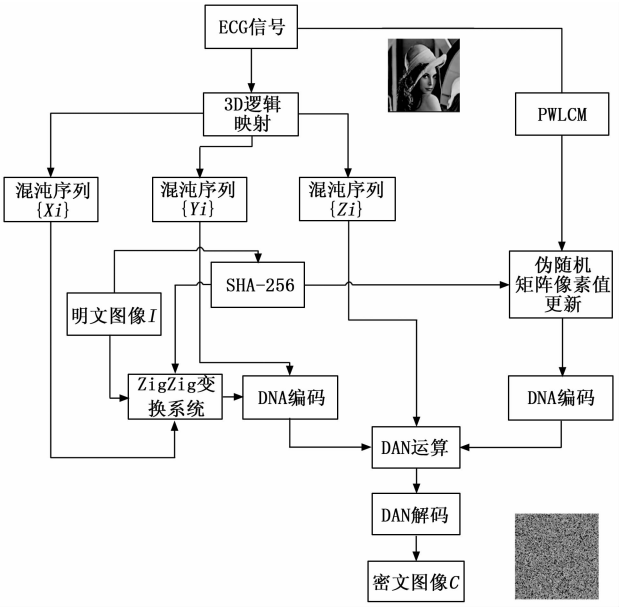

图 4　加密算法流程图

对明文图像的敏感性以及扩大密钥空间。利用 SHA－256 哈希函数生成图像 I 的 256 位哈希值 K。并转换为 32 个十进制数，记为 K_i。

$$K_i=\{K_0,K_1,\cdots,K_{31}\} \tag{3}$$

2）3D 逻辑混沌映射的初始条件的生成，为了增加初始值的复杂性，ECG 信号使用 wolf 算法提取特征值 λ，在公式（4）和（5）生成 3D 逻辑映射的初始参数 α，β，γ 和初始值 x_0，y_0，z_0。

$$\begin{cases}\alpha=3.65+\dfrac{\lambda}{100}\\ \beta=\left|\dfrac{\lambda}{100}\right|\times 2+0.001\\ \gamma=\dfrac{\lambda+2}{10}\end{cases} \tag{4}$$

$$\begin{cases}x_0=\dfrac{\lambda+2}{10}\\ y_0=\dfrac{\lambda+4}{10}\\ z_0=\dfrac{\lambda+6}{10}\end{cases} \tag{5}$$

为了加强初始值跟明文图像的敏感性，利用公式（6）对初始值再进行一次更新，得到新的初始值 x'、y' 和 z'。

$$\begin{cases} x' = x_0 + \dfrac{\sum_0^7 K_i}{10\times 10^4} - floor\left(\dfrac{\sum_8^{15} K_i}{10\times 10^4}\right) \\ y' = y_0 + \dfrac{\sum_8^{15} K_i}{10\times 10^4} - floor\left(\dfrac{\sum_{16}^{23} K_i}{10\times 10^4}\right) \\ z' = z_0 + \dfrac{\sum_{16}^{23} K_i}{10\times 10^4} - floor\left(\dfrac{\sum_{24}^{31} K_i}{10\times 10^4}\right) \end{cases} \tag{6}$$

式中，$|x|$ 表示 x 的绝对值，$floor(x)$ 表示不大于 x 的整数。

3）分段线性混沌映射系统（PWLCM，The piecewise linear chaotic mapsystem）。由式（7）和（8）生成混沌系统的初始参数 p 和初始值 x''_0。

$$p = \frac{\lambda+1}{5} + 0.01 \tag{7}$$

$$x''_0 = \left| \frac{\sum_0^{15} K_i}{16\times 10^4} - floor\left(\frac{\sum_{16}^{31} K_i}{16\times 10^4}\right) \right| \tag{8}$$

4）分段线性混沌映射系统用初始值迭代 $1\ 000+MN$ 次（其中 1 000 为随机数），为了去掉暂态性，将前 1 000 次去掉，得到一维混沌序列 R_i。并根据公式（9）进行量化处理，运算得到 0～255 范围的整数，得到二维矩阵 $\boldsymbol{H}$。

$$R_i = floor(L_i \times 10^{14}) \bmod 256 \tag{9}$$

式中，$A \bmod B$ 表示 A 除以 B 的余数。

5）根据以下式子对矩阵 $\boldsymbol{H}$ 进行更新像素值，依次选择前 $N/2$、后 $N/2$ 列以及前 $M/2$、后 $M/2$ 行与明文图像的哈希值 Ki 进行计算。

