一种超混沌图像加密算法的安全性分析及其改进*

王 静[1)†] 蒋国平[1)2)]

1)(南京邮电大学控制与智能技术研究中心, 南京 210003)

2)(南京邮电大学自动化学院, 南京 210003)

(2010 年 8 月 13 日收到;2010 年 9 月 30 日收到修改稿)

根据 Kerckhoff 准则, 从选择明文攻击和选择密文攻击出发, 对一种超混沌图像加密算法进行分析,结果表明该算法密钥流与明文无关,并且一个明文字节只能影响一个密文字节,导致利用选择明文攻击和选择密文攻击能够以很小的计算代价破译密文. 基于此,本文提出一种改进的超混沌图像加密算法,并进行了统计分析、差分分析、相关性分析及密钥敏感性测试. 理论分析及仿真结果表明,改进算法不仅可以抵御选择明文攻击和选择密文攻击,而且具有较好的统计特性及差分特性等密码学特性.

关键词: 超混沌, 选择明文攻击, 选择密文攻击, Matlab 分析

PACS: 05.45.Gg

1. 引 言

近年来,混沌研究是非线性科学领域的热点问题之一[1—7]. 混沌系统以其类噪声及对初值高度敏感的特点,越来越多地被应用到保密通信系统的设计中,并先后提出了许多基于混沌系统的加密算法. Baptista[8] 提出一种典型的混沌加密方案,并一度成为研究热点,一些新的加密算法也在此基础上被提出来[9,10]. 但是,该类算法存在以下两方面明显不足:首先,密文的长度至少是明文的两倍,这对于大量的数据加密非常不利;其次,密文分布不均匀,不能够抵御统计方法攻击. 针对这一类 Baptista 密码系统存在的问题,文献[11—13]提出了基于混沌映射的加密系统,然而该系统每次新的加密过程为相同的密钥流序列,而获得密钥流就等同于获得了密钥,因此不能够抵御选择明文攻击和选择密文攻击. 最近,文献[14,15]利用混沌的伪随机特性,提出改进的基于混沌映射的图像加密算法,该类算法虽然具有形式简单、产生混沌序列时间短等优点,但是密钥空间太小,并且对于低维混沌加密方案已有很多攻击方法可以将其破解[16].

较之低维混沌系统,高维混沌系统具有更复杂的动力学行为以及更好的随机性,一般低维的破译方法,如相空间重构、回归映像和非线性预测等很难破译超混沌加密的信息,因此,具有 2 个或 2 个以上正性 Lyapunov 指数的超混沌应用研究越来越受到人们的关注[17—20]. Yao 等[21] 提出一种超混沌图像加密算法,该算法利用超混沌产生二进制序列对图像进行预处理,主要包括魔方扰乱及像素移位两部分,然后再进一步改变图像像素值. 然而,当密钥初始值不变时,加密过程使用相同的密钥流序列. Gao 等[22] 提出一种基于超混沌的图像加密算法(HIE 算法),该算法的核心思想是利用 Logistic 混沌映射对像素矩阵进行置乱,然后再通过超混沌产生的密钥流对灰度值进行加密. HIE 算法实现简单,对于实时性要求高的加密系统,该算法是一个很好的选择. 然而,本文通过对 HIE 算法的深入分析后发现:首先,使用低维混沌系统对像素置乱,达不到高维混沌的随机性和保密性;其次,与 Yao 等提出的超混沌图像加密算法存在同样的问题,并且一个明文字节只能影响一个密文字节,导致通过选择明文攻击和选择密文攻击能够很容易地破译密文.

针对上述超混沌加密系统所存在的问题,本文提出一种改进的超混沌图像加密算法. 其核心思想描述如下:首先,利用超混沌系统对图像像素进行

* 国家自然科学基金(批准号:60874091)、江苏省高等学校自然科学基础研究计划(批准号:08KJD510022)、江苏省"六大人才高峰"资助计划(批准号:SJ209006)和南京邮电大学引进人才计划(批准号:NY209021)资助的课题.

† E-mail:jingwang@njupt.edu.cn

置乱,抵御一般低维混沌的破译方法;其次,通过密文反馈方式控制算法中的密钥流,使得加密所需参数通过密文反馈与明文相关,将一个明文字节的影响扩散到更多的密文字节中. 理论分析及实验仿真表明,改进的算法不仅可以有效地避免选择明文攻击和选择密文攻击,而且具有较好的统计及差分特性.

2. HIE 算法概述

HIE 算法主要包括像素置乱及图像扩散和混乱两个部分[22],下面具体介绍 HIE 算法的加密过程.

2.1. 像素置乱

设 $\boldsymbol{P}_{M\times N}$表示大小为 $M\times N$ 的图像,像素值矩阵记为 $\boldsymbol{P}$. 在 HIE 算法中,首先利用 Logistic 映射产生混沌序列如下:

$$x_{n+1} = \mu x_n(1 - x_n),\ x \in [0,1]. \tag{1}$$

混沌动力系统研究指出,当 $3.5699456\cdots < \mu \leqslant 4$ 时,Logistic 映射于混沌状态,计算

$$r = \mathrm{mod}(x_0 \times 10^{14}, M). \tag{2}$$

迭代 Logistic 映射直到产生 M 个完全不同的 r 值,记为$\{r_i, i = 0,1,\cdots,M-1\}$. 根据 r_i 对矩阵 $\boldsymbol{P}$ 进行行变换,行变换后的矩阵记为 $\boldsymbol{P}^{\mathrm{r}}$. 同理,计算 $c = \mathrm{mod}(x_0 \times 10^{14}, N)$,其中 $c \in [0, N-1]$. 迭代 Logistic 映射直到产生 N 个完全不同的 c 值,记为$\{c_j, j = 0,1,\cdots,N-1\}$. 根据 c_j 对矩阵 $\boldsymbol{P}^{\mathrm{r}}$ 进行列变换,经过行列变换后的矩阵记为 $\boldsymbol{P}^{\mathrm{rc}}$.

2.2. 图像扩散和混乱

超混沌系统如下[22]:

$$\begin{aligned}
\dot{x}_1 &= a(x_2 - x_1),\\
\dot{x}_2 &= -x_1x_3 + dx_1 + cx_2 - x_4,\\
\dot{x}_3 &= x_1x_2 - bx_3,\\
\dot{x}_4 &= x_1 + k.
\end{aligned} \tag{3}$$

其中 $a = 36, b = 3, c = 28, d = -16, -0.7 \leqslant k \leqslant 0.7$. 计算

$$\begin{aligned}
x_i = \mathrm{mod}(&(\mathrm{abs}(x_i) - \mathrm{floor}(\mathrm{abs}(x_i)))\\
&\times 10^{14}, 256)\quad i = 1,2,3,4,
\end{aligned} \tag{4}$$

其中 abs(·)表示取绝对值,floor(·)表示向上取整. 计算 $\bar{x}_1 = \mathrm{mod}(x_1, 4)$,根据 $\bar{x}_1$ 从表 1 中选取相应组合对 $\boldsymbol{P}^{\mathrm{rc}}$进行加密,即

$$\begin{aligned}
C_{3\times(i-1)+1} &= P_{3\times(i-1)+1} \oplus B_{x_1},\\
C_{3\times(i-1)+2} &= P_{3\times(i-1)+2} \oplus B_{x_2},\\
C_{3\times(i-1)+3} &= P_{3\times(i-1)+3} \oplus B_{x_3},
\end{aligned} \tag{5}$$

其中 $i = 1,2,\cdots$表示第 i 次超混沌迭代;⊕表示异或;$P_i, i = 1,2,\cdots,M\times N$ 表示置乱后图像的像素值;B_{x_1}, B_{x_2}和 B_{x_3}表示根据 $\bar{x}_1$ 选择的表 1 中的对应组合;$C_i, i = 1,2,\cdots,M\times N$ 表示密文像素值. 解密过程与加密过程相似.

