针对基于感知器模型的混沌图像加密算法的选择明文攻击

朱淑芹 王文宏 李俊青
(聊城大学计算机学院 山东 聊城 252059)

摘 要 对一种基于感知器模型的混沌图像加密算法进行了安全性分析,发现该算法的本质就是根据等效密钥流来改变明文图像像素值的比特位,从而得到密文图像。而等效密钥流与明文图像和对应的密文图像没有任何关系,因此运用选择明文攻击的方法破解出了算法中的等效密钥流,解密出了目标明文图像;同时指出了原算法存在的另外两个安全缺陷;最后对原算法进行了改进,弥补了其缺陷。理论分析和实验结果均证实了所提出的选择明文攻击策略的可行性以及改进算法的有效性。

关键词 混沌图像加密,密码分析,等效密钥,选择明文攻击
中图法分类号 TP391 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.04.030

Chosen Plaintext Attack on Chaotic Image Encryption Algorithm Based on Perceptron Model

ZHU Shu-qin WANG Wen-hong LI Jun-qing
(School of Computer Science, Liaocheng University, Liaocheng, Shandong 252059, China)

Abstract This paper analyzed the security of a chaotic image encryption algorithm based on preceptron model and found that the essence of the algorithm is to change the value of bits of the plaintext image according to the equivalent key stream to get the cipher image. However, there is no relation between the equivalent key stream and the plain text image or the corresponding cipher text image. By applying chosen plaintext attacks, this paper found that the equivalent key can be cracked, which can be further exploited to decrypt the target plain image. In addition, two other security defects were also reported. Finally, the original algorithm was improved to overcome the shortcomings of the original algorithm. Both mathematical analysis and experimental results show that the feasibility of the proposed chosen plaintext attack strategies and the effectiveness of the improved algorithm are verified.

Keywords Chaotic image encryption, Cryptanalysis, Equivalent key, Chosen plaintext attack

1 引言

混沌作为非线性科学的重要分支,是自然界中普遍存在的、确定的、不可预测的复杂运动形式。它具有良好的遍历性以及对参数和初值的敏感性,因此与密码学具有天然的联系[1]。图像信息自身固有的特性,如信息表达直观、信息量大、相邻像素的相关性强、冗余度大,以及人眼视觉系统的特性,使得传统的加密算法如DES,IDEA和RSA已经不再适用于图像信息加密的应用场合[2]。自Baptism于1998年提出使用一维混沌的遍历性进行加密以来[3],基于混沌的数字图像加密逐渐成为了一个研究热点。国内外学者提出了许多加密算法[4-14]。Liu等[4]将鼠标位置的MD5值作为混沌映射的初值,提出了"一次一密"的彩色图像混沌加密算法。文献[5]提出一种通过行、列两轮置乱来进行扩散运算的新的彩色图像加密算法。韩凤英等[6]提出了一种改进型置换-替代结构图像加密算法,在改进算法中进行像素位置置乱时,随机选择两个不同区域内的像素对进行位置交换,明显提高了像素的置乱度;而在进行像素值变换时,为提高密钥矢量的破解难度,将像素值变换的扩散矢量与像素位置变换的置乱矢量相耦合。刘泉等[7]利用真随机数发生器产生的随机数来扰动混沌系统产生的初始密钥,以动态生成图像的置换矩阵和加密密钥流,然后利用不同群中的加法混合运算构造扩散函数,以增加破译复杂度,最后以两轮迭代完成了图像加密过程。Liu等[8]提出了一种基于高维混沌和像素比特位置乱的彩色图像加密算法,该算法首先对像素的比特位进行置乱,然后进行扩散、混淆操作。比特位置乱不仅有置乱的作用,还可以改变像素值,从而使得密码系统的安全性得到较大提升。文献[4-8]提出的算法都是基于图像像素的置乱和像素扩散的加密思想。另外,一些混沌图像加密算法结合了DNA编码的思想[9-11],另一些混沌图像加密算法结合了DNA编码和椭圆曲线公钥密码系统的思想[12]。文献[13]提出了一种基于混沌映射和正交矩阵的压缩感知和抗噪图像加密方案。Wang

