纯位置置乱变换的破解算法*

赵一鸣[1], 赵晓宇[2+], 龚松春[1]

[1](宁波大学 信息学院计算机系,浙江 宁波 315211)

[2](宁波大学 数字技术和应用软件研究所,浙江 宁波 315211)

Decryption of Scramble Algorithms

ZHAO Yi-Ming[1], ZHAO Xiao-Yu[2+], GONG Song-Chun[1]

[1](Department of Computer Science and Technology, Ningbo University, Ningbo 315211, China)

[2](Institute of DSP and Software Techniques, Ningbo University, Ningbo 315211, China)

+ Corresponding author: Phn: +86-547-87600948, E-mail: zhaoxiaoyu@nbu.edu.cn, http://www.nbu-eied.net/DSP/~Zhaoxiaoyu/

Received 2004-06-30; Accepted 2004-08-09

Zhao YM, Zhao XY, Gong SC. Decryption of scramble algorithms. *Journal of Software*, 2004,15(Suppl.): 149~156.

Abstract: Scramble algorithms, which are also called pure-position permutation algorithms, are commonly used as an image encryption, are investigated in this paper. Unfortunately, they are frail under known-text attack. According to the weakness of pure position permutation algorithm, we put forward an effective decryption algorithm for all pure-position permutation algorithms. First, a summary of the pure position permutation image encryption algorithms is given by introducing the concept of ergodic matrices. Secondly, by using probability theory and algebra knowledge, the decryption probability of pure-position permutation algorithms is verified theoretically. Then, by defining operation system of fuzzy ergodic matrices, we improve a specific decryption algorithm. Finally, some simulation results are shown.

Key words: decryption; scramble; image encryption; fuzzy

摘 要: 置乱算法,即纯位置移动算法简单、速度快,目前在图像和多媒体流加密中被广泛使用.但是,其在已知明文的攻击下是脆弱的.通过分析纯位置加密算法的这一弱点,给出了一种有效的破解算法.首先,通过引入遍历矩阵,将所有的纯位置移动算法统一在同一框架中;其次,利用概率统计和代数学的有关知识,从理论上验证了其破解概率;然后,通过定义模糊遍历矩阵和其相关的求交、清晰化等运算,成功的给出了一种非常有效的破解算法.最后,通过编程试验,证实该破解算法的效果令人非常满意.

关键词: 破解;置乱;图像加密;模糊

随着通讯科技的发展,信息安全成为日益重要的一个课题.多媒体技术的广泛使用及网络传输能力提高,使

* Supported by the National Natural Science Foundation of China under Grant No.60302012 (国家自然科学基金); the National Research Foundation of Higher Education of Zhejiang Province under Grant No.20030502 (浙江省教育厅基金)

作者简介: 赵一鸣(1958-),男,陕西榆林人,硕士,副教授,主要研究领域为计算智能,虚拟现实,图像处理;赵晓宇(1978-),男,硕士,助教,主要研究领域为图像处理,信息安全;龚松春(1980-),男,主要研究领域为计算机网络,图像处理.

得人们能够通过图像方式直观、清晰地获取信息,从而对图像数据传输过程中的安全性有了进一步要求.对图像数据的加密,国内外已有众多学者对此作了研究[1~8].

按照基本概念可将其分为三类:位置置换,数值转换和组合形式.位置置换,如:Zig-Zag、Arnold、幻方变换等算法,仅仅通过移动原始图像 I 中的各个像素的位置来得到加密的效果.在文献[3]中,我们引入了遍历矩阵的概念,并运用它来统一表示基于像素移动基础上的置乱算法.然而,这些纯位置置乱算法存在潜在的弱点,它们在已知明文条件的攻击下表现脆弱.

显然,只要将加密前和加密后的图像像素位置作对比,则容易发现其像素位置变换的规律,但是,因为图像不同点的灰度值存在相同的情况,并且这种重复的概率越大,破解就变得愈发困难.针对纯位置置乱算法的弱点,我们提出了破解算法,通过比较原始图像和加密图像,来恢复相应的算法.

