基于高维矩阵变换的雪崩图像置乱变换

邵利平[1)] 覃 征[1),2)] 衡星辰[1)] 高洪江[1),3)] 王羡慧[1)]

[1)](西安交通大学电子与信息工程学院电子商务研究所, 西安 710049)

[2)](清华大学软件学院, 北京 100084) [3)](鲁东大学计算机科学与技术学院, 烟台 264025)

摘 要 传统的以高维 Arnold 变换和高维 Fibonacci-Q 变换为代表的基于高维矩阵变换的图像置乱方法,虽然具备较好的安全性,且能改变被置乱图像的灰度特征,但存在可恢复周期长,且对攻击不具备全局扩散能力等问题,在应用中存在缺陷。针对以上问题,基于高维矩阵变换,构造了雪崩图像置乱变换,该置乱变换可通过逆变换对图像进行置乱,通过正变换对置乱图像进行恢复,因而可减少由置乱图像恢复为原始图像的迭代次数,同时理论和实验结果表明该置乱变换在受到各种攻击时的强脆弱性,因而可用于数字作品完整性鉴别的脆弱水印构造。

关键词 图像置乱变换 图像加密 逆变换阵 雪崩效应 脆弱水印

中图法分类号:TP309.7 **文献标识码**:A **文章编号**:1006-8961(2008)08-1429-08

Avalanche Image Scrambling Transformation Based on High-dimension Matrix Transformation

SHAO Li-ping[1)], QIN Zheng[1),2)], HENG Xing-chen[1)], GAO Hong-jiang[1),3)], WANG Xian-hui[1)]

[1)](*Research Institute of Electronic Commerce, School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an* 710049)

[2)](*School of Software, Tsinghua University, Beijing* 100084)

[3)](*School of Computer Science and Technology, Ludong University, Yantai* 264025)

Abstract Classical image scrambling transformation based on high-dimension matrix transformation, which is represented by high-dimension Arnold transformation or high-dimension Fibonacci-Q transformation, is capable of preferable security and can change the gray characteristic of the scrambled image, however, there exists some deficiency in practice, such as the long restorable period and not having the full diffuse ability to attacks. To address these problems, in this paper, based on high-dimension matrix transformation, an avalanche image scrambling transformation is constructed, which scrambles the original image by inverse transformation and recovers the scrambled image by obverse transformation in order to cut down the iterative times from the scrambled image to the recovered image. Simultaneously, theory and experiments show its strong fragility under attacks and can be used to construct fragile watermarking to ensure digital productions integrality certification.

Keywords image scrambling transformation, image encryption, inverse matrix, avalanche effect, fragile watermarking

1 引 言

图像表达直观,蕴含信息量大,是认识和表达世界的基本方式[1]。随着计算机和网络技术的发展,越来越多的数字化图像信息在互联网中传播,使得图像信息的安全性尤为重要,在网络环境下,如何保障传输中图像信息的安全性,是信息安全领域的重要研究问题[2]。图像置乱变换是一类重要的图像加密方法,其主要目的是将图像搅乱,使人们无法通过人类视觉系统和计算机系统来发现原始图像所表达的真正含义。当前在空间域,置乱方法主要有:(1)基于 1 维序

基金项目:国家重点基础研究发展规划(973)基金项目(2004CB719401);教育部博士点基金项目(20060003060)

收稿日期:2006-10-30;**改回日期**:2007-03-21

第一作者简介:邵利平(1978~),男。西安交通大学电子与信息工程学院电子商务研究所博士研究生。感兴趣的研究领域有信息隐藏、数字水印、可视密码和 XML 数据检索等。E-mail:slpmaster@163.com

列搅乱的置乱方法,如 Fibonacci 变换[3~5]和 Lucas 变换[4];(2)基于 2 维仿射变换的置乱方法,如 2 维 Arnold 变换[1,6]、2 维 Fibonacci-Q 变换[7,8]和扩展的 2 维矩阵置乱变换[9~11];(3)基于位置迁移的置乱方法,如幻方变换[12,13]、魔方变换[14,15]、生命游戏[16,17]、骑士巡游、面包师[18]和 Hilbert 曲线[19~21]等;(4)基于单一像素灰度的置乱方法,如 3 维 Arnold 变换[7,22]、3 维 Fibonacci-Q 变换[7]和异或加密[23,24]等;(5)基于高维矩阵变换的置乱方法,如 n 维 Arnold 变换[7,25,26]、n 维 Fibonacci-Q 变换[7]和扩展的高维矩阵置乱变换[7]等。其中,基于 1 维序列搅乱的置乱方法,尽管具有加密解密简单,迭代周期短等特点,可用于实时加密场合,但置乱参数过于简单,安全性较低,对于 Fibonacci 变换和 Lucas 变换,其取值过于特殊,不具有一般性;基于 2 维仿射变换的置乱方法,对宽高不等的像素矩阵需扩展成方阵[6]或进行小方阵划分[27]才能进一步处理,在置乱过程中,不能改变像素的灰度分布特征;基于像素位置迁移的置乱方法在置乱过程中同样不能改变像素的灰度分布特征;基于单一像素灰度变换的置乱方法尽管可用于处理宽高不等的矩形图像,且能改变像素的灰度分布特征,但对置乱图像攻击不具备分散能力;基于高维矩阵变换的置乱方法,通常以图像像素矩阵的行或列为单位进行置乱,因而在置乱过程中,具备对像素所在行或列的分散能力,可改变像素的灰度特征,具备较好的安全性,但同时存在迭代周期过长,对攻击不具备全局扩散能力等缺点。

本文则在前人工作的基础上,对传统的基于高维矩阵变换的置乱方法加以改造,构造出了一类特殊的高维图像置乱变换,该置乱变换可通过逆变换对原始图像进行置乱,通过正变换对置乱图像进行恢复,因而可减少由置乱图像恢复为原始图像的迭代次数,同时理论和实验表明该变换在受到各种攻击时的强脆弱性,对置乱图像的任意微小攻击,都将导致受损置乱图像无法恢复为原始图像,因此将其称之为雪崩图像置乱变换。

