第21卷 第9期 计 算 机 学 报 Vol. 21 No. 9
1998年9月 CHINESE J. COMPUTERS Sept. 1998

数字图像变换及信息隐藏与伪装技术

丁 玮
(中国科学院计算技术研究所CAD开放实验室 北京 100080)
齐东旭
(北方工业大学CAD研究中心 北京 100041)

摘 要 本文讨论的是数字图像变换及其在信息安全中的应用.首先介绍置乱变换,并提出按空间填充曲线、Arnold变换、幻方的图像置乱算法;其次介绍图像分存并提出了将灰度和彩色图像在计算机上进行分存和恢复的方法.

关键词 图像变换,置乱变换,分存.
分类号: TP391

DIGITAL IMAGE TRANSFORMATION AND INFORMATION HIDING AND DISGUISING TECHNOLOGY

DING Wei
(*CAD Laboratory, Institute of Computing Technology, Chinese Academg of Sciences, Beijing* 100080)
QI Dong-Xu
(*CAD Research Center, North China University, Beijing* 100041)

Abstract This paper discusses about digital image transformation and its application in information security. At first, the image scrambling transformation are introduced, and space-filling curves, Arnold transformation, magic square scrambling algorithms are presented; then the image visual secret sharing technology is introduced, and methods to share and recover gray-scale image and color image on computer are presented.

Keywords Image transformation, scrambling transformation, visual secret sharing.

1 引 言

国际互连网络技术的兴起极大地推动了信息产业的发展.由于网络逐渐普及,使人们的一切活动都通过各种信息系统紧密联系起来.信息的安全保密不仅与国家的政治、军事和外交有关,而且与团体、单位和个人密切相关.大量有关个人的数据(私人存款、医疗记录、财产数据等)都要在网络上处理.信息一旦上网,它将可能被轻而易举地获取.对原始信息的非法复制、蓄意篡改会导致严重的后果,因而近年来无论官方或是民间,对信息的安全存储、保密传输、真伪验证等问题,都给予高度的重视.值得强调指出,信息的安全与保密,是整个社会安全与稳定的重要因素.

本课题得到国家自然科学基金资助.丁 玮,男,1971年生,博士研究生,主要研究方向为计算机图形学、计算机辅助几何设计和图像处理.齐东旭,男,1940年生,教授,博士生导师,主要研究方向为计算机辅助几何设计、数值分析、计算机图形学和图像处理.

传统的保密学着眼于限制资料的存取.而且为达到这一目的,在设计算法时可以不顾及可能伴随的数据膨胀.对于图像信息,传统的保密学尚缺少足够的研究,这也许是图像惊人的数据量阻碍研究的进展.然而近年来计算机处理效率的提高无疑为图像信息的安全处理大开方便之门[1].

图像信息安全问题有着极为广泛的含义,其中信息隐藏与伪装技术是十分有趣而又有用的课题.

把信息隐藏在一张图画中,这不是新鲜事,古已有之.四千多年前人类创造的象形文字,那便是一种原始的密写方式.将正常的图像资料加工成一堆乱码,使人难以辨认,这是传统方式.而现代,人们开始发展了一种将加密资料隐藏或变换成另一非机密性的文件内容之中,使加入隐藏信息的目标文件,看起来难以觉察到有什么变化,且其中的机密资料不能显露.

尽管关于图像加密的模拟置乱技术有所报导[1,2],但总的说来关于图像信号的保密文献公开发表的不多.本文讨论的是数字图像变换及其在信息安全中的应用.首先介绍置乱变换,并提出按空间填充曲线、Arnold 变换、幻方的图像置乱算法;其次介绍图像分存并提出了将灰度和彩色图像在计算机上进行分存和恢复的方法.