到稿日期:2017-01-18 返修日期:2017-03-10 本文受国家自然科学基金面上项目(61573178),聊城大学校基金(318011606),山东省自然科学基金(ZR2017MEM019)资助。

朱淑芹(1979-),女,硕士,讲师,主要研究方向为混沌理论、图像处理,E-mail:shuqinzhu2008@163.com(通信作者);王文宏(1973-),男,博士,副教授,主要研究方向为图像处理、模式识别、机器视觉;李俊青(1976-),男,博士,副教授,主要研究方向为优化调度理论、保密通信。

等[14]提出了一种基于感知器模型的混沌图像加密算法，该算法的基本思想是利用混沌映射生成的伪随机序列动态地调整单层感知器中各个神经元的权重，从而改变神经元的输出，实现图像的加密。该算法首次把感知器模型引入混沌加密系统，具有一定的创新性，这种与其他模型或算法相结合的混沌图像加密算法给混沌图像加密领域注入了新的“血液”，拓宽了人们的思路和视野。但是，一个好的创新算法在与新模型相结合的基础上需要成熟的理论作为支撑，否则很容易被破解，因此对这些融合了新模型的混沌图像加密算法进行安全性分析是必要的。通过深入分析文献[14]的算法发现，该算法的本质是根据密钥流来改变明文图像的像素值的比特值，进而得到密文图像，而密钥流与明文图像和对应的密文图像没有任何关系。因此，可以运用选择明文攻击的方法来破解等效密钥流，从而解密出目标明文图像。本文介绍如何对文献[14]的算法做选择明文的攻击分析并破译出明文图像。

2　原算法描述

原算法采用 Lorenz 系统作为密钥生成源。Lorenz 系统如式(1)所示：

$$\begin{cases}\dfrac{\mathrm{d}x}{\mathrm{d}t}=a(y-x)\\ \dfrac{\mathrm{d}y}{\mathrm{d}t}=cx-xz-y\\ \dfrac{\mathrm{d}z}{\mathrm{d}t}=xy-bz\end{cases}\tag{1}$$

当参数 $a=10$，$b=8/3$，$c=28$ 时，系统进入混沌的状态。

原加密算法的具体描述如下：

1)选取 X_0，Y_0，Z_0 作为系统的初始值，对 Lorenz 系统进行 8 次迭代，即可得到 X_k，Y_k，Z_k，$k\in[1,8]$。

2)按照非线性的变化规则，即式(2)和式(3)，将变换得到的 $keyX(k)$和 $keyY(k)$($k\in[1,8]$)作为感知器权值的参数。

$$keyX(k)=\begin{cases}1, & \text{if } x_k\geqslant 0.5\\ 0, & \text{if } x_k<0.5\end{cases}\tag{2}$$

$$keyY(k)=\begin{cases}1, & \text{if } y_k\geqslant 0.5\\ 0, & \text{if } y_k<0.5\end{cases}\tag{3}$$

其中：

$x_k=(X_k-X_{\min})/(X_{\max}-X_{\min})$

$y_k=(Y_k-Y_{\min})/(Y_{\max}-Y_{\min})$

$X_{\max}=\max\{X_k\}$，$X_{\min}=\min\{X_k\}$

$Y_{\max}=\max\{Y_k\}$，$Y_{\min}=\min\{Y_k\}$

$k=1,2,\cdots,8$

3)为了增强高维 Lorenz 系统的周期性，使用式(4)和式(5)对下轮混沌迭代变量值 X 和 Y 进行扰乱，而将 Z 值用上一轮迭代中的 Z_8 表示。m 由在 Z_8 中随机抽取 8 比特位生成。

$$\begin{cases}w_i=\sum\limits_{k=1}^{8}keyX(k)2^{k-1}\\ w_j=\sum\limits_{k=1}^{8}keyY(k)2^{k-1}\end{cases}\tag{4}$$

$$\begin{cases}X=((w_j\oplus m)x_8/256)(X_{\max}-X_{\min})+X_{\min}\\ Y=((w_i\oplus m)y_8/256)(Y_{\max}-Y_{\min})+Y_{\min}\end{cases}\tag{5}$$