表 1 超混沌序列的不同组合

$\bar{x}_1$	对应组合
0	(x_1, x_2, x_3)
1	(x_1, x_2, x_4)
2	(x_1, x_3, x_4)
3	(x_2, x_3, x_4)

3. HIE 算法破译

根据 Kerckhoff 提出的现代密码学原理,加密系统的安全性不依赖于加密方法本身,而是依赖于所使用的密钥. 这说明除了密钥之外,密码分析者在知道加密算法的前提下,当加密算法能够抵御所有的攻击时才认为该算法是安全的. 对加密算法的攻击分为 4 个级别,按照从难到易的顺序依次排列为:密文攻击、已知明文攻击、选择明文攻击和选择密文攻击[23]. 下面将利用选择明文攻击和选择密文攻击对 HIE 算法进行破译.

3.1. 选择明文攻击

假定已知 3 组大小为 $M\times N$ 的明文矩阵 $\boldsymbol{P}_0, \boldsymbol{P}_1$ 和 $\boldsymbol{P}_2$ 分别为

$$\boldsymbol{P}_0 = \begin{pmatrix} 0 & 0 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \cdots & 0 \end{pmatrix}, \tag{6a}$$

$$\boldsymbol{P}_1 = \begin{pmatrix} p_1 & p_2 & \cdots & p_N\\ \cdots & \cdots & \cdots & \cdots\\ p_1 & p_2 & \cdots & p_N \end{pmatrix}, \tag{6b}$$

$$\boldsymbol{P}_2 = \begin{pmatrix} p_1 & p_1 & \cdots & p_1\\ \cdots & \cdots & \cdots & \cdots\\ p_M & p_M & \cdots & p_M \end{pmatrix}. \tag{6c}$$

根据 HIE 加密算法,得到明文矩阵 $\boldsymbol{P}_0, \boldsymbol{P}_1$ 和 $\boldsymbol{P}_2$ 对应的密文矩阵 $\boldsymbol{C}_0, \boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 如下:

$$\boldsymbol{C}_0 = \boldsymbol{P}_0^{\mathrm{rc}} \oplus \boldsymbol{B}_x, \tag{7a}$$

$$\boldsymbol{C}_1 = \boldsymbol{P}_1^{\mathrm{rc}} \oplus \boldsymbol{B}_x, \tag{7b}$$

$$\boldsymbol{C}_2 = \boldsymbol{P}_2^{\mathrm{rc}} \oplus \boldsymbol{B}_x, \tag{7c}$$

其中 $\boldsymbol{P}_0^{\mathrm{rc}}$ 为明文矩阵 $\boldsymbol{P}_0$ 经过行列置换后的矩阵. 若破解密文矩阵 $\boldsymbol{C}'$并获得其对应的明文矩阵 $\boldsymbol{P}'$,则可以通过三个步骤实现.

步骤 1 根据(6a)式可知 $\boldsymbol{P}_0 = \boldsymbol{P}_0^{\mathrm{rc}}$,那么由(7a)式可得

$$\boldsymbol{B}_x = \boldsymbol{C}_0 \oplus \boldsymbol{P}_0^{\mathrm{rc}} = \boldsymbol{C}_0. \tag{8}$$

明文矩阵 $\boldsymbol{P}'$经过行列置换后对应的矩阵为

$$\boldsymbol{P}'^{\mathrm{rc}} = \boldsymbol{C}' \oplus \boldsymbol{B}_x. \tag{9}$$

步骤 2 根据(6b)式,矩阵 $\boldsymbol{P}_1$ 与其行置换矩阵 $\boldsymbol{P}_1^{\mathrm{r}}$ 的关系是 $\boldsymbol{P}_1^{\mathrm{r}} = \boldsymbol{P}_1$,且(7b)式可以表示为

$$\boldsymbol{P}_1^{\mathrm{rc}} = \boldsymbol{C}_1 \oplus \boldsymbol{B}_x. \tag{10}$$

因此,(10)式表示为 $\boldsymbol{P}_1^{\mathrm{rc}} = \boldsymbol{P}_1^{\mathrm{c}} = \boldsymbol{C}_1 \oplus \boldsymbol{B}_x$,从而计算得到 c 值. 根据(9)式,对行列置换矩阵 $\boldsymbol{P}'^{\mathrm{rc}}$ 进行列反变换得到行置换矩阵 $\boldsymbol{P}'^{\mathrm{r}}$.

步骤 3 根据(6c)式和(7c)式可知

$$\boldsymbol{P}_2^{\mathrm{rc}} = \boldsymbol{C}_2 \oplus \boldsymbol{B}_x. \tag{11}$$

(11)式又可以表示为 $\boldsymbol{P}_2^{\mathrm{r}} = \boldsymbol{C}_2 \oplus \boldsymbol{B}_x$,从而计算出 r 值. 然后,对 $\boldsymbol{P}'^{\mathrm{r}}$ 进行行反变换能够得到明文矩阵 $\boldsymbol{P}'$. 因此,HIE 算法抵御不了选择明文攻击.

为表明上述分析的合理性,下面通过仿真实验进行验证,假设已知三组明密文对. 明文分别为

$$\boldsymbol{P}_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\boldsymbol{P}_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\boldsymbol{P}_2 = \begin{pmatrix} 1 & 1 & 1 \\ 3 & 3 & 3 \\ 5 & 5 & 5 \end{pmatrix}.$$

密文分别为

$$\boldsymbol{C}_0 = \begin{pmatrix} 167 & 0 & 86 \\ 111 & 197 & 174 \\ 190 & 87 & 145 \end{pmatrix},$$

$$\boldsymbol{C}_1 = \begin{pmatrix} 161 & 4 & 84 \\ 105 & 193 & 172 \\ 184 & 83 & 147 \end{pmatrix},$$

$$\boldsymbol{C}_2 = \begin{pmatrix} 162 & 5 & 83 \\ 108 & 198 & 173 \\ 191 & 86 & 144 \end{pmatrix}.$$

现在要破译密文 $\boldsymbol{C}' = \begin{pmatrix} 159 & 98 & 21 \\ 103 & 23 & 243 \\ 191 & 1 & 52 \end{pmatrix}$,得到对应的明文 $\boldsymbol{P}'$. 根据步骤 1 得到

$$\boldsymbol{P}_0 = \boldsymbol{P}_0^{\mathrm{rc}} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

那么,根据(8)式得到

$$\boldsymbol{B}_x = \boldsymbol{C}_0 \oplus \boldsymbol{P}_0^{\mathrm{rc}} = \boldsymbol{C}_0 = \begin{pmatrix} 167 & 0 & 86 \\ 111 & 197 & 174 \\ 190 & 87 & 145 \end{pmatrix}.$$

HIE 算法的密钥不变,每次新的加密过程为相同的密钥流序列,因此,

$$\boldsymbol{P}'^{\mathrm{rc}} = \boldsymbol{C}' \oplus \boldsymbol{B}_x$$

$$= \begin{pmatrix} 159 & 98 & 21 \\ 103 & 23 & 243 \\ 191 & 1 & 52 \end{pmatrix} \oplus \begin{pmatrix} 167 & 0 & 86 \\ 111 & 197 & 174 \\ 190 & 87 & 145 \end{pmatrix}$$

$$= \begin{pmatrix} 56 & 98 & 67 \\ 8 & 210 & 93 \\ 1 & 86 & 165 \end{pmatrix}.$$