1 纯位置算法综述

纯位置置乱算法简单并且速度快,被广泛的应用于许多图像加密系统.我们通过引入遍历矩阵的概念[3],将所有的纯位置置乱限定在一个统一的框架和相应的运算法则,从而有利于我们运用简单的方式实现相关的置乱.因而,我们可以知道,任何位置置乱算法,都可以通过遍历矩阵来表示.

我们首先考虑灰度图像,原始图像记为 I,加密图像记为 E,从而有:

$$I=\begin{bmatrix} I_{11} & I_{12} & \cdots & I_{1n} \\ I_{21} & I_{22} & \cdots & I_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ I_{m1} & I_{m2} & \cdots & I_{mn} \end{bmatrix}, E=\begin{bmatrix} E_{11} & E_{12} & \cdots & E_{1n} \\ E_{21} & E_{22} & \cdots & E_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ E_{m1} & E_{m2} & \cdots & E_{mn} \end{bmatrix}$$

1.1 将所有的纯位置置乱统一于一个框架内

1.1.1 遍历矩阵

对 $m\times n$ 的矩阵 R,如果其中的元素取值自 $\{1,2,\cdots,mn\}$,而且 $r(i,j)=r(i',j')$,当且仅当 $i=i'$, $j=j'$,我们称 R 为遍历矩阵.我们记 $r_{(i-1)n+j}=r(i,j)$.

我们称形如

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ n+1 & n+2 & n+3 & \cdots & 2n \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (m-1)n+1 & (m-1)n+2 & (m-1)n+3 & \cdots & mn \end{pmatrix}_{m\times n}$$

的矩阵为行遍历或基本遍历矩阵.

1.1.2 利用遍历矩阵实现变换

我们可以遍历矩阵来快速实现图像像素位置移动的置乱变换.

例如,对一个图像数据矩阵,我们按照遍历矩阵 $R_{m\times n}$ 所表示的遍历方式来对它进行遍历,并将得到的数据一行行排列下来,则完成了对图像数据的位置置乱.

例:

$$I_{4\times4}=\begin{bmatrix} I_{11} & I_{12} & I_{13} & I_{14} \\ I_{21} & I_{22} & I_{23} & I_{24} \\ I_{31} & I_{32} & I_{33} & I_{34} \\ I_{41} & I_{42} & I_{43} & I_{44} \end{bmatrix}_{4\times4} \longleftrightarrow R=\begin{bmatrix} 7 & 2 & 10 & 3 \\ 15 & 1 & 9 & 11 \\ 4 & 6 & 8 & 13 \\ 14 & 12 & 16 & 5 \end{bmatrix} \longrightarrow \begin{bmatrix} I_{22} & I_{12} & I_{14} & I_{31} \\ I_{44} & I_{32} & I_{11} & I_{33} \\ I_{23} & I_{13} & I_{24} & I_{42} \\ I_{34} & I_{41} & I_{21} & I_{43} \end{bmatrix}_{4\times4}$$

1.2 纯位置置乱变换的弱点和破解算法的基本构想

我们知道,任何位置置乱算法,都以通过遍历矩阵来表示[3].而破解一个置乱加密的算法,最重要的便是找到

相应的置乱矩阵.

显然,若仅有一个加解密的图像对(即一个原始图像和一个运用某种纯位置移动加密算法加密的图像),其中所蕴含的位置变换信息往往不足以恢复出置换所使用的遍历矩阵.假设现在拥有一系列的加解密图像对,即一组 k 个加解密图像对(这些图像对都是通过某一个置乱变换 R 来实现的).如果我们能够将所有图像对的信息综合起来考虑,则可以一步步逼近 R,使得 R 中的数据变得愈加清晰.

1.3 有待解决的问题

为了证实理论上的可行性,我们需要考虑以下几个问题:

①究竟需要多少对加解密图像对,才能使得恢复出来的 R 足够清晰,可以用来破解新的加密后的图像?在第三节中我们通过模拟实验结果回答了这个问题.

②如何来表示这种模糊的 R?因为其中的用来表征位置变换的因素都是不确定的.在第三节中,我们将通过引入模糊遍历矩阵 $\tilde{R}$ 的概念,来完成这一任务.