2 基于高维矩阵变换的置乱方法

基于高维矩阵变换的置乱变换方法是将图像像素矩阵的行(列)映射为一个多维线性坐标,然后将线性坐标通过高维矩阵变换映射为另一个线性坐标,以此来对图像像素矩阵进行置乱。

定义 1 记变换 k 次的像素矩阵为 $(\boldsymbol{P}_{ij}^{k}=(r_{ij}^{k},g_{ij}^{k},b_{ij}^{k}))_{M\times N}$,变换阵为 $\boldsymbol{A}=(a_{ij})_{M\times M}$,变换后的像素矩阵为 $(\boldsymbol{P}_{ij}^{k+1}=(r_{ij}^{k+1},g_{ij}^{k+1},b_{ij}^{k+1}))_{M\times N}$,若 $(\boldsymbol{P}_{ij}^{k})_{M\times N}$ 映射为 $(\boldsymbol{P}_{ij}^{k+1})_{M\times N}$ 的变换满足下式

$$(\boldsymbol{p}_{ij}^{k+1})_{M\times N}\leftarrow(\boldsymbol{P}_{ij}^{k})_{M\times N}\begin{cases}(r_{ij}^{k+1})_{M\times N}=(a_{ij})_{M\times M}(r_{ij}^{k})_{M\times N} & \bmod 256\\ (g_{ij}^{k+1})_{M\times N}=(a_{ij})_{M\times M}(g_{ij}^{k})_{M\times N} & \bmod 256\\ (b_{ij}^{k+1})_{M\times N}=(a_{ij})_{M\times M}(b_{ij}^{k})_{M\times N} & \bmod 256\end{cases}\tag{1}$$

则称该变换为按列置乱的 M 维图像置乱变换,其中 k 为非负整数。

将式(1)简记为

$$(\boldsymbol{P}_{ij}^{k+1})_{M\times N}=(a_{ij})_{M\times M}(\boldsymbol{P}_{ij}^{k})_{M\times N}\bmod 256\tag{2}$$

定义 2 记变换阵为 $\boldsymbol{A}=(a_{ij})_{N\times N}$,若像素矩阵 $(\boldsymbol{P}_{ij}^{k})_{M\times N}$ 映射为 $(\boldsymbol{P}_{ij}^{k+1})_{M\times N}$ 的变换满足下式

$$(\boldsymbol{P}_{ij}^{k+1})_{M\times N}=(\boldsymbol{P}_{ij}^{k})_{M\times N}(a_{ij})_{N\times N}\bmod 256\tag{3}$$

则称该变换为按行置乱的 N 维图像置乱变换。

定理 1[7] 对于定义 1 和定义 2,若 $|\boldsymbol{A}|$ 和 256 互质,即 $Gcd(|\boldsymbol{A}|,256)=1$,则存在可恢复周期,其中 $Gcd()$ 是取最大公因子函数。

在定义 1 和定义 2 中,若变换阵为高维 Arnold 或高维 Fibonacci-Q 变换阵,则称对应的变换为高维 Arnold 置乱变换或高维 Fibonacci-Q 置乱变换。

从定义 1 和定义 2 可看出,基于高维矩阵变换的置乱变换方法虽然能将像素矩阵的行(列)进行搅乱,但只能以搅乱单位对像素灰度进行分散,对像素不具备全局分散能力。另外,在传统的基于矩阵变换的图像置乱技术中,利用最小可恢复周期 T 对置乱图像恢复起重要作用,文献[28]在此方面取得了进展,给出了一类 2 维随机整数变换阵 $\boldsymbol{A}$ 在任意模 N 下,周期 T 的精确表达式及上界估计。但在定义 1 和定义 2 中,由于变换阵的维数比较高,其最小可恢复周期通常情况下比较大。对于一个 n 维 Arnold 变换,其最小可恢复周期上界为 $1/2\times N^{n}$[27],在如此数量规模下,利用周期对置乱图像进行恢复,是不现实的。以下以剩余类集 $\boldsymbol{Z}_{256}$ 上 n 维 Arnold 变换和 n 维 Fibonacci-Q 变换

为例,给出具体的恢复周期如表 1 所示,其中 $n\in[15,20]$。从中可看出,基于高维矩阵变换的置乱变换由置乱图像正向恢复为原始图像的代价往往比较高昂。

表 1　Z_{256}上 Arnold 和 Fibonacci-Q 的周期

Tab.1　Periods of Arnold and Fibonacci-Q over Z_{256}

维数	Arnold 变换的周期	Fibonacci-Q 变换的周期
15	1 984	4 194 176
16	1 984	32 640
17	262 080	34 944
18	5 592 384	32 501 888
19	262 080	52 913 280
20	65 472	97 505 664

3　改进的高维雪崩图像置乱变换

3.1　雪崩图像置乱变换的正变换和逆变换

为解决基于高维矩阵变换的图像置乱变换存在的不足,对其进行了改进,得到了雪崩图像置乱变换,以下分别给出其正变换和逆变换。

定义 3　记变换阵为 $\boldsymbol{A}=(a_{ij})_{M\times M}$、$\boldsymbol{B}=(b_{ij})_{M\times M}$、$\boldsymbol{C}=(c_{ij})_{N\times N}$ 和 $\boldsymbol{D}=(d_{ij})_{N\times N}$。若像素矩阵 $(\boldsymbol{P}_{ij}^{k})_{M\times N}$ 映射为 $(\boldsymbol{P}_{ij}^{k+1})_{M\times N}$ 的变换满足式(4),则称该变换为雪崩图像置乱正变换。其中 $\boldsymbol{A}$ 阵和 $\boldsymbol{C}$ 阵为下三角阵,$\boldsymbol{B}$ 阵和 $\boldsymbol{D}$ 阵为上三角阵,满足的约束条件由式(5)~(8)分别给出。

$$(\boldsymbol{P}_{ij}^{k+1})_{M\times N}=\boldsymbol{AB}(\boldsymbol{P}_{ij}^{k})_{M\times N}\boldsymbol{CD}\bmod 256 \tag{4}$$

$$\boldsymbol{A}=(a_{ij})_{M\times M}\begin{cases} i\geqslant j & Gcd(a_{ij},256)=1,a_{ij}\in\{1,\cdots,255\}\\ \text{其他} & a_{ij}=0\end{cases} \tag{5}$$