由于 $\boldsymbol{P}_1$ 为行相同矩阵,那么根据步骤 2 计算出

$$\boldsymbol{P}_1 = \boldsymbol{P}_1^{\mathrm{r}} = \begin{pmatrix} 2 & 4 & 6 \\ 2 & 4 & 6 \\ 2 & 4 & 6 \end{pmatrix}.$$

同理得到

$$\boldsymbol{P}_1^{\mathrm{c}} = \boldsymbol{P}_1^{\mathrm{rc}} = \boldsymbol{C}_1 \oplus \boldsymbol{B}_x$$

$$= \begin{pmatrix} 161 & 4 & 84 \\ 105 & 193 & 172 \\ 184 & 83 & 147 \end{pmatrix} \oplus \begin{pmatrix} 167 & 0 & 86 \\ 111 & 197 & 174 \\ 190 & 87 & 145 \end{pmatrix}$$

$$= \begin{pmatrix} 6 & 4 & 2 \\ 6 & 4 & 2 \\ 6 & 4 & 2 \end{pmatrix}.$$

从而计算出 $c = \{3; 2; 1\}$. 根据(9)式,对行列置换矩阵 $\boldsymbol{P}'^{\mathrm{rc}}$ 进行列反变换得到

$$\boldsymbol{P}'^{\mathrm{r}} = \begin{pmatrix} 67 & 98 & 56 \\ 93 & 210 & 8 \\ 165 & 86 & 1 \end{pmatrix}.$$

根据步骤 3 计算得到

$$\boldsymbol{P}_2^{\mathrm{r}} = \boldsymbol{P}_2^{\mathrm{rc}} = \boldsymbol{C}_2 \oplus \boldsymbol{B}_x$$

$$= \begin{pmatrix} 162 & 5 & 83 \\ 108 & 198 & 173 \\ 191 & 86 & 144 \end{pmatrix} \oplus \begin{pmatrix} 167 & 0 & 86 \\ 111 & 197 & 174 \\ 190 & 87 & 145 \end{pmatrix}$$

$$= \begin{pmatrix} 5 & 5 & 5 \\ 3 & 3 & 3 \\ 1 & 1 & 1 \end{pmatrix}.$$

由此计算出 $r = \{3; 2; 1\}$. 然后,对 $\boldsymbol{P}'^{\mathrm{r}}$ 进行行反变换得到明文矩阵为

$$\boldsymbol{P}' = \begin{pmatrix} 165 & 86 & 1 \\ 93 & 210 & 8 \\ 67 & 98 & 56 \end{pmatrix}.$$

可见, HIE 算法抵御不了选择明文攻击.

3.2. 选择密文攻击

假定已知三组密文矩阵 $\boldsymbol{C}_0$, $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 分别为

$$\boldsymbol{C}_0 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \tag{12a}$$

$$\boldsymbol{C}_1 = \begin{pmatrix} c_1 & c_2 & \cdots & c_N \\ \cdots & \cdots & \cdots & \cdots \\ c_1 & c_2 & \cdots & c_N \end{pmatrix}, \tag{12b}$$

$$\boldsymbol{C}_2 = \begin{pmatrix} c_1 & c_1 & \cdots & c_1 \\ \cdots & \cdots & \cdots & \cdots \\ c_M & c_M & \cdots & c_M \end{pmatrix}. \tag{12c}$$

根据 HIE 解密算法,得到 $\boldsymbol{C}_0$, $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 对应的行列置换矩阵 $\boldsymbol{P}_0^{\mathrm{rc}}$, $\boldsymbol{P}_1^{\mathrm{rc}}$ 和 $\boldsymbol{P}_2^{\mathrm{rc}}$ 如下:

$$\boldsymbol{P}_0^{\mathrm{rc}} = \boldsymbol{C}_0 \oplus \boldsymbol{B}_x, \tag{13a}$$

$$\boldsymbol{P}_1^{\mathrm{rc}} = \boldsymbol{C}_1 \oplus \boldsymbol{B}_x, \tag{13b}$$

$$\boldsymbol{P}_2^{\mathrm{rc}} = \boldsymbol{C}_2 \oplus \boldsymbol{B}_x. \tag{13c}$$

破解密文矩阵 $\boldsymbol{C}'$,并获得对应明文矩阵 $\boldsymbol{P}'$,可以通过三个步骤.

步骤 1 由于 $\boldsymbol{C}_0$ 为全零阵,根据(13a)式计算得到

$$\boldsymbol{B}_x = \boldsymbol{C}_0 \oplus \boldsymbol{P}_0^{\mathrm{rc}} = \boldsymbol{P}_0^{\mathrm{rc}}, \tag{14}$$

因此,根据 HIE 解密算法,得到明文矩阵 $\boldsymbol{P}'$的行列置换矩阵如下:

$$\boldsymbol{P}'^{\mathrm{rc}} = \boldsymbol{C}' \oplus \boldsymbol{B}_x. \tag{15}$$

步骤 2 根据(12b)式,明文矩阵 $\boldsymbol{P}_1$ 与其行变换矩阵 $\boldsymbol{P}_1^{\mathrm{r}}$ 相同,即 $\boldsymbol{P}_1 = \boldsymbol{P}_1^{\mathrm{r}}$,那么(13b)式可以表示为

$$\boldsymbol{P}_1^{\mathrm{rc}} = \boldsymbol{C}_1 \oplus \boldsymbol{B}_x = \boldsymbol{P}_1^{\mathrm{c}}. \tag{16}$$

根据(16)式计算得到 c 值,然后利用(15)式结果,通过列反变换求得 $\boldsymbol{P}'$的行置换矩阵 $\boldsymbol{P}'^{\mathrm{r}}$.

步骤 3 根据(12c)和(13c)式可知

$$\boldsymbol{P}_2^{\mathrm{rc}} = \boldsymbol{P}_2^{\mathrm{r}} = \boldsymbol{C}_2 \oplus \boldsymbol{B}_x. \tag{17}$$

根据(17)式计算 r 值,然后对行置换矩阵 $\boldsymbol{P}'^{\mathrm{r}}$ 进行反变换得到明文矩阵 $\boldsymbol{P}'$. 由此可知,HIE 算法抵御不了选择密文攻击.

由以上分析可知,根据三组特殊明密文对能够较容易地得到置乱次数,在得到置乱次数后,可以在密钥不变的情况下,通过破译密文就可以得到明文,从而实现了对加密系统的攻击. 只要几步简单的运算即可以得到想要的明文,因此,以较小的计算代价就能够破解 HIE 算法.

4. HIE 算法改进

针对 HIE 算法安全性上的弱点,本文提出一种改进的超混沌图像加密算法,具体实现过程如图 1 所示.

如图 1 所示,改进算法主要分为 3 个部分. 第一部分为超混沌系统,用于产生像素置乱及图像扩散、混乱所需的密钥;第二部分为像素置乱,对原始图像的像素矩阵进行行列置换;第三部分为图像扩散、混乱,进一步对置乱矩阵进行像素值扰乱.