③如何来完成逐个图像对所蕴含位置信息的积累?这一点我们将在第三节中通过定义 $\tilde{R}$ 的求交等运算来实现,并且给出将 $\tilde{R}$ 直接清晰化为 R 的算法.

2 模糊遍历矩阵及其运算体系

首先,我们将通过引入模糊遍历矩阵 $\tilde{R}$ 的概念,来实现对加密图像对之间位置信息的表达.这是一个基于遍历矩阵基础上发展出的新的概念.模糊遍历矩阵中的每一个元素都是一个集合,也就是说映射可能是多元的.此外,我们通过定义其相关求交、求并集和清晰化等运算来形成运算体系.

2.1 概念和定义

2.1.1 模糊遍历矩阵

若一个 $m\times n$ 二维矩阵 $\tilde{R}_{M\times N}=\{\tilde{r}(i,j):1\le i\le M,1\le j\le N\}$,其中,每一个元素都是的子集,并且满足以下条件,则我们称该矩阵为模糊遍历矩阵:

①$\tilde{r}(i,j)\neq\Phi$

②任意两个元素 $\tilde{r}(i_1,j_1),\tilde{r}(i_2,j_2)$,则 $\tilde{r}(i_1,j_1)\cap\tilde{r}(i_2,j_2)=\Phi$,或 $\tilde{r}(i_1,j_1)\cap\tilde{r}(i_2,j_2)=\tilde{r}(i_1,j_1)=\tilde{r}(i_2,j_2)$.

③所有元素的并集为 $\{1,\cdots,MN\}$,即 $\bigcup_{\substack{1\le i\le M\\1\le j\le N}}\tilde{r}(i,j)=\{1,\cdots,MN\}$,

④$\tilde{r}(i,j)$ 在矩阵中出现的次数等于 $\|\tilde{r}(i,j)\|$(集合 $\tilde{r}(i,j)$ 中的元素个数)

则,我们称 $\tilde{R}_{M\times N}$ 为一个 $M\times N$ 阶的模糊遍历矩阵.

2.1.2 确定率/确定位置

$$\text{确定位置}=\text{满足}\|\tilde{r}(i,j)\|=1\text{的位置}$$

$$\text{确定率}=\frac{\text{只有一个元素的集合的个数}}{MN}$$

2.1.3 清晰度/矩阵规模

对一个 $\tilde{R}$ 来说,其所有集合中元素个数的总和,体现其表达时所需要的内存空间.其值越大,则所需要的内存越大,即计算的空间复杂性越大.而依次也可以定义 $\tilde{R}$ 的清晰度.

$$\text{矩阵规模}=\tilde{R}\text{中每个集合中元素个数总和}$$

$$\text{清晰度}=\frac{MN}{\text{矩阵规模}}$$

2.1.4 破解概率/破解空间

我们知道由 $\tilde{R}$ 可以派生出 R,其概率与确定率相关.我们将破解空间和破解概率定义如下:

$$破解空间=\tilde{R}可能构成R的个数$$

$$破解概率=\frac{1}{破解空间}$$

2.2 模糊遍历矩阵的基本运算

我们定义了模糊遍历矩阵,但在后面的具体应用中可以看到,还需要定义其相应的运算.例如,我们为了将若干个的位置信息综合起来考虑,就必须寻找一种"求交"运算;同样,如果要将一个模糊遍历矩阵转化为一个普通的遍历矩阵,则需要一个"清晰化"运算.

2.2.1 求交运算

对同等规模的 $M\times N$ 模糊遍历矩阵 $\tilde{R}_1$ 和 $\tilde{R}_2$,我们可以定义其求交运算为 $\tilde{R}_1$ 中任一位置的集合元素与 $\tilde{R}_2$ 中对应位置的集合元素的求交,其结果显然亦是一个 $M\times N$ 的模糊矩阵,如下:

$$\tilde{R}_1\cap\tilde{R}_2=\begin{bmatrix}R_1(1,1) & R_1(1,2) & \cdots & R_1(1,n)\\ R_1(2,1) & \cdots & \cdots & \cdots\\ \cdots & \cdots & \cdots & \cdots\\ R_1(m,1) & \cdots & \cdots & R_1(m,n)\end{bmatrix}\cap\begin{bmatrix}R_2(1,1) & R_2(1,2) & \cdots & R_2(1,n)\\ R_2(2,1) & \cdots & \cdots & \cdots\\ \cdots & \cdots & \cdots & \cdots\\ R_2(m,1) & \cdots & \cdots & R_2(m,n)\end{bmatrix}$$