$$\boldsymbol{B}=(b_{ij})_{M\times M}\begin{cases} i\leqslant j & Gcd(b_{ij},256)=1,b_{ij}\in\{1,\cdots,255\}\\ \text{其他} & b_{ij}=0\end{cases} \tag{6}$$

$$\boldsymbol{C}=(c_{ij})_{N\times N}\begin{cases} i\geqslant j & Gcd(c_{ij},256)=1,c_{ij}\in\{1,\cdots,255\}\\ \text{其他} & c_{ij}=0\end{cases} \tag{7}$$

$$\boldsymbol{D}=(d_{ij})_{N\times N}\begin{cases} i\leqslant j & Gcd(d_{ij},256)=1,d_{ij}\in\{1,\cdots,255\}\\ \text{其他} & d_{ij}=0\end{cases} \tag{8}$$

在定义 3 中,没有直接给出变换阵,而是通过 $\boldsymbol{A}$ 阵和 $\boldsymbol{B}$ 阵拼成 $M\times M$ 维左变换阵,通过 $\boldsymbol{C}$ 阵和 $\boldsymbol{D}$ 阵拼成 $N\times N$ 维右变换阵,这主要是基于 4 个原因:(1)直接通过计算机随机生成行列式不为 0 的高维变换阵的代价较为高昂;(2)生成满足定理 1 的高维变换阵,更加困难;(3)对高维变换阵直接在 $\boldsymbol{Z}_{256}$ 下,借助杜里特尔分解求整系数逆阵,其代价比较高昂;(4)直接生成满足定理 1 的下三角和上三角变换阵,代价较小;(5)由下三角阵和上三角阵分别在 $\boldsymbol{Z}_{256}$ 下求整系数逆阵则相对容易。在定义 3 中,上三角阵和下三角阵一旦生成,则可直接给出,但为了便于后续讨论,仍将其分为 4 个变换阵给出,在定义 4 中同样满足这个约定。

定义 4　记变换阵为 $\boldsymbol{A}'=(a'_{ij})_{M\times M}$、$\boldsymbol{B}'=(b'_{ij})_{M\times M}$、$\boldsymbol{C}'=(c'_{ij})_{N\times N}$ 和 $\boldsymbol{D}'=(d'_{ij})_{N\times N}$。若像素矩阵 $(\boldsymbol{P}_{ij}^{k})_{M\times N}$ 映射为 $(\boldsymbol{P}_{ij}^{k+1})_{M\times N}$ 的变换满足下式

$$(\boldsymbol{P}_{ij}^{k+1})_{M\times N}=\boldsymbol{B}'\boldsymbol{A}'(\boldsymbol{P}_{ij}^{k})_{M\times N}\boldsymbol{D}'\boldsymbol{C}' \tag{9}$$

则称该变换为雪崩图像置乱逆变换。其中,$\boldsymbol{A}'$ 阵和 $\boldsymbol{C}'$ 阵为下三角阵,$\boldsymbol{B}'$ 和 $\boldsymbol{D}'$ 阵为上三角阵,$\mathbf{I}$ 为单位阵,满足的约束条件为

$$\boldsymbol{A}'=(a'_{ij})_{M\times M}\begin{cases} i=j & a_{ij}a'_{ij}\bmod 256=1,a'_{ij}\in\{1,\cdots,255\}\\ i<j & a'_{ij}=0\\ \text{all} & \boldsymbol{AA}'\bmod 256=\mathbf{I}\end{cases} \tag{10}$$

$$\boldsymbol{B}'=(b'_{ij})_{M\times M}\begin{cases} i=j & b_{ij}b'_{ij}\bmod 256=1,b'_{ij}\in\{1,\cdots,255\}\\ i>j & b'_{ij}=0\\ \text{all} & \boldsymbol{BB}'\bmod 256=\mathbf{I}\end{cases} \tag{11}$$

$$\boldsymbol{C}'=(c'_{ij})_{N\times N}\begin{cases} i=j & c_{ij}c'_{ij}\bmod 256=1,c'_{ij}\in\{1,\cdots,255\}\\ i<j & c'_{ij}=0\\ \text{all} & \boldsymbol{CC}'\bmod 256=\mathbf{I}\end{cases} \tag{12}$$

$$\boldsymbol{D}'=(d'_{ij})_{N\times N}\begin{cases}i=j & d_{ij}d'_{ij}\bmod 256=1,d'_{ij}\in\{1,\cdots,255\}\\ i>j & d'_{ij}=0\\ \text{all} & \boldsymbol{DD}'\bmod 256=\boldsymbol{I}\end{cases}\tag{13}$$

定理 2 雪崩图像置乱正变换存在可恢复周期。

证明:由式(5)和式(6)知:

$$|\boldsymbol{A}|=\prod_{i=j\in[1,M]}a_{ij}\text{ 且 }Gcd(|\boldsymbol{A}|,256)=1\tag{14}$$

$$|\boldsymbol{B}|=\prod_{i=j\in[1,M]}b_{ij}\text{ 且 }Gcd(|\boldsymbol{B}|,256)=1\tag{15}$$

由式(14)和式(15)知:$Gcd(|\boldsymbol{AB}|,256)=1$

由定理 1 知,映射

$$(\boldsymbol{P}_{ij}^{k+1})_{M\times N}=\boldsymbol{AB}(\boldsymbol{P}_{ij}^{k})_{M\times N}\mod 256$$

存在着可恢复周期,同理,

$$(\boldsymbol{P}_{ij}^{k+1})_{M\times N}=(\boldsymbol{P}_{ij}^{k})_{M\times N}\boldsymbol{CD}\mod 256$$

存在着可恢复周期。

设两映射所对应的最小恢复周期分别为 T_1 和 T_2,记 $Lcm(T_1,T_2)$ 为 T_1 和 T_2 的最小公倍数,则有:

$$\boldsymbol{AB}(\boldsymbol{P}_{ij}^{Lcm(T_1,T_2)-1})_{M\times N}\boldsymbol{CD}\mod 256=((\boldsymbol{AB})^{Lcm(T_1,T_2)}(\boldsymbol{P}_{ij}^{0})_{M\times N})(\boldsymbol{CD})^{Lcm(T_1,T_2)}\mod 256=(\boldsymbol{P}_{ij}^{0})_{M\times N}$$