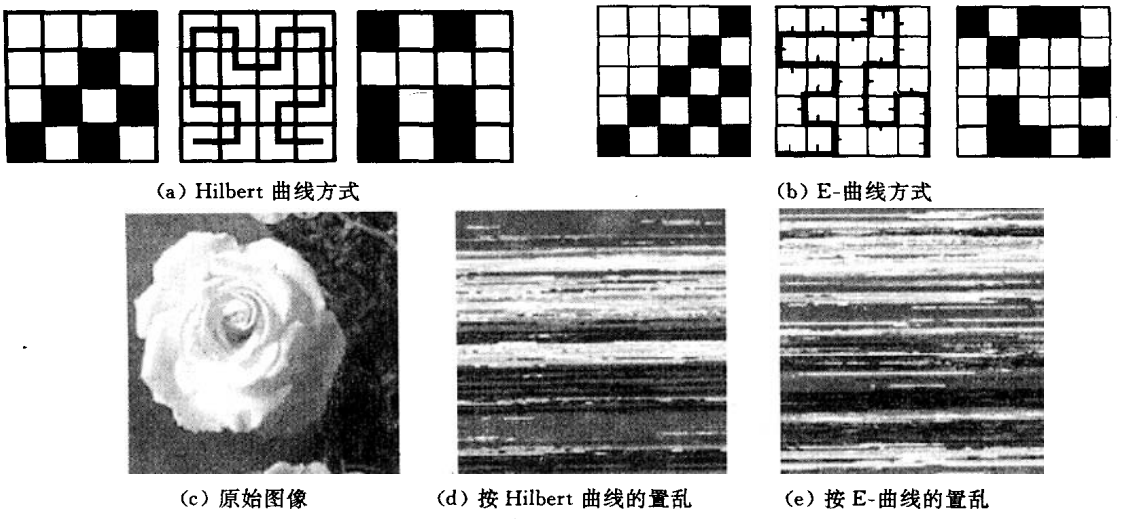
2　图像置乱变换

图像可看作是平面区域上的二元函数 $Z=F(x,y),(x,y)\in R$.在绝大多数情况下区域 R 是一个矩形.对 R 中任意的点 (x,y),则 $F(x,y)$ 代表图像的信息(如灰度值,RGB 分量值等).表示图像的二元函数有其特殊性,这就是相关性.在图像被数字化之后,$Z=F(x,y)$ 则相应于一个矩阵,其元素所在的行与列对应于自变量取值,元素本身代表图像信息.离散化的数字图像相应于元素之间有相关性的一类特别的矩阵.

矩阵的初等变换可以将图像转换成为另一幅图像,但其置乱作用较差.非线性变换则有可能增强置乱作用.

2.1　按空间填充曲线的图像置乱变换

大约 100 年前,数学家发展了一类 FASS 曲线,即充满空间(Space-filling)、非自交(Self-avoiding)、自相似(Self-similar)的简单(Simple)曲线.这类曲线,位于一个维数大于 1 的欧几里德空间,并且在该空间内有一个非空的内部.1890 年意大利数学家 Peano 及 1891 年德国数学家 Hilbert 给出填满一个单位正方形 $S=[0,1]\times[0,1]$ 的曲线.利用 L 系统的边改写与点改写规则,Hilbert 曲线是容易生成的[3].按 FASS 曲线做图像置乱,示意如图 1.



(a) Hilbert 曲线方式　　(b) E-曲线方式

(c) 原始图像　　(d) 按 Hilbert 曲线的置乱　　(e) 按 E-曲线的置乱

图 1　按 FASS 曲线的图像置乱变换

在图 1(a) 中的第一幅为 4 × 4 象素的原图,图 1(a) 中的第三幅是按 H- 曲线次序,将原图的象素点从第一行第一列开始,由上到下、由左到右重新排列的置乱图像;图 1(b) 类同.