例:

$$=\tilde{R}=\begin{bmatrix}R_1(1,1)\cap R_2(1,1) & R_1(1,2)\cap R_2(1,2) & \cdots & R_1(1,n)\cap R_2(1,n)\\ R_1(2,1)\cap R_2(2,1) & \cdots & \cdots & \cdots\\ \cdots & \cdots & \cdots & \cdots\\ R_1(m,1)\cap R_2(m,1) & \cdots & \cdots & R_1(m,n)\cap R_2(m,n)\end{bmatrix}$$

$$\tilde{R}_1=\begin{bmatrix}8 & 7 & (4,6,9)\\ (4,6,9) & 3 & (4,6,9)\\ (1,5) & 2 & (1,5)\end{bmatrix}\qquad \tilde{R}_2=\begin{bmatrix}(8,7,2) & (8,7,2) & (6,9)\\ (6,9) & (3,5) & 4\\ 1 & (8,7,2) & (3,5)\end{bmatrix}$$

则

$$\tilde{R}=\tilde{R}_1\cap\tilde{R}_2=\begin{bmatrix}8 & 7 & (4,6,9)\\ (4,6,9) & 3 & (4,6,9)\\ (1,5) & 2 & (1,5)\end{bmatrix}\cap\begin{bmatrix}(8,7,2) & (8,7,2) & (6,9)\\ (6,9) & (3,5) & 4\\ 1 & (8,7,2) & (3,5)\end{bmatrix}$$

$$=\begin{bmatrix}8\cap(8,7,2) & 7\cap(8,7,2) & (4,6,9)\cap(6,9)\\ (4,6,9)\cap(6,9) & 3\cap(3,5) & (4,6,9)\cap 4\\ (1,5)\cap 1 & 2\cap(8,7,2) & (1,5)\cap(3,5)\end{bmatrix}$$

$$=\begin{bmatrix}8 & 7 & (6,9)\\ (6,9) & 3 & 4\\ 1 & 2 & 5\end{bmatrix}$$

同理,我们可以定义:

$$\tilde{R}_1\cap\tilde{R}_2\cap\tilde{R}_3=\tilde{R}_1\cap(\tilde{R}_2\cap\tilde{R}_3)$$

依次类推即可定义

$$\tilde{R}_1\cap\tilde{R}_2\cap\cdots\cap\tilde{R}_k,k=2,3,\ldots\ldots$$

2.3 清晰化

对于图像解密/加密来说,模糊遍历矩阵并没有实际的价值,但我们可以通过它来恢复相应的遍历矩阵.但由于信息量不足,尚有位置信息无法确定,所以我们有若干种清晰化的过程:

$$\tilde{R}=\begin{bmatrix}\tilde{R}(1,1) & \cdots & \tilde{R}(1,n)\\ \cdots & \cdots & \cdots\\ \tilde{R}(m,1) & \cdots & \tilde{R}(m,n)\end{bmatrix}\xrightarrow{\text{清晰化}}R=\begin{bmatrix}R(1,1) & \cdots & R(1,n)\\ \cdots & \cdots & \cdots\\ R(m,1) & \cdots & R(m,n)\end{bmatrix}$$

则,我们选择一种遍历方式(例如行遍历)[3].我们将 $\tilde{R}(i,j)$ 中最小的一个元素取出(这种我们称为最小值法),作为 $R(i,j)$ 的值,而将 $\tilde{R}(i,j)$ 之后(即 $\tilde{R}_{i\times N+j}$ 之后)的集合元素中的 $R(i,j)$ 的值全部减去.

按这种方式,则可以生成清晰后的 R.