采用第一个 DNA 编码规则，将其转换为 $M*4N$ 大小的矩阵 $\boldsymbol{P}$。

$$\begin{cases} \boldsymbol{H}(i,j) = \left(\boldsymbol{H}\left(i,1:\dfrac{N}{2}\right) + floor\left(\sum_0^7 K_i\right)\right) \bmod 256 \\ \boldsymbol{H}(i,j) = \left(\boldsymbol{H}\left(i,\dfrac{N}{2}+1:N\right) + floor\left(\sum_8^{15} K_i\right)\right) \bmod 256 \\ \boldsymbol{H}(i,j) = \left(\boldsymbol{H}\left(1:\dfrac{M}{2},j\right) + floor\left(\sum_{16}^{23} K_i\right)\right) \bmod 256 \\ \boldsymbol{H}(i,j) = \left(\boldsymbol{H}\left(\dfrac{M}{2}+1:M,j\right) + floor\left(\sum_{24}^{31} K_i\right)\right) \bmod 256 \end{cases}$$

6）将 3D 逻辑映射的初始条件进行代入，对混沌系统进行迭代 $1\ 000+MN$ 次，同样为防止发生暂态效应，去掉前 1 000 次，得到 3 个混沌序列 $\{X_i\}$、$\{Y_i\}$ 和 $\{Z_i\}$。

7）假设 ZigZag 变换的起始元素位置为明文图像 I 的 (m, n) 元素（其中 $1\leqslant m\leqslant M, 1\leqslant n\leqslant N$）。明文图像的哈希值和混沌序列 $\{X_i\}$ 动态选择起始位置初始值，如式（10）～（11）所示。经过 ZigZag 变换再按着从左到右，从上到下转化为一维矩阵为 $\boldsymbol{L}(i)$，$i=1, 2, 3, \cdots, mn$；其中 mn 为 $M*N$ 的结果值。

$$m = floor(X_i \times 10^4) + \sum_0^7 K_i) \bmod M + 1 \tag{10}$$

$$n = floor(X_i \times 10^4) + \sum_8^{15} K_i) \bmod N + 1 \tag{11}$$

8）对一维矩阵 $\boldsymbol{L}$ 进行平均分组，令：

$$\begin{cases} \boldsymbol{L}_1 = \boldsymbol{L}(i), i = 1, 2, \cdots, \dfrac{mn}{4} \\ \boldsymbol{L}_2 = \boldsymbol{L}(i), i = \dfrac{mn}{4}+1, \dfrac{mn}{4}+2, \cdots, \dfrac{mn}{2} \\ \boldsymbol{L}_3 = \boldsymbol{L}(i), i = \dfrac{mn}{2}+1, \dfrac{mn}{2}+2, \cdots, \dfrac{3\times mn}{4} \\ \boldsymbol{L}_4 = \boldsymbol{L}(i), i = \dfrac{3\times mn}{4}+1, \dfrac{3\times mn}{4}+2, \cdots, mn \end{cases}$$

得到 4 个等长的一维矩阵 $\boldsymbol{L}_i$（$i=1$，2，3，4）。

9）对 4 个一维矩阵 $\boldsymbol{L}_i$（$i=1$，2，3，4）进行单独的矩阵内部排序，正为保持原有的顺序不变，而逆为对一维矩阵进行逆序排序。根据混沌序列 $\{X_i\}$ 和哈希值，动态选择矩阵内部的排序规则，如公式（12）所示。假设值为 7，根据表所示，L_1 和 L_4 保持原有的顺序，而 L_2 和 L_3 则为逆序。

$$v1 = floor(X_i \times 10^4 + \sum_{16}^{23} K_i) \bmod 16 + 1 \tag{12}$$

10）对 4 个一维矩阵 $\boldsymbol{L}_i$（$i=1$，2，3，4）进行重新排序成一个新的一维矩阵 $\boldsymbol{L}'=[L_1, L_2, L_3, L_4]$，排序规则共有 $C_4^1C_3^1C_2^1C_1^1=24$ 种，可根据式（13）的结果值进行矩阵间动态排序。