2.2　按 Arnold 变换的图像置乱变换

Arnold 在遍历理论的研究中提出了一类裁剪变换.假设图像为 $S=[0,1]\times[0,1],(x,y)\in S$.令

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod 1$$

这就是 Arnold 变换[3]. 我们探讨利用 Arnold 变换对一幅图像做置乱处理. 实际上,可以令离散图像的象素坐标 $x,y \in \{0,1,2,\cdots,N-1\}$,于是 Arnold 变换改写为

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod N$$

并由此作迭代程序:记变换中的矩阵为 A,及右端$(x,y)^{\mathrm{T}}$ 为输入,左端$(x',y')^{\mathrm{T}}$ 为输出,考虑其反馈. 有

$$P_{ij}^{n+1} = AP_{ij}^{n} (\mathrm{mod}\ N), P_{ij}^{n} = (i,j)^{n}, n = 0,1,2,\cdots$$

通过离散点集的置换,同时把图像信息(灰度、颜色)移植过来. 当遍历了原图像所有的点之后,便产生了一幅新的画面.

下面是对一幅数字化图片的变换结果,n 表示迭代步骤. 原图为 128 × 128 图像.

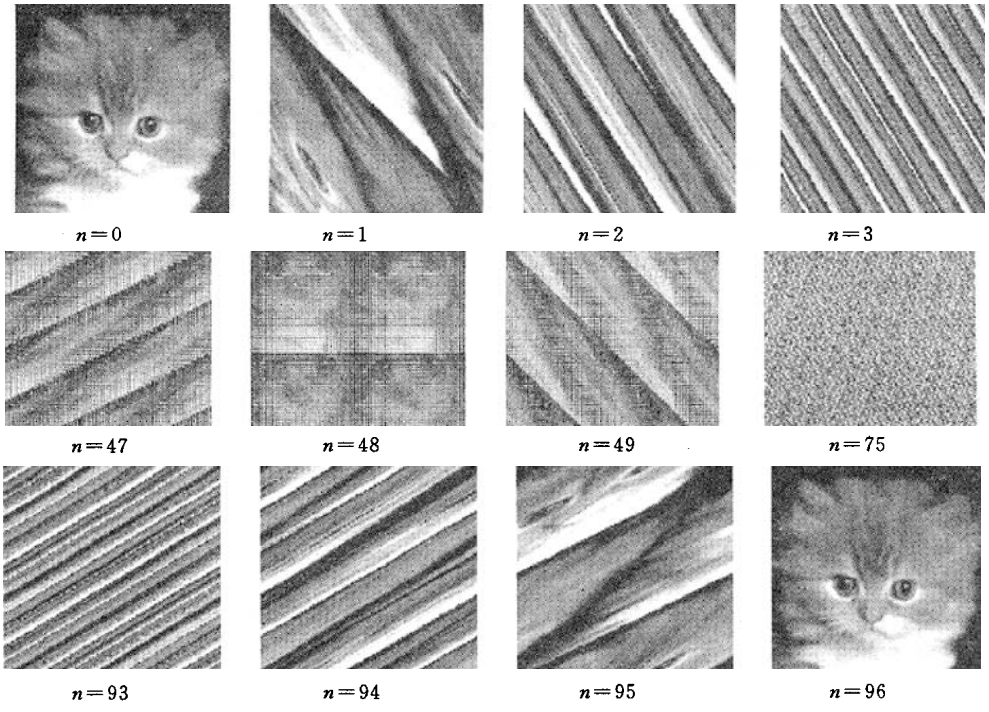


图 2 图像的 Arnold 置乱变换

2.3 按幻方的图像置乱变换

以自然数 $1,2,\cdots,n^2$ 为元素的 n 阶矩阵

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

满足

$$\sum_{\substack{j=1 \\ (i=1,2,\cdots,n)}}^{n} a_{ij} = \sum_{\substack{i=1 \\ (j=1,2,\cdots,n)}}^{n} a_{ij} = \sum_{i=1}^{n} a_{ii} = \sum_{i+j=n+1}^{n} a_{ij} = c \tag{1}$$

其中

$$c = \frac{n^2(n^2+1)}{2}$$

则称 A 为标准幻方.