4.1. 超混沌系统

超混沌系统[24]用如下方程描述:

$$\begin{aligned} \dot{x}_1 &= a(x_2 - x_1) + x_4, \\ \dot{x}_2 &= dx_1 - x_1x_3 + cx_2, \\ \dot{x}_3 &= x_1x_2 - bx_3, \\ \dot{x}_4 &= x_2x_3 + rx_4, \end{aligned} \tag{18}$$

其中 a, b, c, d 和 r 为系统的控制参数. 在 $a = 35, b = 3, c = 12, d = 7$ 条件下, r 处于区间 $[0, 0.085]$, $(0.085, 0.798]$, $(0.798, 0.90]$ 时,系统分别表现为混沌运动、超混沌运动、周期运动. 本文在 Matlab7.0 的环境下进行仿真,图 2 给出了超混沌系统在 $a = 35, b = 3, c = 12, d = 7$ 和 $r = 0.6$ 条件下的仿真结果. 系统(18)有两个正的 Lyapunov 指数 0.9076 和 0.0021,系统呈现超混沌行为,表现出比一般混沌系统更加复杂的动力学特性. 从安全性角度考虑,超混沌系统比低维混沌系统具有更复杂的相空间,因此用它设计加密系统能够获得比低维混沌系统更高的安全性.

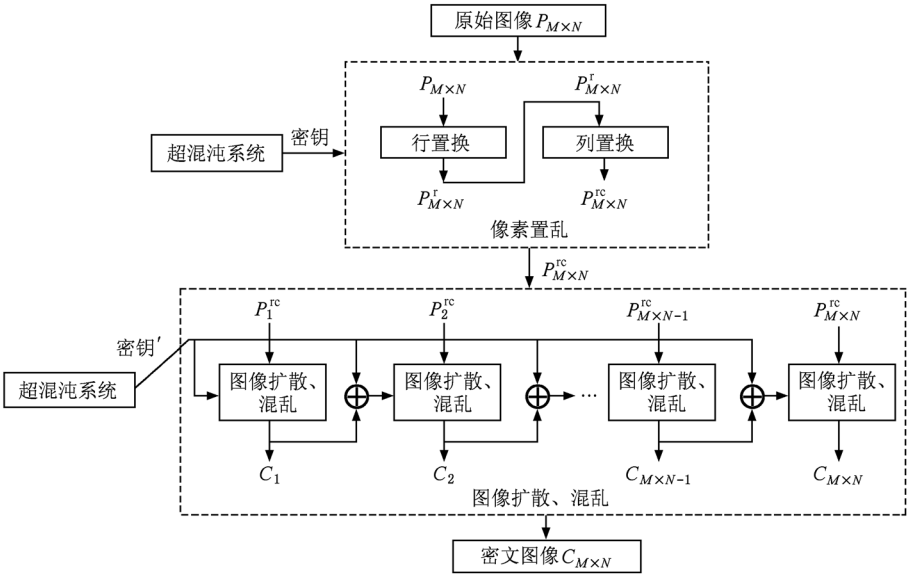

图 1 改进算法框图

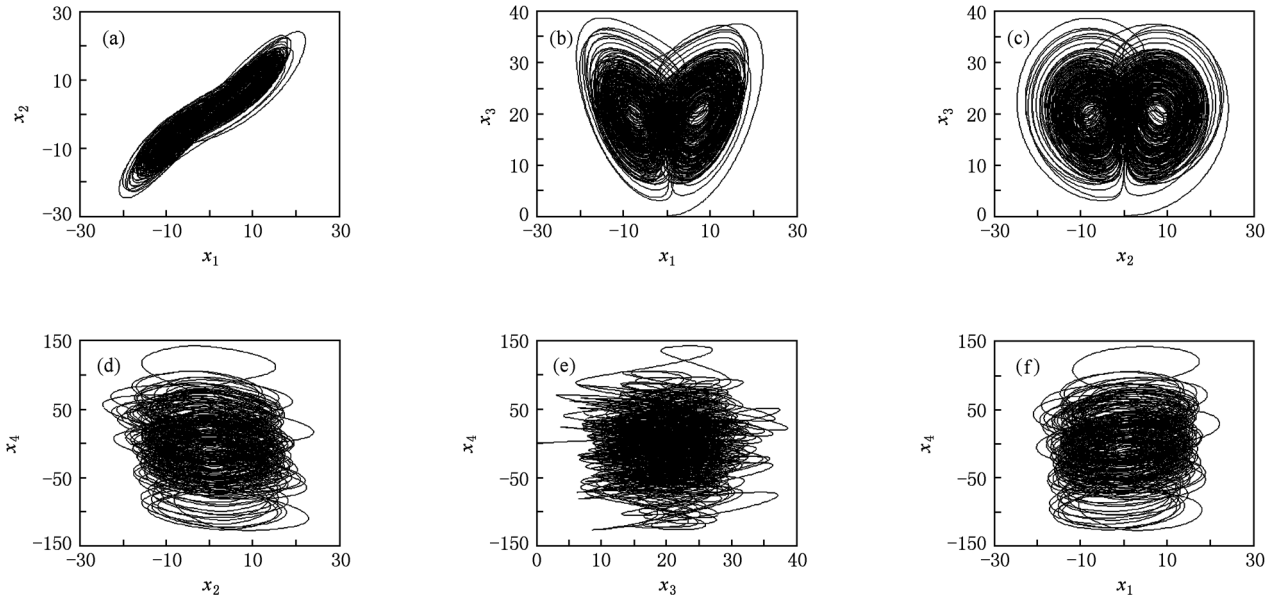

图 2 系统(18)的超混沌吸引子在平面上的投影 (a)(x_1,x_2)平面;(b)(x_1,x_3)平面;(c)(x_2,x_3)平面;(d)(x_2,x_4)平面;(e)(x_3,x_4)平面;(f)(x_1,x_4)平面

4.2. 像素置乱

利用数字图像具有数字阵列的特点,对图像矩阵进行有限步的初等矩阵变换,打乱图像像素的排列位置使之变成一幅杂乱无章的图像,达到无法辨认出原始图像的目的,从而起到图像加密的作用.

设原始图像为 $\boldsymbol{P}_{M\times N}$,像素矩阵可以表示为

$$\boldsymbol{P}=\begin{pmatrix} p_1 & p_2 & \cdots & p_N \\ \cdots & \cdots & \cdots & \cdots \\ p_{N(M-1)+1} & \cdots & \cdots & p_{MN} \end{pmatrix}. \tag{19}$$

步骤 1 利用 Runge-Kutta 算法将超混沌系统迭代 N_0 次,用于防止过渡效应. 对于给定的系统,

迭代次数 N_0 可能与初始条件及系统参数等有关，本文将丢弃前 $N_0 = 200$ 次迭代产生的数据，然后计算

$$r = \mathrm{mod}((\mathrm{abs}(x_1) - \mathrm{floor}(\mathrm{abs}(x_1))) \times 10^{14}, M). \tag{20}$$

显然，$r \in [0, M-1]$. 迭代超混沌系统直到产生 M 个完全不同的 r 值，记为 $\{r_i, i = 0,1,\cdots,M-1\}$. 根据 $\{r_i, i = 0,1,\cdots,M-1\}$ 对矩阵 P 进行行变换，结果记为

$$\boldsymbol{P}^{\mathrm{r}} = \begin{pmatrix} p_1^{\mathrm{r}} & p_2^{\mathrm{r}} & \cdots & p_N^{\mathrm{r}} \\ \cdots & \cdots & \cdots & \cdots \\ p_{N(M-1)+1}^{\mathrm{r}} & \cdots & \cdots & p_{MN}^{\mathrm{r}} \end{pmatrix}. \tag{21}$$

步骤 2 同理，计算

$$c = \mathrm{mod}((\mathrm{abs}(x_2) - \mathrm{floor}(\mathrm{abs}(x_2))) \times 10^{14}, N). \tag{22}$$

其中，$c \in [0, N-1]$. 迭代直到产生 N 个完全不同的 c 值，记为 $\{c_j, j = 0,1,\cdots,N-1\}$. 根据 $\{c_j, j = 0,1,\cdots,N-1\}$ 对(21)式的行置换矩阵 $\boldsymbol{P}^{\mathrm{r}}$ 进行列置换，变换后的矩阵记为

$$\boldsymbol{P}^{\mathrm{rc}} = \begin{pmatrix} p_1^{\mathrm{rc}} & p_2^{\mathrm{rc}} & \cdots & p_N^{\mathrm{rc}} \\ \cdots & \cdots & \cdots & \cdots \\ p_{N(M-1)+1}^{\mathrm{rc}} & \cdots & \cdots & p_{MN}^{\mathrm{rc}} \end{pmatrix}. \tag{23}$$

$\boldsymbol{P}^{\mathrm{rc}}$ 为原始矩阵 $\boldsymbol{P}$ 经过超混沌置乱后的矩阵，下面对 $\boldsymbol{P}^{\mathrm{rc}}$ 进行加密.