例如:

$$\tilde{R}=\begin{bmatrix}8 & 7 & (4,6,9)\\ (4,6,9) & 3 & (4,6,9)\\ (1,5) & 2 & (1,5)\end{bmatrix}\xrightarrow{1}\begin{bmatrix}8 & 7 & 4\\ (6,9) & 3 & (6,9)\\ (1,5) & 2 & (1,5)\end{bmatrix}\xrightarrow{2}\begin{bmatrix}8 & 7 & 4\\ 6 & 3 & 9\\ (1,5) & 2 & (1,5)\end{bmatrix}\xrightarrow{3}\begin{bmatrix}8 & 7 & 4\\ 6 & 3 & 9\\ 1 & 2 & 5\end{bmatrix}=R$$

3 纯位置移动图像加密的破解算法

由概率论的相关知识,我们可以证明当获得大量的原始图像和加密图像对作为参考时,运用纯位置置乱加密的图像是可以被破解的.

假定共有 k 对加解密图像对,其矩阵规模均为 $M\times N$,而其直方图集合为 $G=\{0,1,\ldots,L\}$,图像矩阵所有位置集合 $\Omega=\{(1,1),\ldots,(M,N)\}=\{1,2,\ldots,MN\}$.

3.1 加解密图像对的定义

3.1.1 源图像

$$I_1=\begin{bmatrix}I_1(1,1) & \cdots & I_1(1,n)\\ \cdots & \cdots & \cdots\\ I_1(m,1) & \cdots & I_1(m,n)\end{bmatrix}_{M\times N},I_2,\ldots,I_k$$

3.1.2 对应的加密图像

$$E_1=\begin{bmatrix}E_1(1,1) & \cdots & E_1(1,n)\\ \cdots & \cdots & \cdots\\ E_1(m,1) & \cdots & E_1(m,n)\end{bmatrix}_{M\times N},E_2,\ldots,E_k$$

3.1.3 其它加密图像(无相应源图像)

$$E_{k+1}=\begin{bmatrix}E_1(1,1) & \cdots & E_1(1,n)\\ \cdots & \cdots & \cdots\\ E_1(m,1) & \cdots & E_1(m,n)\end{bmatrix}_{M\times N},E_{k+2},\ldots,E_{k+p}$$

3.2 生成模糊遍历矩阵

前面定义了模糊遍历矩阵 $\tilde{R}$,现在我们利用其来表示加解密图像对间的位置关系.

一幅图像数字矩阵 $I_{M\times N}$ 通过置换成为 $E_{M\times N}$,则我们需要知道 $E(i,j)$ 这个元素是来自 I 中的哪一个位置,

为做到此,我们可以在 I 中寻找所有和 $E(i,j)$ 值相等的元素的位置,并记录在 $\tilde{R}(i,j)$ 的相应位置中.

举 1 个例子:

$$I_{M\times N}=\begin{bmatrix}A & E & F\\ B & A & B\\ C & D & B\end{bmatrix}\xrightarrow{f_R}E_{M\times N}=\begin{bmatrix}D & C & B\\ B & F & B\\ A & E & A\end{bmatrix}$$

我们记 $I(i,j)=I_{i\times N+j}$,

因而有,$I_1=A,I_2=E,I_3=F,I_4=B,I_5=A,I_6=B,I_7=C,I_8=D,I_9=B$,

同理知,

$$E_1=D,E_2=C,E_3=B,E_4=B,E_5=F,E_6=B,E_7=A,E_8=E,E_9=A,$$

由此,我们可生成 $\tilde{R}$ 如下

$$\tilde{R}=\begin{bmatrix}\{8\} & \{7\} & \{4,6,9\}\\ \{4,6,9\} & 3 & \{4,6,9\}\\ \{1,5\} & 2 & \{1,5\}\end{bmatrix}$$

4 实验结果与结论

我们选取一系列 128×128 的灰度图作为待加密的图像,并使用纯位置置乱算法进行加密(随机矩阵变换).随后,我们利用一些图像对作为参考,对加密图像进行破解.实验结果令人满意.