4)采用流加密策略对图像进行加密。取图像中的任意一个像素值 b，b_k($k\in[1,8]$)是像素值的第 k 个比特位。加密之后的密文的像素值为 b'，b_k'($k\in[1,8]$)是像素值的第 k 个比特位。密文的输出如式(6)所示：

$$b_k'=\begin{cases}f(w_{1,k}b_k+w_{2,k}c_k-\theta_k), & w_{1,k}=1\\ f(w_{1,k}b_k-w_{2,k}c_k+\theta_k), & w_{1,k}=-1\end{cases}\tag{6}$$

其中：

$$f(x)=\begin{cases}1, & x\geqslant 0\\ 0, & x<0\end{cases}$$

$$w_{1,k}=\begin{cases}1, & \text{if } keyX(k)=1\\ -1, & \text{else}\end{cases}$$

$$w_{2,k}=\begin{cases}1, & \text{if } keyY(k)=1\\ -1, & \text{else}\end{cases}$$

$$c_k=\begin{cases}-0.5, & w_{1,k}=1\\ 0.5, & w_{1,k}=-1\end{cases}$$

$$w'_{1,k}=\begin{cases}1, & w_{1,k}=1\\ 0, & w_{1,k}=-1\end{cases}$$

$$w'_{2,k}=\begin{cases}1, & w_{2,k}=1\\ 0, & w_{2,k}=-1\end{cases}$$

$\theta_k=w'_{1,k}\oplus w'_{2,k}$

5)重复步骤 2)－步骤 4)，直到整个图像加密完成。

3　原算法的密码分析

密码分析是分析、破解密码的一门科学，能在不知道密钥的情况下设法恢复出密钥或者相关明文。另一方面，密码分析能够发现密码体制中的弱点，对提高密码设计有促进作用。根据 Kerchhoff 原则[15]，安全的密码系统是假设密码分析者知道除密钥以外的所有可能信息，包括加密、解密的算法以及部分明文或者部分明文-密文对等，而系统的安全仅仅依赖于密钥的安全。根据密码分析者知道信息的多少，密码攻击由难到易有以下 4 种类型：1)唯密文攻击；2)已知明文攻击；3)选择明文攻击；4)选择密文攻击。

3.1　选择明文攻击分析

选择明文攻击是指攻击者暂时获得加密机的使用权，他能加密任意的明文，并获得相对应的密文，以此破译出全部或部分明文和密钥[5]。在进行选择明文攻击之前，先给出原加密算法的一个性质，这正是选择明文攻击的核心。

性质 1　在原加密算法的步骤 4)中，式(6)等价于式(7)：

$$b_k'=\begin{cases}f(b_k-0.5), & w_{1,k}=1\\ f(0.5-b_k), & w_{1,k}=-1\end{cases}\tag{7}$$

证明：1)当 $w_{1,k}=1$，$w_{2,k}=1$ 时，可以得到：$c_k=-0.5$，$w'_{1,k}=1$，$w'_{2,k}=1$，$\theta_k=0$。因此，由原加密算法中的式(6)可得式(8)：

$$b_k'=f(b_k-0.5)\tag{8}$$

2)当 $w_{1,k}=1$，$w_{2,k}=-1$ 时，可以得到 $c_k=-0.5$，$w'_{1,k}=1$，$w'_{2,k}=0$，$\theta_k=1$。因此，由原加密算法中的式(6)可得式(9)：

$$b_k'=f(b_k-0.5)\tag{9}$$

因此，由情况 1)和情况 2)知：当 $w_{1,k}=1$ 时，$b_k'=f(b_k-0.5)$。

3)当 $w_{1,k}=-1$，$w_{2,k}=1$ 时，可以得到 $c_k=0.5$，$w'_{1,k}=0$，$w'_{2,k}=1$，$\theta_k=1$。因此，由原加密算法中的式(6)可得式(10)：