4.3. 图像扩散和混乱

扩散是要求将单个明文或密钥的影响尽可能扩大到更多的密文中，使得攻击者寻求明文冗余度增加了难度. 混乱则要求掩盖密文统计特性和明文统计特性之间的关系. 然而，文献[22]中由 Logistic 映射及超混沌系统产生的随机序列仅与初始值及系统参数有关，而不依赖于明文，导致一个明文字节只能影响其加密后的一个密文字节，给选择明文攻击和选择密文攻击带来了可乘之机. 基于这一缺陷，本文提出新的扩散混乱方法，以克服这一弱点并获得更高的安全性.

步骤 1 利用超混沌系统产生的随机序列计算

$$x_i = \mathrm{mod}((\mathrm{abs}(x_i) - \mathrm{floor}(\mathrm{abs}(x_i))) \times 10^{14}, 256) \quad i = 1,2,3,4. \tag{24}$$

显然，$x_i \in [0, 255]$. 然后计算

$$\bar{x}_1 = \mathrm{mod}((x_1 + x_2 + x_3 + x_4), 4). \tag{25}$$

步骤 2 根据 $\bar{x}_1 \in [0,3]$，从表 1 中选取相应组合对 4.2. 节产生的行列置换矩阵 $\boldsymbol{P}^{\mathrm{rc}}$ 进行加密，即

$$\begin{aligned} \boldsymbol{C}_{3\times(i-1)+1} &= \boldsymbol{P}^{\mathrm{rc}}_{3\times(i-1)+1} \oplus \boldsymbol{D}_{x_1}, \\ \boldsymbol{C}_{3\times(i-1)+2} &= \boldsymbol{P}^{\mathrm{rc}}_{3\times(i-1)+2} \oplus \boldsymbol{D}_{x_2}, \\ \boldsymbol{C}_{3\times(i-1)+3} &= \boldsymbol{P}^{\mathrm{rc}}_{3\times(i-1)+3} \oplus \boldsymbol{D}_{x_3}, \end{aligned} \tag{26}$$

其中，$\boldsymbol{D}_{x_1}$，$\boldsymbol{D}_{x_2}$ 和 $\boldsymbol{D}_{x_3}$ 如下式所示：

$$\begin{aligned} \boldsymbol{D}_{x_1} &= \mathrm{mod}((\boldsymbol{B}_{x_1} \oplus \boldsymbol{C}_{3\times(i-1)}), 256), \\ \boldsymbol{D}_{x_2} &= \mathrm{mod}((\boldsymbol{B}_{x_2} \oplus \boldsymbol{C}_{3\times(i-1)+1}), 256), \\ \boldsymbol{D}_{x_3} &= \mathrm{mod}((\boldsymbol{B}_{x_3} \oplus \boldsymbol{C}_{3\times(i-1)+2}), 256), \end{aligned} \tag{27}$$

显然，$\boldsymbol{D}_x \in [0, 255]$，其中 $i = 1,2,\cdots$ 表示第 i 次超混沌迭代.

步骤 3 若所有明文都已加密，则加密过程结束，否则转向步骤 1.

解密过程与加密过程相似. 首先，利用参数和初始值产生相同的超混沌序列，将(26)式替换为

$$\begin{aligned} P^{rc}_{3\times(i-1)+1} &= C_{3\times(i-1)+1} \oplus D_{x_1}, \\ P^{rc}_{3\times(i-1)+2} &= C_{3\times(i-1)+2} \oplus D_{x_2}, \\ P^{rc}_{3\times(i-1)+3} &= C_{3\times(i-1)+3} \oplus D_{x_3}. \end{aligned} \tag{28}$$

然后，根据 $\{r_i, i = 0,1,\cdots,M-1\}$ 和 $\{c_j, j = 0,1,\cdots,N-1\}$ 对矩阵进行行列反变换，就能够恢复出原始图像.

5. 实验仿真

5.1. 统计分析

在仿真过程中，为了评估改进算法的性能，本文选择了 256 kbit 的图像文件进行仿真，根据 Shannon 理论，统计分析通常用于密码分析和破译. 因此，一个密码系统在抗统计攻击方面应该具有很好的性能.

仿真结果如图 3 所示，图(a)为 256 kbit 的原始图像，图(b)为置乱后的图像. 由图 3 可见，置乱图像的像素点浓淡分布发生了很大的变化，画面类似白噪声，显示出了良好的置乱效果. 在图像置乱时，若不动点的数目越少，则说明置乱效果就越好，保密性就越高. 通常利用下式对不动点进行统计：

$$\delta = \left(\sum_{n=1}^{M\times N} \frac{\nabla_n}{M \times N}\right) \times 100\%, \tag{29}$$

$$\nabla_n = \begin{cases} 0 & (\mathrm{find}(p_n)\big|_{p_n \in p} \neq \mathrm{find}(p_n)\big|_{p_n \in p^{rc}}), \\ 1 & (\mathrm{find}(p_n)\big|_{p_n \in p} = \mathrm{find}(p_n)\big|_{p_n \in p^{rc}}), \end{cases} \tag{30}$$

其中,find(·)为 Matlab 中的位置命令;P 及 P^{rc} 概念和 4.2 节相同;p_n 对应像素值;M,N 为明文矩阵的尺寸. 根据(29)和(30)式,对图 3(b)的置乱不动点进行了统计,计算得到图 3(b)的置乱不动点比例为 $\delta = 0.257\%$,能够获得较好的置乱效果. 但是置乱后的图像仅仅是破坏了原来相邻像素之间的相关性,而没有改变各点的像素值,所以图像的灰度分布直方图不会改变,须对置乱图像的像素值做进一步的加密. 最终加密后的结果如图 3(c)所示,可见已经完全隐藏了原始图像,看不出原始图像的轮廓. 并且由图 3(d)和(e)能够看出,与分布不均匀的原始直方图相比,加密后的直方图平坦并且灰度值呈均匀分布. 这表明密文的像素值在[0—255]范围内的取值概率均等,即对整个密文空间呈均匀分布特性,从而说明本文提出的改进算法能够有效地防止统计攻击.