4.1 一系列加密图像对

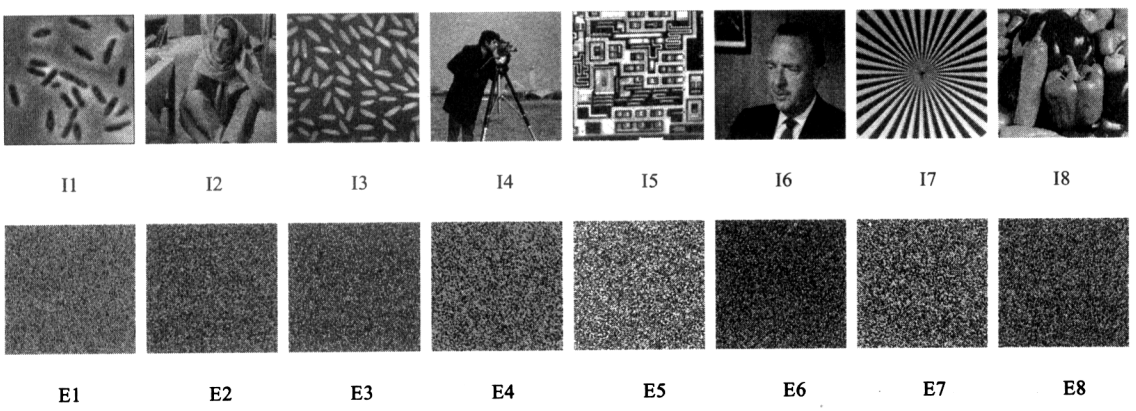


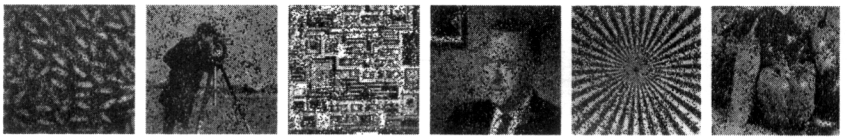
图 1 一系列原始图像和相应的加密图像

4.2 破解结果

4.2.1 恢复后的图像

图 2~图 6 给出了恢复后的图像:

当 k=2 时(如图 2),我们利用前两个图像对(I1-E1, I2-E2)的加密图像对的信息,来尝试对(E3~E8)破解,确定率为 39.843750%,清晰度为 44.226097%,破解概率为 0.000000%.



S1 S2 S3 S4 S5 S6 S7 S8

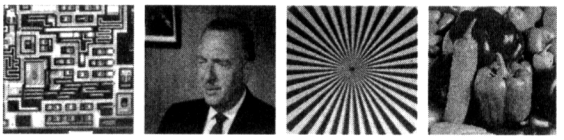
图 2 恢复后的图像 (k=2)

当 k=3 时(如图 3),我们利用前 3 个图像对(I1-E1, I2-E2, I3-E3)的加密图像对的信息,来尝试对(E4~E8)破解,确定率为 96.539307%,清晰度为 96.376471%,破解概率为 0.000000%.

S1 S2 S3 S4 S5 S6 S7 S8

图 3 恢复后的图像 (k=3)

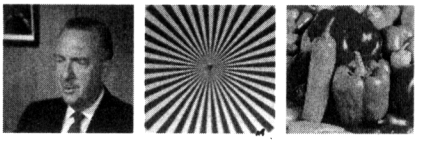
当 k=4 时(如图 4),我们利用前 4 个图像对(I1-E1, I2-E2, I3-E3, I4-E4)的加密图像对的信息,来尝试对(E5~E8)破解,确定率为 99.639893%,清晰度为 99.623009%,破解概率为 0.000000%..



S1 S2 S3 S4 S5 S6 S7 S8

图 4 恢复后的图像 (k=4)

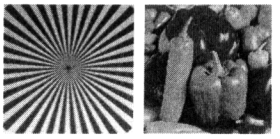
当 k=5 时(如图 5),我们利用前 5 个图像对(I1-E1, I2-E2, I3-E3, I4-E4, I5-E5)的加密图像对的信息,来尝试对(E6~E8)破解,确定率为 99.987793%,清晰度为 99.987794%,破解概率为 50%.



S1 S2 S3 S4 S5 S6 S7 S8

图 5 恢复后的图像 (k=5)

当 k=6 时(如图 6),我们利用前 6 个图像对(I1-E1, I2-E2, I3-E3, I4-E4, I5-E5, I6-E6)的加密图像对的信息,来尝试对(E7~E8)破解,确定率为 100%,清晰度为 100%,破解概率为 100%.