$$v2 = floor(X_i \times 10^4 + \sum_{16}^{31} K_i) \bmod 24 + 1 \tag{13}$$

变换后的一维矩阵转化为从左到右、从上到下的大小为 $M*N$ 的二维矩阵 $\boldsymbol{Q}1$。

11）将置换矩阵 $\boldsymbol{Q}1$ 转换成 0～255 范围的整数，根据 DNA 编码共有 8 种不同的标准规则，混沌序列 $\{Y_i\}$ 通过公式（14）计算的结果值来确定置乱图像 $\boldsymbol{Q}1$ 的动态 DNA 编码方式，并生成大小为 $M*4N$ 的矩阵 $\boldsymbol{Q}2$。

$$y(i) = floor(Y_i \times 10^4) \bmod 8 + 1 \tag{14}$$

12）经过 DNA 编码的矩阵 $\boldsymbol{Q}2$ 与矩阵 $\boldsymbol{P}$ 进行动态 DNA 运算得到矩阵 $\boldsymbol{Q}3$。而运算方式有三种，由混沌序列 $\{Zi\}$ 通过式（21）计算的结果来确定选择运算方式，式（14）如下所示：

$$z(i) = floor(Z_i \times 10^4) \bmod 3 + 1 \tag{15}$$

其中：$z(i)$ 为 1 时，DNA 运算为加法，当为 2 时，DNA 运算为减法，当为 3 时，DNA 运算为异或。

13）DNA 解码对应有 8 种编码规则，由式（16）～（21）的结果值共同决定解码规则进行动态解码，如式（16）所示，并获得密文图像 C。

$$w = (m+n+v1+v2+y(i)+z(i)) \bmod 8 + 1 \tag{16}$$

解密过程是加密过程的逆运算操作。

3 实验仿真和安全分析

实验硬件环境为 1.7 GHz 的 Intel 处理器，内存为 4.0 G，仿真软件为 Matlab R2016a，运行在 64 位的 Windows 10 操作系统。不同一个人以及不同时刻的 ECG 信号如图 1 所示。通过 wolf 算法提取 ECG 信号的特征值和 SHA－256 产生的哈希值来控制混合混沌系统的初始条件。以 256×256 的 Lena 和 Cameraman 明文图像和 512×512 的 Peppers 明文图像的标准灰度图像作为明文图像进行实验分

析。图 5 分别为明文图像、对应的密文图像以及解密之后的图像。

3.1　密钥空间分析

密钥空间是用于加密的密钥的数量，一个较大的密钥空间超过 2^{100} 可以抵抗穷举攻击[20]。本文算法使用了 Physionet 在线数据库[21]的 1 000 个样本的 ECG 信号和 SHA－256 哈希函数生成 256 位哈希值来生成混合混沌系统的初始条件和 ZigZag 变换的初始位置。如果心电信号中存在一个样本移位或明文图像改变一个像素，则无法解密出正确的明文图像。也可选用文献［8］提出的心电采集装置进行实时测试。因此该算法的密钥空间足够大，可抵抗穷举攻击。

图 5　加密解密效果

3.2　直方图分析

图 6 显示出了图像像素强度值的分布。优异的加密算法使密文图像的直方图是近似均匀分布的。如图 6（a）～（c）为明文图像的直方图，而图 6（d）～（f）为对应的加密图像直方图，加密图像在［0，255］区间内呈现均匀的分布，相对于不同类型的明文图像，该加密系统对图像加密具有良好的分散功能，可抵抗统计攻击。

3.3　相邻像素点的相关性分析

明文图像的相邻元素点的相关性比较高（接近于 1），然而一个优秀的算法，可以使相邻像素点的相关性变得更小（接近于 0），可以抵御任何蛮力攻击。分别从明文图像和密文图像中随机选取 1 000 对像素点，根据公式（17）～（20）来计算两相邻像素点的水平、垂直和对角线上方向的相关性，并与近年的图像加密算法文献进行对比，结果如表 6 所示。由表 6 看出，密文图像相邻像素的相关系数要接近于 0，对比其他文献，本加密算法具备更好的抗攻击能力。