$b_k'=f(0.5-b_k)$ (10)

4)当 $w_{1,k}=-1,w_{2,k}=-1$ 时,可以得到 $c_k=0.5,w'_{1,k}=0,w'_{2,k}=0,\theta_k=0$。因此,由原加密算法中的式(6)可得式(11):

$b_k'=f(0.5-b_k)$ (11)

由情况 3)和情况 4)可知:当 $w_{1,k}=-1$ 时,$b_k'=f(0.5-b_k)$。

综合情况 1)-情况 4)可得式(7),证明完毕。

从式(7)可以看出:当 $w_{1,k}=1$ 时,b_k' 与 b_k 的值相同;当 $w_{1,k}=-1$ 时,若 $b_k=1$,则 $b_k'=0$;若 $b_k=0$,则 $b_k'=1$。因此,原算法中的等效密钥流就是 $w_{1,k}$,而 $w_{1,k}$ 的生成完全依赖于 Lorenz 混沌系统(1),与明文图像和对应的密文图像没有任何关系,即加密不同的图像所用的密钥流是相同的,故可以采用选择明文攻击的方法来破解等效密钥流,进而破译出目标明文图像。

3.2 选择明文攻击的具体步骤

1)加密一幅与目标密文图像同大小且像素值全为 0 的图像 T,设其大小为 $M\times N$,得到其对应的密文图像矩阵为 CT,然后把 CT 中的每个元素转化为 8 位二进制数,得到大小为 $M\times(N\times 8)$的二进制矩阵 BT。

2)把矩阵 BT 中的 0 替换为 1,把 BT 中的 1 替换为-1,从而得到一个新的矩阵 W,W 就是由 $w_{1,k}$ 构成的密钥流矩阵。

3)假设需解密的目标密文图像矩阵 C 的大小为 $M\times N$,把 C 中的每个元素转化为 8 位二进制数,得到大小为 $M\times(N\times 8)$的二进制矩阵 BC,然后根据得到的等效密钥流矩阵 W 进行解密操作。Matlab 伪代码的描述为:

```
H=ones(M,N×8);
for i=1:M
  for j=1:N×8
    if W(i,j)==1
  H(i,j)=BC(i,j);
    else if W(i,j)==-1&BC(i,j)==1
      H(i,j)=0;
      else
      H(i,j)=1;
  end
end
  end
end
```

经过上述步骤后,便得到一个新的二进制矩阵 H,把 H 中的每 8 位 0,1 序列转化为一个十进制数,从而得到一个大小为 $M\times N$ 的矩阵 P。P 就是解密出的目标明文图像矩阵。

3.3 原算法中的另外两个安全性缺陷

1)算法中密文对明文的变化不敏感

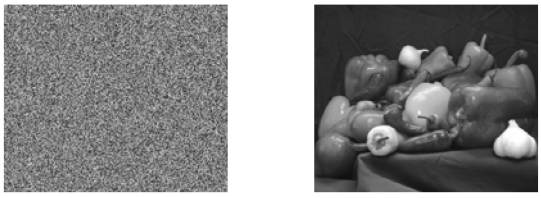
密文对明文的敏感性是指明文图像的任何变化都将导致加密后的密文图像与原密文图像完全不同。密文对明文敏感,说明算法具有很好的抗差分攻击性能。原加密算法中没有像素值的扩散和混淆操作,同时所用混沌系统的初始值与明文/密文没有任何关系。显然,由原算法步骤 4)中的式(6)可知,明文图像中一个像素值的变化只会影响到对应密文图像的一个像素值,因此原算法中密文对明文的变化不敏感。