假定数字图像相应于 n 阶数字矩阵 B. 对取定的 n 阶幻方 A,将 B 与 A 按行列作一一对应. 我们把 A 中的元素 1 移至元素为 2 的位置,将元素 2 移至 3 的位置,…. 一般说来,对任何 $m \in \{1,2,\cdots,n^2-1\}$,它从其在 A 中的位置移至 $m+1$ 在 A 中所在的位置. 若 $m=n^2$,则将 n^2 移至 1 在 A 中所在的位置. 经过这样的置换之后,矩阵 A 转换为矩阵 A_1,记 $A_1=EA$. 对 A_1 来说,可以重复上述置换得矩阵 $A_2=EA_1$,继而 $A_3=EA_2$,$A_4=EA_3$ 等等,这便是一系列的置乱变换. 经过 n^2 步,$A_{n^2}=A$. 一般说,$A_1,A_2,\cdots,A_{n^2-1}$ 并不满足式(1),它们不是幻方.

对数字图像矩阵 B,注意 B 与 A 元素之间的对应关系,随 A 转换为 A_1 而把 B 中对应象素信息(灰度,RGB) 做相应的移置,产生数字图像矩阵 B_1,记为 $EB=B_1$,一般地,有 $E^mB=B_m$.

例如,我们考虑一个由 4×4 象素组成的图像 B,它可以被看作是一个 4 阶方阵

$$B=\begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}$$

在如下 4 阶幻方 A

16	2	3	13
5	11	10	8
9	7	6	12
4	14	15	1

置乱作用下,得到新的 4 阶方阵 B_1

$$B_1=EB=\begin{pmatrix} b_{43} & b_{44} & b_{12} & b_{34} \\ b_{41} & b_{23} & b_{31} & b_{32} \\ b_{24} & b_{33} & b_{21} & b_{22} \\ b_{13} & b_{14} & b_{42} & b_{11} \end{pmatrix}$$

下面是一个用幻方做图像置乱变换的例子,原图像为 64×64 象素真彩色图像.

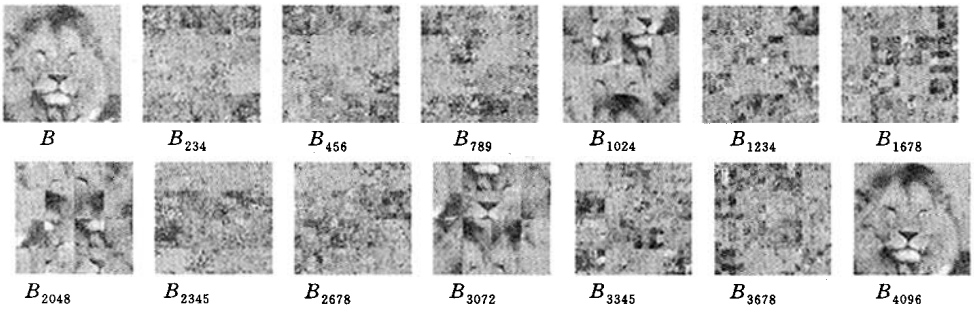


图 3　图像按照幻方的置乱变换

3　图像信息的分存

3.1　二值图像信息分存

Shamir 于 1979 年提出了密钥分存的概念[4],即把密钥 D 分解为 n 个子密钥 D_i,$0\le i<n$,并且满足任意 $k(1\le k<n)$ 个子密钥相结合才能恢复密钥 D,而若少于 k 个子密钥则不能获得密钥 D 的任何信息. 在 1994 年欧洲密码学会议上,Shamir 又提出了二值图像信息分存方案[5]. 苏中民、林行良在文献[6] 中研究了二值图像的任意分存方法. 图像信息分存方法比较直观,但一般说来数据量会发生膨胀.