故原始像素矩阵得以恢复,故定理 2 得证。

定理 3 雪崩图像置乱逆变换存在可恢复周期。

证明:$a_{ii}a'_{ii}\bmod 256=1,i\in\{1,2,\cdots,M\}$ 且 $Gcd(a_{ii},256)=1$,则 $Gcd(a'_{ii},256)=1$。同定理 2 可证。

定理 4 定义 3 给出的正变换可被定义 4 给出的逆变换恢复,反之亦然。

证明:略

3.2 变换阵和逆变换阵生成算法

在定义 3 和定义 4 中,涉及到了上三角阵和下三角阵,以及对应的变换阵在 $\boldsymbol{Z}_{256}$ 上的逆变换阵。其中,下三角阵生成算法如下:

算法 1 下三角变换阵(***A*** 阵和 ***C*** 阵)生成算法

输入:N

输出:$N\times N$ 维下三角阵 $(a_{ij})_{N\times N}$

伪码:

```
rand_initial(key)
for i:=1 to N do
  for j:=1 to N do
    if i≥j then
      r:=random(255)+1
      while Gcd(r,256)≠1 do
        r:=random(255)+1
      a_ij:=r
    else
      a_ij:=0
```

随机数由线形同余法产生,用以保证伪随机数的均匀分布。

在算法 1 中伪码第 1 行初始化伪随机数序列;伪码 5 至 8 行保证生成下三角变换阵主对角线和主对角线以下元素和 256 互质,且为介于 1 到 255 之间的整数,这里除了按最大公约数为 1 进行判别,也可根据奇偶性进行判别。若将算法 1 中,伪码第 4 行由“$i\geqslant j$”修改为“$i\leqslant j$”,则为上三角阵生成算法。

对于算法 1 生成的下三角阵,可按算法 2 对其在 $\boldsymbol{Z}_{256}$ 下求逆。

算法 2 下三角阵的逆阵(***A***′阵和 ***C***′阵)生成算法

输入:下三角阵 $(a_{ij})_{N\times N}$

输出:下三角阵 $(a_{ij})_{N\times N}$ 在 $\boldsymbol{Z}_{256}$ 下的逆变换阵 $(a'_{ij})_{N\times N}$

伪码:

```
for j:=1 to N
  for i:=1 to N
    if j=i then
      k1:=0
      temp1:=floor((k1×256+1)÷a_ij)//floor()表示
             向下取整
      while temp1×a_ij≠k1×256+1 do
      k1:=k1+1
      temp1:=floor((k1×256+1)÷a_ij)
      a'_ij:=temp1 mod 256
    else if i>j then
      temp2:=0
      for k2:=j to i-1 do
        temp2:=temp2+a_ik2×a'_k2j
      k3:=0
      temp3:=temp2+k3×a_ii
      while temp3 mod 256≠0 do
        k3:=k3+1
        temp3:=temp2+k3×a_ii
      a'_ij:=k3 mod 256
        else
      a'_ij:=0
```

在算法 2 中,伪码第 3 至 9 行用递增法求取主对角线元素 $a_{ii}(i\in\{1,\cdots,N\})$ 在 Z_{256} 上的乘法逆元;第 10 至 19 行,用递增法求主对角线以下元素 a'_{ij},对于元素 a'_{ij},在求解过程中所需要的元素 a'_{kj},$k\in[j,i-1]$ 在按先列序后行序的计算中可得到,

而 $a_{ik}, k \in [j,i]$ 则由正变换阵给出。伪码 20 至 21 行,直接对主对角线以上元素赋 0。利用类似的方法,可得到上三角阵在 $\boldsymbol{Z}_{256}$ 上的求逆算法,这里不再给出。

以下给出由本文算法生成的正变换阵和逆变换阵,和在 $\boldsymbol{Z}_{256}$ 上矩阵相乘的实验结果,其中矩阵元素记录在对应的像素矩阵中,如图 1 所示。

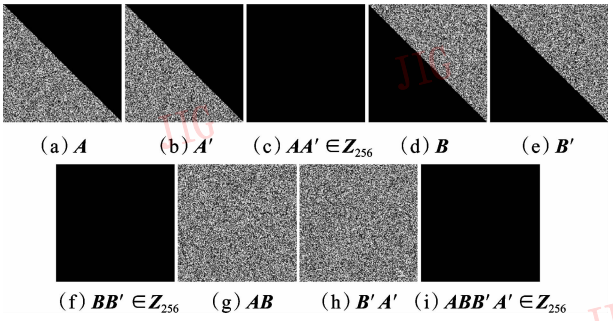


图 1　生成矩阵和运算结果

Fig. 1　Generated matrices and results of matrix operation

3.3　雪崩图像置乱变换的雪崩效应分析

雪崩在传统密码学中是指明文或密钥的微小改变能引起密文的很大改变,并导致密文的不可恢复性。在本文中,将其作为置乱扩散性能的一项重要特征,在本小节和后面的实验中,将可以看到,所提方法对攻击的强敏感性,对置乱图像的任意微小攻击,都将导致原始图像的彻底不可恢复。

定义 5　设模 Q 下的一个整数 X,若对其引入一个整数偏差 Δ,且 $\Delta \in [1,Q) \cup (-Q,-1]$,将模 Q 下的整数 X 修改为 X',即 $X' \leftarrow (X+\Delta) \mod Q$,则称 Δ 为模 Q 下的误差量。

定理 5　若 $Gcd(L,Q)=1$,则 $L\Delta \mod Q$ 仍为模 Q 下的一个误差量。

证明:用反证法。设 $\exists l_1 \in L$ 且 l_1 且 $Gcd(l_1,Q)=1$ 且 $l_1\Delta \mod Q=0$,则由 $Gcd(l_1,Q)=1$ 且 $l_1\Delta \mod Q=0$,有 $\Delta \mod Q=0$,而 $\Delta \in [1,Q) \cup (-Q,-1]$,则推出矛盾,故定理 5 得证。