2)原算法不能抵抗剪切攻击

文献[14]称其提出的算法能够抵抗剪切攻击,这是不对的。因为密文图像被剪切的部分在解密后的明文图像中不能被恢复,具体请参考文献[14]中的章节 4。主要原因在于,该算法的本质就是根据密钥流 $w_{1,k}$ 来改变像素的比特位的值,没有像素的置乱操作。

3.4 密文破译仿真实验

仿真实验在 Matlab2014a 平台上进行,选用大小为 384×521 的 256 级灰度图像 peppers,选定 Lorenz 混沌系统参数 $a=10,b=8/3,c=28$;系统的初始值为 $x=0,y=0,z=10^{-10}$,对 peppers 加密的结果如图 1(a)所示。在未使用加密密钥的前提下,由第 3.2 节的密码分析算法破译出图 1(a)对应的明文图像,结果如图 1(b)所示。上述结果表明,密码破译是成功的。



(a)Peppers 的密文图像 (b)破译出的明文图像

图 1 用选择明文攻击破解出的图像

Fig. 1 Decrypted images by using chosen plaintext attacks

4 改进算法及其安全性分析

4.1 改进算法

针对原算法存在的安全缺陷,本文进行了 3 方面的改进:1)为使算法进一步抵抗剪切、噪声污染及压缩的攻击,增加置乱操作;2)为使算法抵抗选择明文的攻击,将原算法步骤 3)中式(5)的 m 值用前一步加密得到的密文像素值代替,使得密钥流与密文图像相关,可以达到“一次一密”的加密效果;3)为了进一步提高系统的安全性,利用密文反馈机制进行扩散操作。具体步骤如下:

1)设待加密的图像为 A,其大小为 $m\times n$,将明文图像 A 转换为长度为 $m\times n$ 的一维序列 $L=\{l_1,l_2,l_3,\cdots,l_{m*n}\}$。设置 Logistic 映射 $x(k+1)=ax(k)(1-x(k))(a\in[3,5699456,4])$的初值 $x(0)$,生成长度为 $m\times n$ 的混沌序列 $X=\{x_1,x_2,x_3,\cdots,x_{m*n}\}$。

2)对混沌序列 X 进行从小到大的排序,产生一个用于记录排序后的序列中各元素在原序列 K 中所在位置的位置序列 $T=\{t_1,t_2,t_3,\cdots,t_{m*n}\}$,并借助其来对明文序列 L 进行位置置乱,从而得到置乱后的图像序列 L'。

3)对置乱后的图像序列 L' 进行文献[14]中原算法的操作,但将原算法步骤 3)中式(5)的 m 值用前一步加密得到的密文像素值代替,从而得到密文流 $B'=\{b_1',b_2',\cdots,b'_{mn}\}$。改进算法有置乱操作并且在下轮迭代时,混沌系统的初值与密文相关,因此改进算法克服了原算法不能抵抗选择明文攻击、剪切攻击和密文对明文不敏感的不足。

4)为进一步加强系统的安全性,对 Logistic 映射产生的混沌序列 X 进行如式(12)所示的操作,得序列 S。

$$S=\mathrm{mod}(\mathrm{round}(10^{15}X),256)=(s_1,s_2,s_3,\cdots,s_{mn}) \quad (12)$$

对中间密文流 B' 和序列 S 做式(13)、式(14)的操作，得到最终的密文流 $C=(c_1,c_2,c_3,\cdots,c_{mn})$。

$$c_1=\mathrm{bitxor}(\mathrm{mod}(b_1'+s_0,256),\mathrm{mod}(s_1+c_0,256)) \quad (13)$$

$$c_i=\mathrm{bitxor}(\mathrm{mod}(b_i'+s_{i-1},256),\mathrm{mod}(s_i+c_{i-1},256)) \quad (14)$$