在 Shamir 的二值图像信息分存方案中,原始图像的每个黑白象素被 2 个子块所代替,其中每个子块由 2×2 个黑白象素构成. 这样就生成了两幅膨胀了的图像,这两幅图像的叠加得到放大 4 倍且对比度有所降低的原始图像. 具体说来,对于黑白象素,分别有如图 4 所示的分解方法.

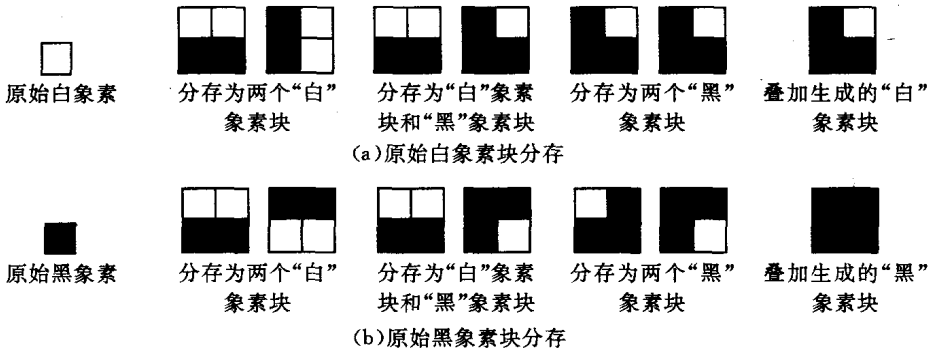


图 4 二值图像信息分存方案

图 5 是一个二值图像信息分存的例子.

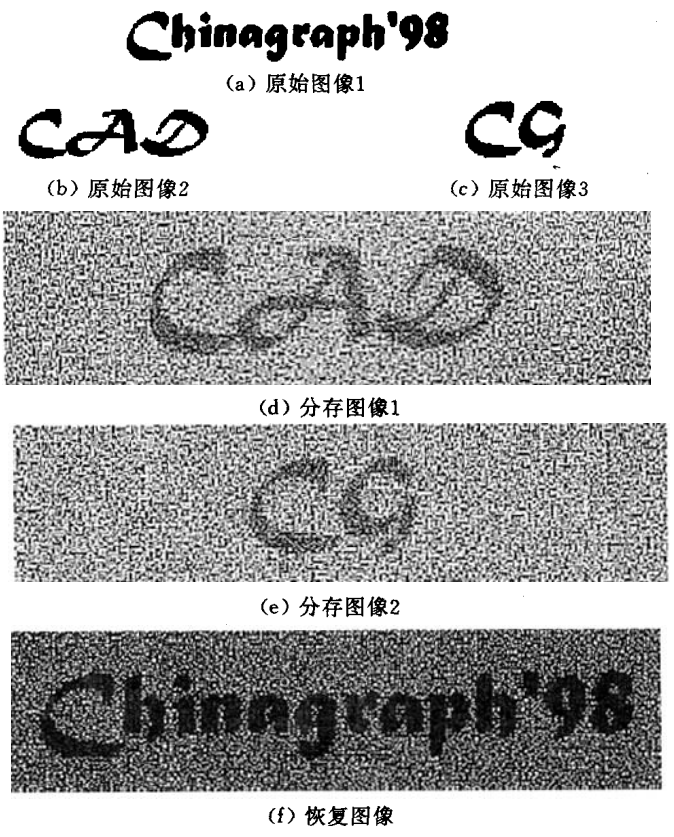
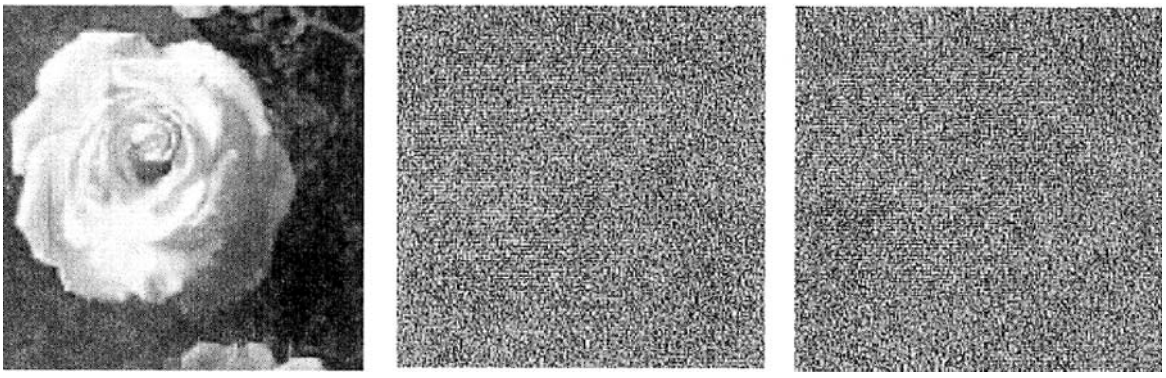