S1 S2 S3 S4 S5 S6 S7 S8

图 6 恢复后的图像 (k=6)

本文中,经过第 6 步之后,我们可以破解任意一个运用纯位置置乱加密算法进行加密的图像.实际上,我们已经检测了 1000 多幅 256 级的灰度图像对(规格从 64×64,128×128,256×256 到 512×512),几乎所有的实验在 6 步内完全破解(即最多需要 6 对参考图象对即可破解加密图像).

5 结束语

本文给出了一种针对纯位置置乱加密的有效破解算法.文中"模糊遍历矩阵"是一个新引入的概念,这有助于对破解中原始信息的积累和相互印证.并通过定义矩阵的求交、清晰化等运算,实现了破解算法.

因为图像模型错重复杂,本算法通过大量的图像对进行破解的模拟仿真.精心挑选了的 1000 多对图像对,设计人物(例如 Lenna 图、摄影师图)、风景、物品、微观照片、电脑合成图等各种类别均选出一定数量进行测试.其中大约有 10 多个特例.通过对它们的特性进行分析,我们发现这些特例图像中像素的灰度值分布极其不平衡.显然,灰度值重复的概率越高,破解的难度越大,因为从理论上来说,其蕴涵的破解信息随着灰度值的增加急剧降低.所以,本算法的对真实的照片作为参照对的破解中非常行之有效;而对于电脑合成图像、太空照片等效果不佳.

随着图像规模的增加,破解所需要的内存空间急剧增加(我们可以很容易证明,破解空间随着图像规模的阶乘成正比).在实验室,在 PentiumII,256M 内存的机器上运行 VC 编写的程序:破解 20 幅以 128×128 规模的 256 级灰度图像,大约需要几秒钟;破解 20 幅以 218×218 规模的 256 级灰度图像,大约需要 10 多分钟;破解 20 幅以 512×512 规模的 256 级灰度图像,大约需要 10 个小时;对于更大规模的图像,限于机器的内存和 CPU 性能,未作进一步实验.但可以估计,在配置 1G 以上内存的服务器中,是可以有效破解至少 1024×768 的加密图像对的.

在今后的论文中,我们将给出对所有图像模型的理论分析,并计算破解概率.利用概率论和代数学知识,可以证明对纯位置置乱算法的破解在理论上是可行的.

致谢 在此,我们向对本文的工作给予支持和建议的同行,尤其是浙江大学数学科学研究中心董光昌教授领导的"图像处理及相关的数学问题"国际研讨班(2004.5.16-28,杭州)的老师和同学表示感谢.

References:

[1] Clifton C, Leavens GT, Chambers C, Millstein T. MultiJava: modular open classes and symmetric multiple dispatch for Java. ACM SIGPLAN Notices, 2000,35(10):130~145.

[2] Qiao LT, Nahrstedt K. Comparison of MPEG encryption algorithms, Comput. & Graphics, 1998,22(4):437~448.

[3] Zhao XY, Chen G. Ergodic matrix in image encryption. SPIE Vol. 4875, 2002. 4875~4878.

[4] Holographic Information Storage and Image Restoration. JICC 2002, The 8th Join International Computer Conference. 2002.

[5] Region-of-interest based flower images retrieval, 2003, III – 589 IEEE ICASSP 2003

[6] MATLAS Y, Shamir A. A video scrambling technique based on space filling curves. In: Proc. of the CPYPTO'87. 1987. 550~559.

[7] Bourbakis N, Alexopoulos C. Picture data encryption using SCAN patter, Pattern Recognition, 1992,25(6):567~581.

[8] Yen JC, Guo JI. A chaotic neural network for signal encryption/decryption and its VLSTI architecture. In: Proc. of the 10th VLSI Design/CAD Symp. Nantou, 1999. 319~322.

[9] 丁玮,齐东旭.数字图像变换及信息隐藏与伪装技术.计算机学报,1998,21(9).

[10] 李均利,陈刚.图像三构件模型的重要性分析.中国图象图形学报,2003 年特刊.