其中，$i=2,3,\cdots,mn$，c_0 和 s_0 为{0，255}上的随机数。

4.2　改进算法的安全性分析

对于改进算法的安全性分析，本文只进行密文对明文的变化敏感性分析和密文抵抗压缩、噪声污染及剪切攻击的分析。其他的安全分析在此不再赘述，具体请参见文献[14]。

4.2.1　密文对明文的变化敏感性分析

一般用像素数改变率 NPCR 和归一化平均改变强度 UACI 这两个指标来度量加密算法对明文的敏感性。对于 8 位灰度图像，*NPCR* 与 *UACI* 的理想期望值分别为99.6094%和 33.4635%。*NPCR* 与 *UACI* 的计算公式[16]分别为式(15)和式(16)：

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D_{ij}}{M\times N}\times 100\% \quad (15)$$

$$UACI=\frac{(\sum_{i=1}^{M}\sum_{j=1}^{N}(\frac{c_1(i,j)-c_2(i,j)}{255}))}{M\times N}\times 100\% \quad (16)$$

当两个明文图像仅存在一个像素不同时，假设它们的密文图像中点(i,j)的像素值分别为 $C_1(i,j)$和 $C_2(i,j)$，则定义 $D(i,j)$为：

$$D(i,j)=\begin{cases}0, & \text{if } C_1(i,j)=C_2(i,j)\\ 1, & \text{if } C_1(i,j)\neq C_2(i,j)\end{cases} \quad (17)$$

所提算法随机选取原图像中的 5 个像素点并改变其像素值，计算出的 *NPCR* 和 *UACI* 如表 1 所列。

表 1　改进算法对明文图像微小改变的 *NPCR* 和 *UACI* 测试结果

Table 1　*NPCR* and *UACI* test results of improved algorithm for slight change of plaintext images

（单位：%）

明文的微小改变	*NPCR*	*UACI*
$G(38,95)$由 210 变为 211	99.5318767	33.478924
$G(312,157)$由 134 变为 135	99.5856892	33.562819
$G(235,45)$由 119 变为 120	99.7458758	33.456112
$G(135,215)$由 125 变为 26	99.5890947	33.3573057
$G(428,173)$由 229 变为 230	99.5657975	33.2340506

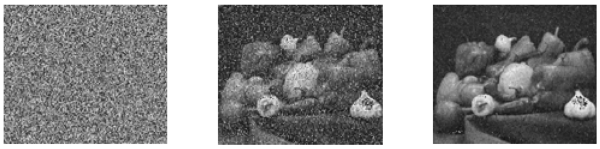
由表 1 可看出，原图像中一个像素灰度值的改变会导致密文图像中几乎所有的像素值都发生变化，说明改进算法的密文对明文敏感。

4.2.2　抗攻击测试

抗攻击测试主要是测试密文图像抗压缩、噪声污染及剪切等攻击的能力。

1)抗压缩攻击测试

首先对密文图像进行压缩，再对压缩后的密文图像解密，以进行抗压缩攻击测试。图 2(b)和图 3(b)分别是把密文图像压缩为原图像的 60%和 80%后(图 2(a)和图 3(a))解密出的图像。可以看出，压缩比越大，解密后的图像含噪声越多，图像越模糊，但仍然可看出图像的大体轮廓。解密出的图像经过中值滤波后(图 2(c)和图 3(c))，视觉效果良好。