定理 6　若 $L \mod Q=0$,则 $L\Delta \mod Q$ 不是模 Q 下的误差量。

证明:由定义 5 可证。

定理 7　若 Δ_1 和 Δ_2 为模 Q 误差量,则 $(\Delta_1+\Delta_2) \mod Q$ 仍近似看作误差量,其中 $Q>100$。

证明:这里按古典概型估计误差量的概率。

若 $\Delta_1+\Delta_2=0$,则需满足:

(1)若 $\Delta_1>0$,则 $(\Delta_2=-\Delta_1)$ 或 $(\Delta_2=Q-\Delta_1)$

(2)若 $\Delta_1<0$,则 $(\Delta_2=-\Delta_1)$ 或 $(\Delta_2=-Q-\Delta_1)$

由(1)和(2)可估计:

$$P(\Delta_1>0)=(Q-1)/2(Q-1)=1/2$$

$$P(\Delta_1<0)=(Q-1)/2(Q-1)=1/2$$

$$P((\Delta_1+\Delta_2) \bmod Q=0 \mid \Delta_1>0)=2/2(Q-1)=1/(Q-1)$$

$$P((\Delta_1+\Delta_2) \bmod Q=0 \mid \Delta_1<0)=2/2(Q-1)=1/(Q-1)$$

$$P((\Delta_1+\Delta_2) \bmod Q=0)=P((\Delta_1+\Delta_2) \bmod Q=0 \mid \Delta_1>0)\cdot P(\Delta_1>0)+P((\Delta_1+\Delta_2) \bmod Q=0 \mid \Delta_1<0)\cdot P(\Delta_1<0)=1/(Q-1)$$

当 $Q>100$,$(\Delta_1+\Delta_2) \mod Q$ 不为误差量的概率最大仅为 0.01,故定理 7 成立。

定理 8　设 $\Delta_1,\Delta_2,\cdots,\Delta_n$ 为模 Q 误差量,则 $\sum_{i=1}^{n}\Delta_i \mod N$ 仍近似看作误差量,其中 $Q>100$。

证明:由定理 7 类似的方法可证。

对于误差量,只考虑影响,不考虑其大小,若其引起新的误差量,则将该误差量仍记为 Δ。

以下对雪崩效应作简单分析。设在 P_{ij} 处引入模 256 下的误差量 Δ 的像素矩阵为 $(\boldsymbol{P}_{ij}^{O})_{M\times N}$,记中间过程产生的矩阵为

$$(\boldsymbol{P}_{ij}^{B})_{M\times N}=(\boldsymbol{B}(\boldsymbol{P}_{ij}^{O})_{M\times N}) \mod 256$$

$$(\boldsymbol{P}_{ij}^{BA})_{M\times N}=(\boldsymbol{A}(\boldsymbol{P}_{ij}^{B})_{M\times N}) \mod 256$$

$$(\boldsymbol{P}_{ij}^{BAC})_{M\times N}=((\boldsymbol{P}_{ij}^{BA})_{M\times N}\boldsymbol{C}) \mod 256$$

$$(\boldsymbol{P}_{ij}^{BACD})_{M\times N}=((\boldsymbol{P}_{ij}^{BAC})_{M\times N}\boldsymbol{D}) \mod 256$$

则由定理 5、定理 6 和定理 8 知:

$$(\boldsymbol{P}_{ij}^{B})_{M\times N}=\begin{bmatrix} \boldsymbol{P}_{11}^{B} & \cdots & \boldsymbol{P}_{1j}^{B}+\Delta & \cdots & \boldsymbol{P}_{1N}^{B} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \boldsymbol{P}_{i1}^{B} & \cdots & \boldsymbol{P}_{ij}^{B}+\Delta & \cdots & \boldsymbol{P}_{iN}^{B} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \boldsymbol{P}_{M1}^{B} & \cdots & \boldsymbol{P}_{Mj}^{B} & \cdots & \boldsymbol{P}_{MN}^{B} \end{bmatrix} \tag{16}$$

$$(\boldsymbol{P}_{ij}^{BA})_{M\times N}=\begin{bmatrix} \boldsymbol{P}_{11}^{BA} & \cdots & \boldsymbol{P}_{1j}^{BA}+\Delta & \cdots & \boldsymbol{P}_{1N}^{BA} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \boldsymbol{P}_{i1}^{BA} & \cdots & \boldsymbol{P}_{ij}^{BA}+\Delta & \cdots & \boldsymbol{P}_{iN}^{BA} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \boldsymbol{P}_{M1}^{BA} & \cdots & \boldsymbol{P}_{Mj}^{BA}+\Delta & \cdots & \boldsymbol{P}_{MN}^{BA} \end{bmatrix} \tag{17}$$

$$(\boldsymbol{P}_{ij}^{BAC})_{M\times N}=\begin{bmatrix}\boldsymbol{P}_{11}^{BAC}+\Delta & \cdots & \boldsymbol{P}_{1j}^{BAC}+\Delta & \cdots & \boldsymbol{P}_{1N}^{BAC}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ \boldsymbol{P}_{i1}^{BAC}+\Delta & \cdots & \boldsymbol{P}_{ij}^{BAC}+\Delta & \cdots & \boldsymbol{P}_{iN}^{BAC}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ \boldsymbol{P}_{M1}^{BAC}+\Delta & \cdots & \boldsymbol{P}_{Mj}^{BAC}+\Delta & \cdots & \boldsymbol{P}_{MN}^{BAC}\end{bmatrix} \tag{18}$$

$$(\boldsymbol{P}_{ij}^{BACD})_{M\times N}=\begin{bmatrix}\boldsymbol{P}_{11}^{BACD}+\Delta & \cdots & \boldsymbol{P}_{1j}^{BACD}+\Delta & \cdots & \boldsymbol{P}_{1N}^{BACD}+\Delta\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ \boldsymbol{P}_{i1}^{BACD}+\Delta & \cdots & \boldsymbol{P}_{ij}^{BACD}+\Delta & \cdots & \boldsymbol{P}_{iN}^{BACD}+\Delta\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ \boldsymbol{P}_{M1}^{BACD}+\Delta & \cdots & \boldsymbol{P}_{Mj}^{BACD}+\Delta & \cdots & \boldsymbol{P}_{MN}^{BACD}+\Delta\end{bmatrix} \tag{19}$$