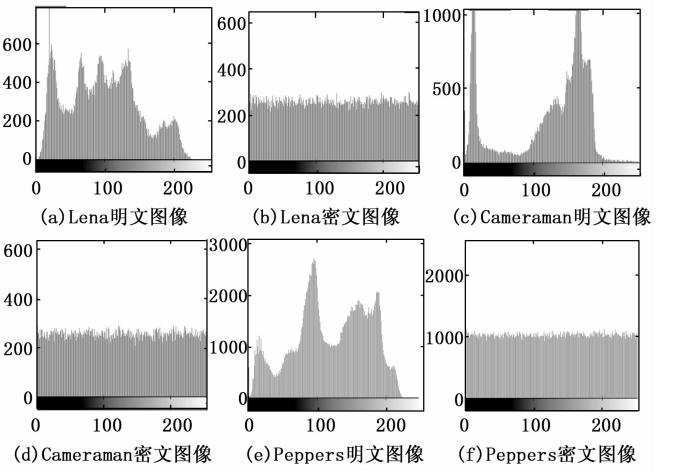

图 6　明文和密文的直方图

表 6　相邻像素点比较

图像	方向	Lena	Cameraman	Peppers
原图像	水平	0.955 6	0.930 4	0.977 1
	垂直	0.962 1	0.956 5	0.981 6
	对角线	0.931 6	0.898 6	0.966 5
本文加密	水平	0.955 6	0.930 4	0.977 1
	垂直	0.962 1	0.956 5	0.981 6
	对角线	0.931 6	0.898 6	0.966 5
本文加密	水平	0.004 9	0.001 5	−0.006 1
	垂直	0.003 2	−0.003 8	−0.001 5
	对角线	0.002 4	0.005 4	0.003 5
文献[20]	水平	0.005 6	0.002 4	0.000 6
	垂直	0.003 7	0.001 3	0.003 8
	对角线	0.003 2	0.009 8	0.001 0
文献[22]	水平	0.002 3	0.019 8	0.005 3
	垂直	0.001 9	0.013 2	0.013 8
	对角线	0.001 0	0.000 3	0.001 9

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{17}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{18}$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{19}$$

$$r_{xy}=\frac{|\operatorname{cov}(x,y)|}{\sqrt{D(x)}\times\sqrt{D(y)}} \tag{20}$$

式中，$E(x)$ 和 $D(x)$ 分别是变量 x 的期望和方差，x 和 y 为明文和密文中同一位置两个像素的灰度值，$cov(x, y)$ 为像素 x 和 y 处的协方差，r_{xy} 为相关系数。

3.4　信息熵

信息熵是反映出图像灰度值的分配和随机性，像素值分布越均匀，图像的信息熵就越大。信息熵的公式为：

$$H(x)=\sum_{i=1}^{n}P(x_i)\log\frac{1}{P(x_i)} \tag{21}$$

式（21）中，$P(x_i)$ 是像素值为 x_i 出现的概率，n 是图像像素的个数。密文图像信息熵的理想值为 8。本文提出算法

得到密文图像的信息熵如表 7 所示，并与同近年的图像加密方案文献进行对比。结果表明，本加密算法的信息熵数值接近理想值 8，能够有效抵抗信息熵的攻击。

表 7 信息熵比较

图像	输入图像	加密图像				
		本文算法	文献[18]	文献[20]	文献[23]	文献[24]
Lena	7.553 4	7.997 6	7.997 4	7.997 6	7.997 5	7.997 1
Camer－aman	7.104 8	7.997 9	7.997 8	7.997 5	7.997 8	7.997 1
Peppers	7.592 5	7.999 3	7.999 3	7.999 3	7.999 4	7.997 3

3.5 抗差分攻击能力

攻击者经常使用加密算法对变换前后的明文图像进行加密，通过对两幅密文图像的比较，找出明文图像与密文图像之间的联系。这种类型的攻击称为差异攻击[25]。通常用像素变化率（*NPCR*）和归一化平均变化强度（*UACI*）这两个指标来衡量抗差分攻击的能力，其表达式如下：

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \tag{28}$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |D1(i,j) - D2(i,j)|}{255 \times M \times N} \times 100\% \tag{29}$$

$$D(i,j) = \begin{cases} 1, C1(i,j) = C2(i,j) \\ 0, C1(i,j) \neq C2(i,j) \end{cases} \tag{30}$$