图 5 二值图像信息分存的例子

其中(a),(b),(c)分别为原始二值图像,将图5(a)分存到(b)和(c)当中去,得到分存图像(d)和(e),它们的叠加恢复出对比度稍差的原始图像(f). 如果恢复的图像的对比度不令人满意,可以去掉多余的“噪声”,使之清晰地显现原始图像.

3.2 灰度图像信息分存

灰度图像信息的分存要复杂的多. 由于灰度图像信息比二值图像信息要复杂的多,使得分存灰度图像并直观地叠加予以恢复变得极其困难. 在这里,我们不再考虑将原始图像的分存图像直观叠加进行恢复,而是利用二值分存的算法,在计算机上通过对分存图像运行恢复程序来得到清晰的原始图像. 这样做的好处是,恢复后的图像与原始图像是完全相同的,不会有任何能量损失. 下面是对一幅真彩色图像进行分存的例子.



(a)原始图像　　(b)分存图像1　　(c)分存图像2

图 6　灰度图像分存的例子

对于灰度图像,我们依然采用二值图像分存的方法.在这里,把灰度图像数据的每一位当作二值图像的一个象素来处理.显然,这样分存生成的两个分存图像是不能通过简单的叠加来获取原始图像信息的.我们需要将它们在计算机上进行运算来提取原始图像的信息.简略的算法描述如下:

```
while(还有图像数据未处理)
{
 p = 未处理的图像数据的第 1 位;
 if(p == 0) 按二值图像信息分存方法中分存"黑"象素的方法分拆;
 else 按二值图像信息分存方法中分存"白"象素的方法分拆;
 将分拆生成的二组数据分别输出到两个分存图像中;
}
```

图像信息的分存算法,可以在信息的隐蔽传输与存储的实际问题中得到应用.对二值图像而言,由于可以相当任意地选取两幅不相干的黑白图像(如图 5 中的"CAD"和"CG")作为掩护,而真正想要传输的图像,即原始图像(如图 5 中的"Chinagraph'98")从分存的两幅图像的直观叠加得以恢复.对灰度图像而言,本文给出的算法采用了直接分拆图像信息的方法,而分拆出的数据并不要求各自形成指定的图像,而是两组"乱"码.

作为图像信息隐藏与伪装技术,还应进一步研究其编码与解码速度、传输过程的稳定性(即任何误差或改动造成的影响)等等,这都是有待进一步研究的问题.

参 考 文 献

1　王育民,何大可.保密学——基础与应用.西安:西安电子科技大学出版社,1990

2　江　早.信息伪装——一种崭新的信息安全技术.中国图像图形学报,1998,3(1):83－86

3　齐东旭.分形及其计算机生成.科学出版社,1994

4　Shamir A. How to share a secret. *Communications of ACM*, 1979, 22(11):612－613

5　Naor M, Shamir A. Visual cryptography. In: Proc Eurocrypt'94, 1994. 1－12

6　苏中民,林行良.图视秘密的任意分存.计算机学报,1996,19(4):293－299