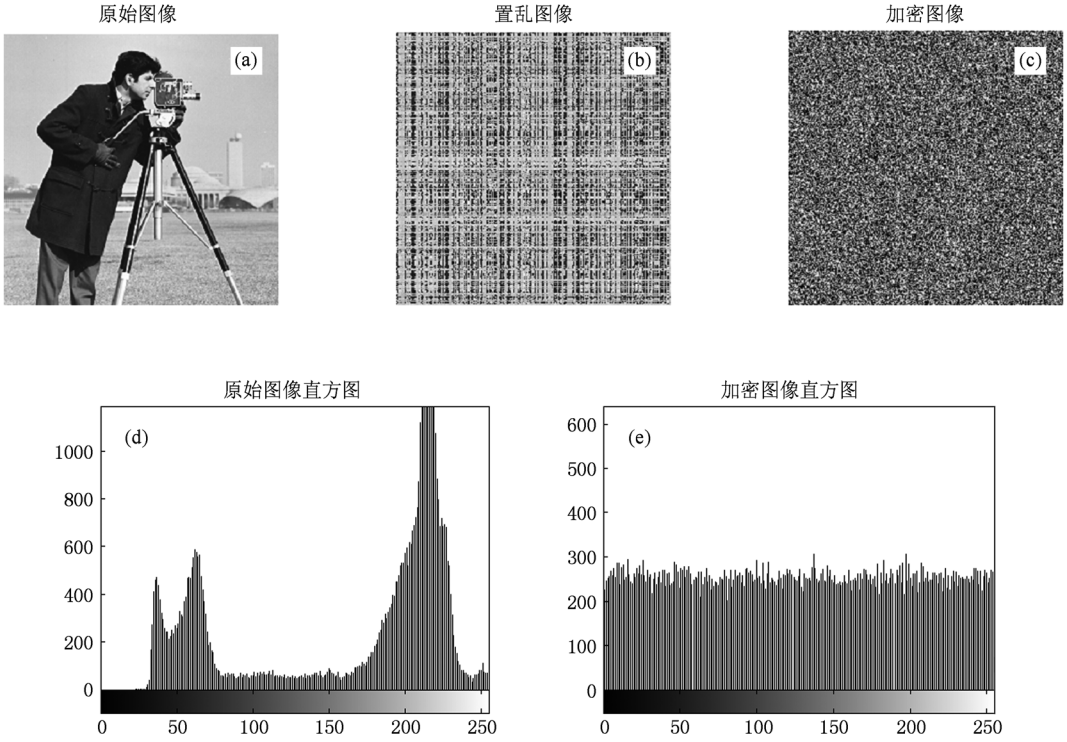

图 3 原始图像及加密图像的仿真 (a)原始图像;(b)置乱图像;(c)加密图像;(d)原始图像灰度分布直方图;(e)加密图像灰度分布直方图

5.2. 差分分析

像素数变化率(R_{NPC})和归一化平均变化强度(I_{UAC})是衡量图像加密算法抵抗差分攻击的重要指标. R_{NPC}和 I_{UAC}分别表示随机地改变原始图像的某个像素值以后,加密图像像素值发生改变的数目所占的比例以及变化程度. 若图像的某个像素值的改变可以很大程度地改变加密图像,则说明该算法具有较强的抵抗差分攻击能力.

下面令两幅加密图像分别为 $\boldsymbol{C}$ 和 $\boldsymbol{C}'$,这两幅图像对应的明文矩阵只有一个像素值不同. 位置(i,j)处的像素值分别记为 $C(i,j)$和 $C'(i,j)$. 定义矩阵 $\boldsymbol{D}$ 和 $\boldsymbol{C}$,$\boldsymbol{C}'$具有相同的大小,若 $C(i,j) = C'(i,j)$,则 $D_{i,j} = 0$;否则 $D_{i,j} = 1$. 则 R_{NPCR}和 I_{UACI}分别为

$$R_{\mathrm{NPC}} = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D_{i,j}}{M \times N} \times 100\%, \tag{31}$$

$$I_{\mathrm{UAC}} = \frac{1}{M \times N}\left(\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \frac{C(i,j) - C'(i,j)}{255}\right) \times 100\%. \tag{32}$$

将原始图像图 3(a)中位置(1, 89)处的像素值由 227 改变为 226,然后根据(31)和(32)式,计算得到 $R_{\mathrm{NPC}} = 99.75\%$,$I_{\mathrm{UAC}} = 33.92\%$. 由此可知,原始图像的稍微变化会引起密文图像的明显变化,所以改进算法能够有效地抵御差分攻击.

图 4 为密文差值图,为了更加直观地说明改进算法能够很好地抵御差分攻击,下面以图 4 为例进行说明. 扩散即为了隐藏明文的统计特性,使每一

位明文和密钥影响到较多的密文位. 混乱则是将密钥、明文和密文之间的统计特性尽可能复杂化. 通过扩散和混乱,才能够有效地抵抗差分攻击. 下面用文献[22]的算法和改进算法对明文进行微小的变化,改变前后密文的差值如图4(a),(b)所示;然后对参数 r 和初值 x_1 进行微小的变化,使用改进算法进行加密,改变前后密文的差值如图4(c),(d)所示.

由图4(a)能够看出,使用文献[22]中的算法进行加密,一位明文的微小变化将引起相应位密文的微小变化. 从图4(b)则能够直观地看出,使用改进算法对图像进行加密,若原始图像的一个像素值发生变化,则几乎导致了密文的完全变化. 同样通过图4(c),(d)能够看出,稍微改变参数 r 和初值 x_1,也将会引起密文的同样变化,进一步验证了改进算法的抗差分攻击特性.

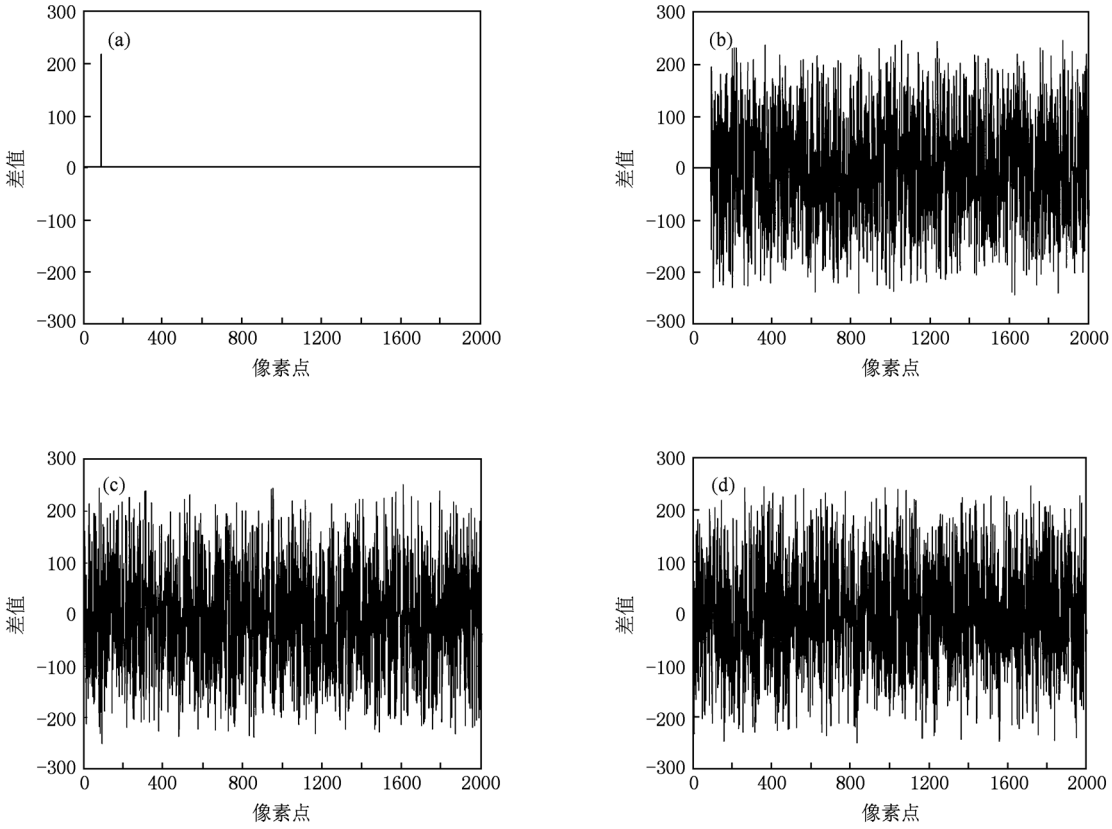

图4 密文差值 (a) HIE 算法:像素点(1, 89)的值由 227 改变为 226;(b)改进算法:像素点(1,89)的值由 227 改变为 226;(c)改进算法:参数 $r=0.6$ 改变为 $r=0.599$;(d)改进算法:初值 $x_1=0.2$ 改变为 $x_1=0.21$

5.3. 密钥敏感性测试

为了测试改进算法对密钥的敏感性,分别用 $r=0.6$ 和 $r=0.6001$ 对图像进行解密. 一种好的加密体制不仅应该对明文敏感,同时也应该对密钥敏感. 实验结果如图5所示,使用与正确密钥差值很小的错误密钥进行解密时,得到的是与原始图像大相径庭的错误图像,说明该算法对密钥具有高度的敏感性. 实验结果表明,尽管参数 r 只有微小的差异,但是也导致解密的完全失败,因此,改进算法拥有对密钥的极度敏感性.