由式(19)知，$(\boldsymbol{P}_{ij}^{0})_{M\times N}$ 在 $\boldsymbol{P}_{ij}$ 处引入的误差量 Δ，经过 $\boldsymbol{B}$、$\boldsymbol{A}$、$\boldsymbol{C}$ 和 $\boldsymbol{D}$ 阵变换后，将散布到变换后的像素矩阵的每一个元素上，由此可知定义 3 所给出的正变换经一次变换即可将引入的误差量，遍布到像素矩阵的每一个像素上，从而具有强雪崩效应。在此基础上，将置乱变换迭代 $k(k>1$ 且 $k\ll T)$ 次，则每次置乱系数的微小误差，都将在像素矩阵中引入新的误差，从而导致整个像素矩阵的雪崩效应，因此所构造的置乱方法具有高安全性。

4 实 验

4.1 实验评价标准

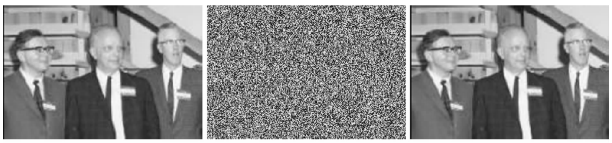
在实验中，用峰值信噪比(PSNR)衡量攻击前后置乱图像相似程度和攻击后置乱图像恢复图像的相似程度，其中 $(\boldsymbol{P}_{ij}^{0}=(r_{ij}^{0},g_{ij}^{0},b_{ij}^{0}))_{M\times N}$ 为攻击前的置乱图像或由置乱图像恢复的图像，$(\boldsymbol{P}_{ij}^{1}=(r_{ij}^{1},g_{ij}^{1},b_{ij}^{1}))_{M\times N}$ 为攻击后的置乱图像或攻击后置乱图像恢复图像。

$$\mathrm{PSNR_r}=10\lg\left|\frac{MN\cdot 255^2}{\sum_{i=1}^{M-1}\sum_{j=1}^{N-1}(r_{ij}^{0}-r_{ij}^{1})^2}\right| \tag{20}$$

$$\mathrm{PSNR}=\frac{(\mathrm{PSNR_r}+\mathrm{PSNR_g}+\mathrm{PSNR_b})}{3} \tag{21}$$

4.2 雪崩效应测试

以初始密钥 1，生成变换阵和逆变换阵。使用的测试图像(图 2)，由逆变换 1 次迭代的图像如图2(b)所示，由正变换 1 次迭代恢复的图像如图2(c)所示，攻击参数如表 2 所示，攻击图像如图 3 所示，正变换恢复图像如图 4 所示。



(a) 176×260 (b) 置乱图像 (c) 恢复图像

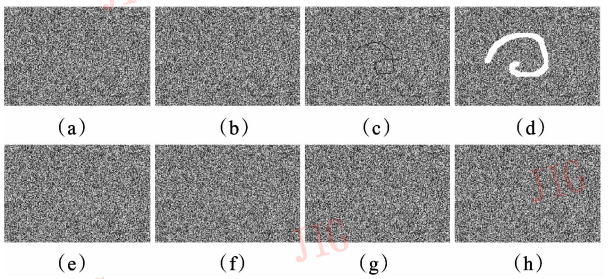
图 2 实验图样

Fig. 2 Experimental images

表 2 置乱攻击图像和恢复图像的实验数据

Tab. 2 Experimental data of attacked scrambled and recovered images

攻击方法	攻击参数	攻击图样(图 3)	恢复图样(图 4)	置乱 PSNR	恢复 PSNR
清最低位	(100,23)	a	a	91.203 8	5.022 5
清最低位	(167,18)	b	b	91.203 8	5.056 4
随机划线	—	c	c	24.270 6	5.083 1
随机擦除	—	d	d	13.915 9	5.036 6
随机噪声	1000 个	e	e	20.964 6	5.070 0
随机噪声	1000 个	f	f	14.154 8	5.068 7
有损压缩	质量 99	g	g	50.910 0	5.074 1
有损压缩	质量 98	h	h	46.232 1	5.040 0

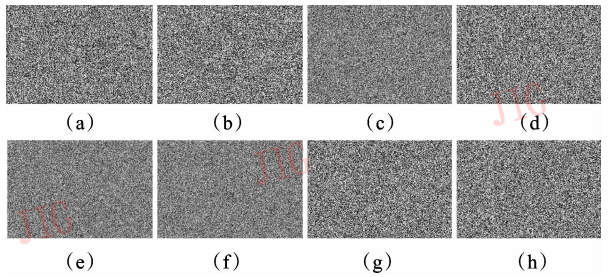


(a) (b) (c) (d)

(e) (f) (g) (h)

图 3 置乱图像的攻击图样

Fig. 3 Attacked images of the scrambled images



(a) (b) (c) (d)

(e) (f) (g) (h)

图 4 由攻击图样恢复的置乱图像

Fig. 4 Recovered images of the scrambled images

从实验结果可看出，对置乱图像的任意微小攻击都将导致受损置乱图像无法恢复为原始图像，因而所构造的置乱变换具有强雪崩效应。

4.3　扩散性能对比测试

将本文方法同 3 维 Arnold 变换、3 维Fibonacci-Q 变换、简单异或操作、高维 Arnold 变换和高维 Fibonacci-Q 变换相比较,实验参数如表 3 所示,置乱图像攻击图样如图 5,恢复图样如图 6。

表 3　被剪切的置乱图像和恢复图像

Tab. 3　Cropped images and recovered images

置乱方法	T	受损图像		恢复图像	
		迭代次数	图像(图 5)	迭代次数	图像(图 6)
Arnold-3	448	300	a	148	a
Fibonacci-Q-3	896	300	b	596	b
XOR	2	1	c	1	c
Arnold-176	—	300	d	-300	d
Fibonacci-Q-176	—	300	e	-300	e
Arnold-260	—	300	f	-300	f
Fibonacci-Q-260	—	300	g	-300	g
雪崩置乱变换	—	1	h	-1	h