$C1$（i，j）和 $C2$（i，j）为两幅密文图像在（i，j）坐标的灰度值，且对应的两幅大小为 $M * N$ 的明文图像只有一个像素值的不同。

为了测试明文图像的敏感性，从明文图像中随机选取一个像素值，并在同一位置的像素值进行更改，得到修改的明文图像。使用同一密钥对明文图像和修改的明文图像进行加密处理，生成 2 个密文图像。测试中采用 3 张不同的明文图像，比较不同方案的 *NPCR* 和 *UACI* 数据，如表 8 和表 9 所示。从表中可以看出，本文算法的 *NPCR* 和 *UACI* 测试数据接近理论理想值（*NPCR*≈99.609 4%，*UACI*≈33.463 5%），优于其他方案，因此具有较强的抗差分攻击能力。

表 8 *NPCR*(%)的比较

图像	加密图像				
	本文算法	文献[18]	文献[20]	文献[23]	文献[24]
Lena	99.622	99.628	99.620	99.519	99.640
Camer－aman	99.615	99.584	99.610	99.004	99.610
Peppers	99.607	99.593	99.620	99.302	99.690

表 9 *UACI*(%)的比较

图像	加密图像				
	本文算法	文献[18]	文献[20]	文献[23]	文献[24]
Lena	33.546	33.396	33.417	33.585	33.630
Camer－aman	33.537	33.480	33.532	33.103	33.580
Peppers	33.462	33.424	33.537	33.003	33.280

4 结束语

基于混合混沌系统和 ECG 信号，提出了一种新的图像加密算法。首先利用 3D 逻辑混沌系统产生的混沌序列对明文图像进行像素随机置乱和动态 DNA 编码，像素随机置乱是基于改进的 ZigZag 变换，具有很高的置乱率；PWLCM 混沌映射生成的伪随机矩阵与置乱图像进行动态 DNA 运算达到像素的散乱，可得到密文图像。混合混沌系统的初始值和初始参数不仅跟明文图像的哈希值有关，还跟 ECG 信号的特征值有关，两者都具有很强的随机性；且对 ZigZag 变换的起始位置以及序列的置乱起了决定性作用，不仅大大增强了密钥的敏感性，也提升了密钥空间，加强了算法的可靠性。与其他方案的数据进行对比分析，该方案具有良好的加密性能，提高了抵抗选择明文攻击、已知明文攻击、穷举攻击和差分攻击的能力。

参考文献：

[1] Zhang X Q，Wang X S. Multiple－image encryption algorithm based on DNA encoding and chaotic system [J]. Multimedia Tools and Applications，2019，78 (6)：7841－7869.

[2] Lin Y T，Wang C M，Chen W S，et al. A novel data hiding algorithm for high dynamic range images [J]. IEEE Trans. Multimed，2016，19 (1)：196－211.

[3] Hukum S. Watermarking image encryption using deterministic phase mask and singular value decomposition in fractional Mellin transform domain [J]. IET Image Processing，2018，12 (11)：1994－2001.

[4] Zarebnia M，Pakmanesh H，Parvaz R. A fast multiple－image encryption algorithm based on hybrid chaotic systems for gray scale images [J]. Optic，2019，179：761－773.

[5] 闫 兵，柏 森，刘博文，等. 基于交叉混沌映射的小波域图像加密算法 [J]. 计算机应用研究，2018，35 (6)：1797－1799，1811.

[6] 朱淑芹，王文宏. 对一维复合混沌图像加密算法的安全分析和改进 [J]. 计算机应用研究，2019，36 (8)：2432－2435.

[7] 刘 垒，楼光海，黄 微. 结合双树复小波变换和滑动平均滤波的心电信号去噪方法 [J]. 电子测量技术，2018，41 (19)：112－117.

[8] Chen C K，Lin C L，Chiang C T，et al. Personalized information encryption using ECG signals with chaotic functions [J]. Information Sciences，2012，193：125－140.

[9] Ye G D，Huang X L. An image encryption algorithm based on auto－blocking and ECG signal [J]. IEEE MultiMedia，2015，23：64－71.

[10] Li C Q，Lin D D，Lyu J H，et al. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography [J]. IEEE Multimedia，2018，25 (4)：46－56.

[11] Li Y Z，Li X D，Xin J，et al. An image Encryption algorithm based on Zigzag transformation and 3－dimension chaotic logistic map [J]. Application and Techniques in Information Security，2015，119：3－13.

（下转第 201 页）