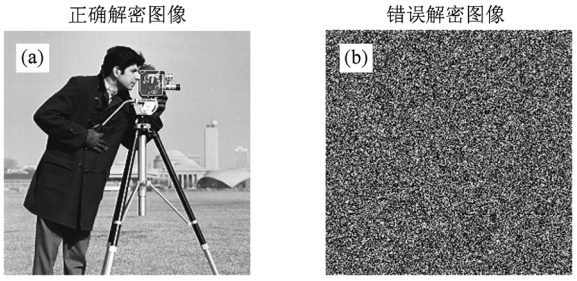

图5 $r=0.6$ 和 $r=0.6001$ 的解密图像 (a) r 正确时的解密图像;(b) r 错误时的解密图像

直观地将解密图像图5(a)及原始图像图3(a)进行比较,发现两者基本没有差别. 为了说明图像

的恢复功能,计算解密图像和原始图像的均方误差(E_{MS}).假定这两幅图像分别表示为 $\boldsymbol{P}$ 和 $\boldsymbol{P}'$,位置(i,j)处的像素值分别记为 $P(i,j)$ 和 $P'(i,j)$,则均方误差为

$$E_{MS} = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\{P(i,j) - P'(i,j)\}^2 . \tag{33}$$

将加密图像图 3(c)通过电子邮件发送、接收,然后进行解密. 根据(33)式进行计算,得到解密图像和原始图像之间的均方误差为 6.6129×10^{-7}. 由此可见,改进算法对恢复图像的性能影响不大.

5.4. 相关性分析

数字图像中各个像素不是独立的,其相关性很大. 这说明大块区域中的灰度值相差不大. 例如在一幅数字电视图像中,同一行中相邻两个像素或相邻两行的像素,其相关系数可达 0.9,而相邻两帧电视图像之间的相关性比帧内相关性还要大一些,因此图像信息的冗余度很大. 图像加密的目标之一就是减小相邻像素相关性,主要包括水平像素、垂直像素和对角线像素间的相关性. 显然,相关性越小,说明图像加密效果越好,安全性越高.

图 6 所示为垂直方向与水平方向上原始图像及改进算法的加密图像相邻像素的相关性,其中 Matlab 仿真时,坐标取值间隔为(1:10:255). 由图 6 可见,原始图像像素间的相关性呈现明显的线性关系,而加密图像像素间的相关性呈现随机的对应关系.

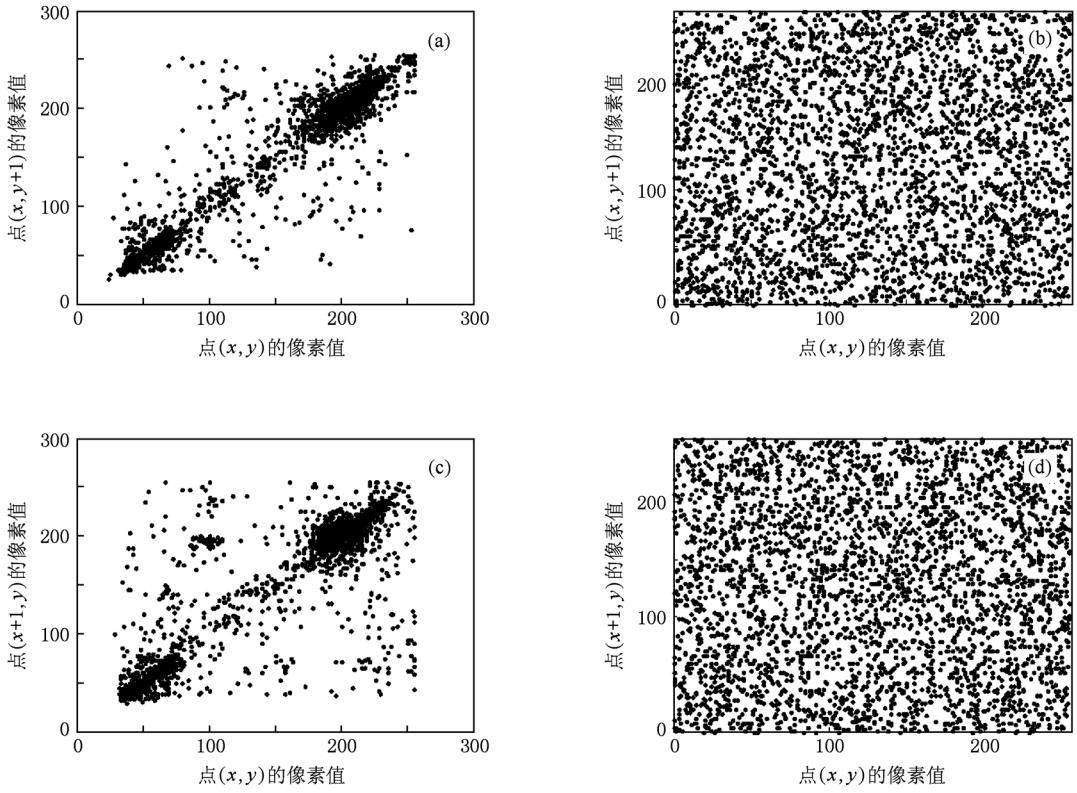

图 6 相邻像素相关性 (a)原始图像垂直方向相邻像素;(b)加密图像垂直方向相邻像素;(c)原始图像水平方向相邻像素;(d)加密图像水平方向相邻像素

表 2 所列为原始图像和改进算法的加密图像相邻像素之间按水平、垂直和对角 3 个方向计算所得的相关系数. 像素相关系数 ρ_{xy} 计算方法如下:

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

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 , \tag{34}$$

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

$$\rho_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)} \cdot \sqrt{D(y)}}, \tag{35}$$

其中 x 和 y 分别表示图像中相邻两个像素点的像素值,ρ_{xy} 为相邻两个像素点的相关系数. 由表 2 可见,原始图像的相邻像素高度相关,相关系数接近于 1. 而密

文图像的相邻像素相关系数很小,接近于零,其相邻像素已基本不相关,这表明原始图像的统计特征已经被扩散到随机的密文图像中了. 为了进一步说明改进算法的性能优于 HIE 算法,本文使用 USC-SIPI 图像数据库中的图像进行验证,通过 HIE 算法和改进算法对图像进行加密,然后计算得到的相关系数如表 3 所列.