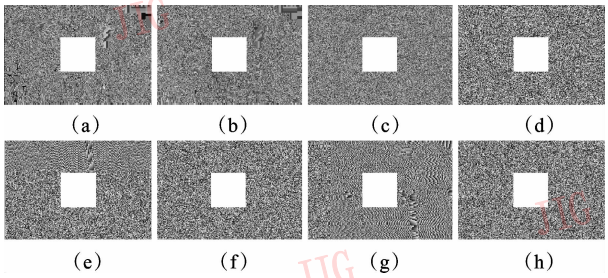


图 5　置乱图像的攻击图样

Fig. 5　Attacked images of the scrambled images

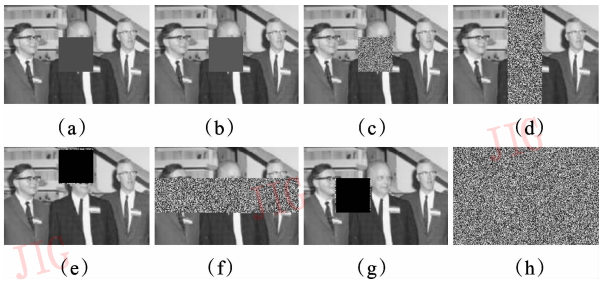


图 6　由攻击图样恢复的置乱图像

Fig. 6　Recovered images of the scrambled images

从实验结果可看出,本文方法具有全局扩散能力,其扩散能力优于所比较的方法。这里需指出的是,基于 2 维仿射变换的置乱方法和基于位置迁移的置乱方法也具备对攻击的全局分散能力,但是这类方法是将各种攻击分散均匀,从而保证恢复图像的健壮性。而本文所构造的方法,是将攻击扩散在每个像素上面,强化其脆弱性,从而使任意微小攻击,都将导致攻击图像的不可恢复性,从而可用于数字作品完整性鉴别的脆弱水印构造。

5　结　论

基于高维矩阵变换的雪崩图像置乱变换方法,通过逆变换对图像置乱,通过正变换对图像恢复,避免了对置乱图像正向迭代恢复的高昂代价,降低了迭代次数,使得置乱和恢复可在较少的迭代次数下完成;通过上三角阵和下三角阵分别在 $\boldsymbol{Z}_{256}$ 下分别求逆取代高维矩阵在 $\boldsymbol{Z}_{256}$ 下直接求逆,使得在不降低安全性的情况下,避免了在 $\boldsymbol{Z}_{256}$ 下求逆的高昂代价;所构造的雪崩图像置乱变换具有全局扩散能力;对置乱图像像素矩阵任意微小攻击,都将扩展到整个图像像素矩阵元素上,导致整个图像的不可恢复性;所构造的变换阵维数和图像像素矩阵的高度和宽度分别相等,可将其加密后,分给不同人员进行管理,其安全性近似为密码学中的一次密钥体系,因而所提方法具有安全性。同时实验结果表明本文所构造的雪崩图像置乱变换,可在较少的迭代次数下,具有较好的全局扩散能力,对微小攻击的强敏感性,从而可用于数字作品的完整性鉴别的脆弱水印构造。

参考文献(References)

1　Ding Wei, Yan Wei-qi, Qi Dong-xu. Digital image scrambling technology based on Arnold transformation[J]. Journal of Computer Aided Design and Computer Graphics, 2001, **13**(4):338 ~ 441. [丁玮,闫伟齐,齐东旭. 基于 Arnold 变换的数字图像置乱技术[J]. 计算机辅助设计与图形学学报,2001,**13**(4): 338 ~ 341.]

2　Ding Wei, Yan Wei-qi, Qi Dong-xu. Digital image scrambling[J]. Progress in Natural Science, 2001, **11**(6): 454 ~ 460.

3　Zou Jian-cheng, Ward Rabab K, Qi Dong-xu. A new digital image scrambling method based on Fibonacci numbers[A]. In: Proceeding of the IEEE Inter Symposium on Circuits and Systems [C], Vancouver, Ganada, 2004:965 ~ 968.

4　Zou Jian-cheng, Ward Rabab K, Qi Dong-xu. The generalized Fibonacci transformations and application to image scrambling[A]. In: Proceedings of the IEEE International conference on Acoustic, speech and signal processing[C], Montreal, Canada, 2004:385 ~ 388.

5　Zou Jian-cheng, Qi Dong-xu, Ward Rabab K. A novel watermarking method based on Fibonacci numbers [A]. In: International Conference on Virtual Reality Continuum and Its Applications[C], Hongkong, China, 2006:335 ~ 338.

6　Kong Tao, Zhang Dan. A new anti-Arnold transformation algorithm [J]. Journal of Software, 2004, **15**(10): 1558 ~ 1564. [孔涛,张亶. Arnold 反变换的一种新算法[J]. 软件学报,2004,**15**(10):

1558 ~ 1564.]

7 Qi Dong-xu, Zou Jian-cheng, Han Xiao-you. A new class of transformation and its application in the image transformation covering [J]. Science in China(Series E),2000,**43**(3):304 ~ 312.

8 Yin De-hui, Li Bing-fa. Using improved Fibonacci hash transform to increase the robustness of meaningful watermarking algorithm[J]. Journal of Wuhan University of Science and Technology (Natural Science Edition), 2005, **26**(7): 1241 ~ 1245. [尹德辉,李柄法. 一种基于改进的 Fibonacci 变换的数字水印算法[J]. 武汉科技大学学报(自然科学版),2005,**26**(7):1241 ~ 1245.]

9 Zhu Cong-xu, Chen Zhi-gang. Novel binary image digital watermarking algorithm based on DWT and chaotic scrambling[J]. Mini-micro Systems, 2005, **26**(7): 1241 ~ 1245. [朱从旭,陈志刚. 基于 DWT 域的混沌置乱二值图像数字水印新算法[J]. 小型微型计算机系统,2005,**26**(7):1241 ~ 1245.]