(a)加密后的图像压缩为原图像的 60%后的图像　(b)解密图像　(c)对(b)进行中值滤波后的图像

图 2　针对改进算法的密文抗压缩攻击的测试

Fig. 2　Anti-compression attack test of ciphertext for improved algorithm

(a)加密后的图像压缩为原图像的 80%后的图像　(b)解密图像　(c)对(b)进行中值滤波后的图像

图 3　针对改进算法的密文抗压缩攻击的测试

Fig. 3　Anti-compression attack test of ciphertext for improved algorithm

2)抗噪声污染攻击测试

通过在加密后的图像中人为地加入各种噪声来测试加密图像的抗击噪声能力。椒盐噪声的强度最大，噪声分布最稀松。泊松噪声和高斯噪声的分布较密，高斯噪声的强度比泊松噪声的强度更大。密文图像如果能够抗击高斯噪声的污染，则一定也能够抗击其他噪声的污染。限于篇幅，此处只给出密文图像抗击高斯噪声污染的实验结果。图 4(b)为密文图像被强度为 0.002 的高斯噪声污染后(图 4(a))解密图像，可以看出解密后的图像带有严重的噪声，但是经过中值滤波后(图 4(c))视觉效果良好。

(a)加密后的图像经强度为 0.002 的高斯噪声污染后的图像　(b)解密图像　(c)对(b)进行中值滤波后的图像

图 4　针对改进算法的密文抗噪声污染攻击的测试

Fig. 4　Anti-noise pollution attack test in ciphertext for improved algorithm

3)抗裁剪测试

对密文图像进行不同程度的剪切，再对剪切后的密文图像解密，以测试算法抗击裁剪攻击的能力。图 5(a)和图 5(b)分别为加密后的图像经中间部分裁剪后的图像及其解密图像。从图 5 可以看出，加密后的图像经过不同程度的裁剪后，解密后的图像存在细微的噪声，但不影响图像的整体效果。其原因在于，混沌序列对图像各点置乱均匀，无论剪切哪个部位的一定面积的加密后的图像，解密后的图像都能基本辨清其轮廓。

(下转第 189 页)

[7] CHEN L，CONG G，JENSEN C S，et al. Spatial keyword query processing：an experimental evaluation[J]. Proceedings of the VLDB Endowment，2013，6(3)：217-228.

[8] DE FELIPE I，HRISTIDIS V，RISHE N. Keyword Search on Spatial Databases[C]// International Conference on Data Engineering. IEEE Computer Society，2008：656-665.

[9] ZHANG D，TAN K L，TUNG A K H. Scalable top-k spatial keyword search[C]// International Conference on Extending Database Technology. ACM，2013：359-370.

[10] ZHOU Y H，XIE X，WANG C，et al. Hybrid index structures for location-based Web search[C]// DBLP. 2005：155-162.

[11] CONG G，JENSEN C S，WU D. Efficient retrieval of the top-k most relevant spatial web objects[J]. Proceedings of the VLDB Endowment，2009，2(1)：337-348.

[12] ZHANG D X，CHEE Y M，MONDAL A，et al. Keyword search in spatial databases：Towards searching by document[C]// International Conference on Data Engineering. IEEE，2009：688-699.

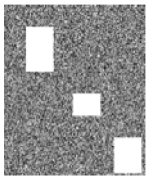
[13] LI Y H，HUANG Q，JIANG H，et al. Research on Processing Continuous Spatial Keyword Range Queries in Road Networks [J]. Computer Science，2014，41(7)：232-235. (in Chinese)
李艳红，黄群，蒋宏，等. 路网中空间关键字连续范围查询算法研究[J]. 计算机科学，2014，41(7)：232-235.

[14] HMEDEH Z，KOURDOUNAKIS H，CHRISTOPHIDES V，et al. Subscription indexes for web syndication systems[C]// International Conference on Extending Database Technology. ACM，2012：312-323.

[15] MANNING C D，RAGHAVAN P，SCHÜTZE H. An Introduction to Information Retrieval[J]. Journal of the American Society for Information Science & Technology，2008，43(3)：824-825.

[16] SILBERSCHATZ A，KORTH H F，SUDARSHAN S. Database System Concepts[M]. New York，USA：McGraw-Hill，2006.