表 2 原始图像和本文密文图像像素的相关系数

方向	原始图像	加密图像
水平	0.90575508240	−0.00091802226
垂直	0.95386852852	0.00366950017
对角	0.89619061295	0.00020674145

表 3 USC-SIPI 图像数据库中原始图像与加密图像的相关系数

图像文件名	垂直方向相关系数		水平方向相关系数		对角方向相关系数		原始图像及加密图像的相关系数	
	HIE 算法	改进算法	HIE 算法	改进算法	HIE 算法	改进算法	HIE 算法	改进算法
5.1.09	0.0156	0.0026	0.0175	0.0027	0.0083	−0.0007	0.0102	0.0006
5.1.10	0.0186	0.0013	0.0209	0.0030	0.0009	−0.0006	0.0081	−0.0017
5.1.12	0.0146	0.0058	0.0117	0.0084	0.0102	0.0019	0.0179	−0.0019
5.1.14	0.0147	0.0008	0.0089	0.0007	0.0076	0.0046	0.0017	0.0006
5.2.08	0.0142	0.0076	0.0103	0.0019	0.0061	−0.0004	0.0024	−0.0004
5.2.10	0.0097	−0.0043	0.0094	0.0006	−0.0100	0.0013	0.0061	0.0007
5.3.01	0.0073	−0.0027	0.0107	−0.0008	−0.0085	−0.0037	0.0028	0.0011
5.3.02	0.0286	0.0107	0.0069	0.0003	0.0071	0.0003	0.0034	0.0008
7.1.01	0.0137	0.0073	0.0094	0.0007	0.0016	0.0003	0.0019	−0.0003
7.1.02	0.0245	0.0082	0.0170	−0.0037	0.0082	0.0007	0.0040	−0.0009
7.1.03	0.0153	0.0026	0.0076	0.0007	−0.0103	0.0025	−0.0018	0.0007
7.1.04	0.0245	0.0175	0.0127	0.0008	−0.0057	−0.0008	0.0011	−0.0002
7.1.05	0.0084	−0.0037	0.0091	0.0049	−0.0107	0.0013	0.0017	0.0004
7.1.06	0.0147	0.0122	−0.0240	0.0072	0.0018	0.0005	0.0032	−0.0011
7.1.07	0.0093	0.0056	−0.0078	0.0009	0.0025	0.0007	0.0027	−0.0008
7.1.08	0.0200	−0.0138	−0.0073	−0.0017	0.0032	−0.0006	−0.0029	0.0005
7.1.09	0.0079	0.0024	0.0130	0.0053	0.0047	0.0002	0.0019	−0.0008
7.1.10	0.0093	0.0073	0.0778	0.0017	0.0081	−0.0002	0.0015	0.0001
7.2.01	0.0098	0.0025	0.0134	0.0008	−0.0019	0.0004	0.0031	0.0004

6. 结 论

混沌理论经过近些年的发展,已经取得了很多的研究成果,并被广泛地应用到通信安全领域. 然而,有些混沌加密系统没有遵循密码学中的一些基本准则,很容易被破译. 本文对一种超混沌图像加密算法进行了分析,发现该算法存在两个安全性缺陷. 基于此,本文给出了一种改进的超混沌图像加密算法. 在改进算法中,每个明文字节仍然保持一次加密运算,不采用反复迭代增加复杂性,因此加解密速度快,适用于实时通信. 同时,实验仿真表明,改进算法具有较好的统计特性、差分特性以及密钥敏感性等密码学特性.

[1] Pisarchik A N, Zanin M 2008 *Physica* D **237** 2638
[2] Yang D G, Liao X F, Wang Y 2009 *Chaos Soliton. Fract.* **41** 505
[3] Rontani D, Sciamanna M, Locquet A 2009 *Phys. Rev.* E **80** 066209
[4] Liu S B, Sun J, Xu Z Q 2009 *J. Computers* **4** 1091
[5] Mazloom S, Eftekhari-Moghadam A M 2009 *Chaos Soliton. Fract.* **42** 1745

[6] Xu S J, Wang J Z, Yang S X 2008 *Chin. Phys.* B **17** 4027
[7] Jin J X, Qiu S S 2010 *Acta Phys. Sin.* **59** 792 (in Chinese) [晋建秀、丘水生 2010 物理学报 **59** 792]
[8] Baptista M S 1998 *Phys. Lett.* A **240** 50
[9] Pareek N K, Patidar V 2005 *Commun. Nonlinear Sci. Numer. Simulat.* **10** 715
[10] Wong K W, Ho S W, Yung C K 2003 *Phys. Lett.* A **310** 67
[11] Xiang T, Liao X F, Tang G P 2006 *Phys. Lett.* A **349** 109
[12] Sun F Y, Liu S T, Li Z Q 2008 *Chaos Soliton. Fract.* **38** 631
[13] Behnia S, Akhshana A, Mahmodi H 2008 *Chaos Soliton. Fract.* **35** 408
[14] Yoon J W, Kim H 2010 *Commun. Nonlinear Sci. Numer. Simulat.* **15** 3998
[15] Yang H Q, Wong K W 2010 *Commun. Nonlinear Sci. Numer. Simulat.* **15** 3507
[16] Wang S H, Kuang J Y, Li J H 2002 *Phys. Rev.* E **66** 065202
[17] Chen C H, Sheu L J, Chen H K 2009 *Nonlinear Analysis: Real World Applications* **10** 2088
[18] Wang H, Han Z Z, Xie Q Y, Zhang W 2009 *Commun. Nonlinear Sci. Numer. Simulat.* **14** 2239
[19] Cokal C, Solak E 2009 *Phys. Lett.* A **373** 1357
[20] Aguilar-Bustos A Y, Cruz-Hernández C, López-Gutiérrez R M, Tlelo-Cuautle E 2010 *Hyperchaotic Encryption for Secure E-Mail Communication* (London: *Springer London*) p471
[21] Yao H X, Li M 2009 *Inter. J. Nonlin. Sci.* **7** 379
[22] Gao T G, Chen Z Q 2008 *Phys. Lett.* A **372** 394
[23] Rhouma R, Belghith S 2008 *Phys. Lett.* A **372** 5973
[24] Park J H 2005 *Chao Soliton. Fract.* **26** 959

Cryptanalysis of a hyper-chaotic image encryption algorithm and its improved version*

Wang Jing[1)†] Jiang Guo-Ping[1)2)]

1) (*Center for Control and Intelligence Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

2) (*College of Automation, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

(Received 13 August 2010; revised manuscript received 30 September 2010)

Abstract

According to the Kerckhoff principle, a kind of image encryption algorithm based on hyper-chaos is discussed through choosing plaintext attack and ciphertext attack. The result shows that the key stream is independent of plaintext and one plain-text word is correlated with single cipher-text word for the algorithm, which makes the ciphertext decrypted easily with little computing by choosing plaintext and ciphertext attack. Considering the above problems, an improved algorithm based on hyper-chaos is proposed and the performance analysis is conducted, including statistical analysis, differential analysis, correlation analysis and key sensitivity testing. Theoretical analysis and simulation results show that the improved algorithm not only can resist the chosen plaintext attack and chosen ciphertext attack, but also can obtain better cryptographic properties, such as statistical characteristics, difference characteristics and so on.

Keywords: hyper-chaos, chosen plaintext attack, chosen ciphertext attack, Matlab analysis

PACS: 05.45.Gg

* Project supported by the National Natural Science Foundation of China (Grant No. 60874091), the Natural Science Basic Research Program of Institution of Higher Education of Jiangsu Province, China (Grant No. 08KJD510022), the "Summit of the Six Top Talents" Program of Jiangsu Province, China (Grant No. SJ209006), and the Program for Talents in Nanjing University of Posts and Telecommunications, China (Grant No. NY209021).

† E-mail: jingwang@njupt.edu.cn