10 Ma Zai-guang, Qiu Shui-sheng. An image cryptosystem based on general cat map[J]. Journal of China Institute of Communications, 2003, **24**(2):51 ~ 57. [马在光,丘水生. 基于广义猫映射的一种图像加密系统[J]. 通信学报,2003,**24**(2):51 ~ 57.]

11 Zhang Xian-hai, Yang Yong-tian, Zhu Yan. A secure hierarchical fragile watermarking method with tamper localization[A]. In: The International Multi-Symposiums on Computer and Computational Sciences[C], Hangzhou, China, 2006:69 ~ 74.

12 Wang Dong-mei. The quasi-period of odd order magic square transformation on digital image[J]. Journal of Zhejiang University of Technology, 2005, **33**(3): 292 ~ 294. [王冬梅. 奇数阶幻方变换数字图像的准周期[J]. 浙江工业大学学报,2005,**33**(3): 292 ~ 294.]

13 Wang Dong-mei, Jin Yi-qing. Semi-period of doubly even order magic square transformed digital image[J]. Journal of Zhejiang University(Sciences Edition), 2005, **32**(3):274 ~ 276. [王冬梅,金一庆. 双偶阶幻方变换数字图像的半周期[J]. 浙江大学学报(理学版),2005,**32**(3):274 ~ 276.]

14 Shen Jian-bing, Jin Xiao-gang, Zhou Chuan. A color image encryption algorithm based on Magic cube transformation and modular arithmetic operation[A]. In:Proceedings of 6th Pacific Rim Conference on Multimedia[C], Jeju Island, Korea,2005:270 ~ 280.

15 Zhang Li, Ji Shi-ming, Xie Yi, *et al*. Principle of image encrypting algorithm based on Magic cube transformation[A]. In:proceedings of Computational Intelligence and Security[C], Xi'an, China, 2005:977 ~ 982.

16 Dai Kan-fei, Huang Wen-long, Chen Zhen-yong, *et al*. An MPEG-4 motion vector watermarking scheme based on scrambling using game of life [J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2004, **43**(s2): 192 ~ 195. [戴侃斐,黄文勇,陈真勇等. 基于生命游戏置乱的 MEPG-4 运动矢量水印算法[J]. 中山大学学报(自然科学版),2004,**43**(s2):192 ~ 195.]

17 Ding Wei, Yan Wei-qi, Qi Dong-xu. Digital image scrambling and digital watermarking technology based on Conway's game [J]. Journal of North China University of technology, 2000, **12**(1): 1 ~ 5. [丁玮,闫伟齐,齐东旭. 基于生命游戏的数字图像置乱与数字水印技术[J]. 北方工业大学学报,2000,**12**(1):1 ~ 5.]

18 Han Feng-jing, Hu Jian-kun, Yu Xing-huo. A biometric encryption approach incorporating fingerprint indexing in key generation[A]. In: Proceedings of International Conference on Biometrics [C], Kunming, China, 2006:675 ~ 681.

19 Qi Dong-xu. Matrix transformation and its applications to image hiding[J]. Journal of North China University of Technology, 1999, **11**(1):24 ~ 28. [齐东旭. 矩阵变换及其在图像隐藏中的应用研究[J]. 北方工业大学学报,1999,**11**(1):24 ~ 28.]

20 Ding Wei, QI Dong-xu. Digital image transformation and information hiding and disguising technology [J]. Chinese Journal of Computers, 1998, **21**(9): 838 ~ 843. [丁玮,齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报,1998,**21**(9): 838 ~ 843.]

21 Lin Xue-hui, Cai Li-dong. Scrambling research of digital image based on Hilbert curve[J]. Chinese Journal of Stereology and Image Analysis, 2004, **9**(4): 224 ~ 227. [林雪辉,蔡利栋. 基于 Hilbert 曲线的数字图像置乱方法研究[J]. 中国体视学与图像分析,2004,**9**(4):224 ~ 227.]

22 Hong Chun-Yong, Zou Wei-gang. Digital image scrambling technology based on three dimension Arnold transformation and its periodicity[J]. Journal of Nanchang University(Natural Science), 2005, **29**(6): 619 ~ 621. [洪春勇,邹玮刚. 基于三维 Arnold 变换的数字图像置乱技术及其周期性[J]. 南昌大学学报(理科版),2005,**29**(6):619 ~ 621.]

23 Huang Shi, Ren Jun, Guo Wen-pu. Research on image chaos arithmetic based on gray transforming [J]. Microcomputer Development, 2003, **13**(11): 123 ~ 124. [黄石,任俊,郭文普. 基于灰度变换的图像置乱算法研究[J]. 微机发展,2003,**13**(11): 123 ~ 124.]

24 Sun Yu-feng, Chen Jian-hua. A novel image scrambling method based on the model of the law of gravity [J]. Journal of Fuzhou University (Natural Science Edition), 2006, **34**(1): 47 ~ 50. [孙玉峰,陈建华. 一种基于万有引力模型的图像置乱新方法[J]. 福州大学学报,2006,**34**(1):47 ~ 50.]

25 Zao Hui. Arnold transformation of *N* dimensions and its periodicity [J]. Journal of North China University of Technology, 2002, **14**(1):21 ~ 24. [赵慧. *N* 维 Arnold 变换及其周期性[J]. 北方工业大学学报, 2002,**14**(1):21 ~ 24.]

26 Li Zi-rong, Guo Jun-ping, Xu Ri-zhou, *et al*. Study on multidimensional digital image scrambling [J]. Aero Weaponry, 2005, (2): 22 ~ 25. [李自荣,郭军平,徐日洲等. 高维数字图像置乱技术研究[J]. 航空兵器,2005,(2):22 ~ 25.]

27 Yang Ya-li, Caina, Ni Guo-qiang. Digital image scrambling technology based on the symmetry of Arnold transform[J]. Journal of Beijing Institute of Technology,2006,**15**(2):216 ~ 220.

28 Wang Ze-hui. On the peiod of 2D random matrix scrambling transformation and its applications in image information hiding[J]. Chinese Journal of Computers,2006,**29**(12):2218 ~ 2224. [王泽辉. 二维随机矩阵置乱变换的周期及在图像信息隐藏中的应用[J]. 计算机学报,2006,**29**(12): 2218 ~ 2224.]