(上接第 181 页)



(a)加密后的图像经部分裁剪后的图像

(b)解密图像

(c)对(b)进行中值滤波后的图像

图 5　针对改进算法的密文抗裁剪测试攻击的测试

Fig. 5　Anti-cutoff test attack test in improved algorithm

结束语　本文对基于感知器模型的混沌图像加密算法进行了安全性分析，结果发现该算法不能抵抗选择明文的攻击。通过选择明文攻击，得出了该密码算法的等效密钥，从而破解出了目标明文。同时，指出了该算法存在的另外两个安全缺陷：1)密文对明文的变化不敏感；2)算法不能抵抗剪切攻击。基于前面的分析，对原算法进行了改进，以提高其安全性能。改进措施主要包括：1)增加置乱操作，使算法进一步抵抗剪切、噪声污染及压缩的攻击；2)将原算法步骤 3)中式(5)的 m 值用前一步加密得到的密文像素值代替，使得密钥流与密文图像有关，从而达到“一次一密”的加密效果；3)为进一步提高系统的安全性并增加算法的复杂度，进行了必要的扩散、混淆操作。

参 考 文 献

[1] SHANNON C E. Communication theory of secrecy system[J]. Bell System Technical Journal，1949，28(11)：656-715.

[2] SCHIENER B. Applied cryptography：protocols，algorithms and source code in C [M]. New York：John Wiley and Sons，1996：30-40.

[3] BAPTISTA M S. Cryptography with chaos[J]. Physics Letters A，1998，240(1/2)：50-54.

[4] LIU H J，WANG X Y. Color image encryption based on one-time keys and robust chaotic maps[J]. Computers and Mathematics with Applications，2010，59(10)：3320-3327.

[5] WANG X Y，TENG L，QIN X. A novel colour image encryption algorithm based on chaos[J]. Signal Processing，2012，92(4)：1101-1108.

[6] HAN F Y，ZHU C X. New permutation-substitution image encryption scheme based on chaos[J]. Journal of Wuhan University(Natural Science Edition)，2014，60(5)：447-452. (in Chinese)
韩凤英，朱从旭. 新型置换和替代结构的图像混沌加密算法[J]. 武汉大学学报(理学版)，2014，60(5)：447-452.

[7] LIU Q，LI P Y，ZHANG M C，et al. Image encryption algorithm based on chaos system having markov portion[J]. Journal of Electronics & Information Technology，2014，36(6)：1271-1277. (in Chinese)
刘泉，李佩玥，章明朝，等. 基于可 Markov 分割混沌系 统的图像加密算法[J]. 电子与信息学报，2014，36(6)：1271-1277.

[8] LIU H J，WANG X Y. Color image encryption using spatial bit-level permutation and high-dimension chaotic system[J]. Optics Communications，2011，284(16/17)：3895-3903.

[9] LIU H J，WANG X Y. Image encryption using DNA complementary rule and chaotic maps[J]. Applied Soft Computing，2012，12(5)：1457-1466.

[10] ANCHAL J，NAVIN R. A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps[J]. Multimedia Tools Applications，2015，29(1)：1-18.

[11] HUANG X L，YE G D. An image encryption algorithm based on hyper-chaos and DNA sequence[J]. Multimedia Tools Applications，2014，72(1)：57-70.

[12] KUMAR M，IQBAL A，KUMAR P. A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography[J]. Signal Processing，2016，125(C)：187-202.

[13] AHMAD J，KHAN M A，HWANG S O，et al. A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices[J]. Neural Computing and Applications，2017，28(1)：953-967.

[14] WANG X Y，YANG L，LIU R，et al. A chaotic image encryption algorithm based on perceptron Model[J]. Nonlinear Dynamics，2010，62(3)：615-621.

[15] WILLIAM S，等. 密码编码学与网络安全：原理与实践[M]. 杨明，等译. 北京：电子工业出版社，2001：50-60.

[16] RHOUMA R，BELGHITH S. Cryptanalysis of a new image encryption algorithm based on hyper-chaos [J]. Physics Letters A，2008，372(38)：5973-5978.