文章编号:1005-0523(2010)04-0044-04

基于双置乱与奇异值分解的彩色图像水印算法

石红芹,吕方亮

(华东交通大学 软件学院,江西 南昌 330013)

摘要:提出了一种基于水印和载体双双置乱的安全水印算法。首先将载体图像由 RGB 色彩空间转换为 YUV 彩色空间,再经 Fibonacci 变换置乱后,对 Y 分量进行 8×8 分块,对各块进行奇异值分解。将二值图像经过 Arnold 置乱后嵌入到 Y 分量的各块的奇异值中。经仿真实验证明,该算法对 JPEG 压缩、剪切、旋转、滤波等几何攻击具有比较好的稳健性。

关 键 词:奇异值分解;彩色空间转换;双置乱变换

中图分类号:TP391 **文献标识码**:A

数字水印是信息安全的重要组成部分,作为数字产品认证和版权保护的重要手段,已得到越来越多的关注和发展。数字水印应具有以下几个基本特性:(1) 不易察觉性:数字产品引入数字水印后,应不易被接收者察觉,同时又不能影响原作品的质量。(2) 鲁棒性:能在多种无意或有意的信号处理过程后产生一定的失真,但仍保持水印完整性和鉴别的准确性。(3) 水印容量:嵌入宿主图像水印的多少,将直接影响图像的不可见性。数字水印的不易察觉性与鲁棒性是相互矛盾的,解决这矛盾的有效途径是充分利用人类视觉系统的掩蔽特性。目前在灰度图像中嵌入数字水印受到了广泛深入的研究,并且形成了产品[1]。但在实际应用中,彩色图像和视频占主导地位。因此,近年来人们的研究兴趣逐渐转向在彩色图像和视频中嵌入数字水印。文献[2]提出了一种基于 SVD 的水印算法,虽然其对抗常规的信号处理攻击鲁棒性较高,但是利用伪造攻击[3]对该算法进行攻击能使算法失去意义。本文利用水印和载体图像双双置乱,进一步消除了像素之间的相关性且提高了水印信息的安全性。水印嵌入到奇异值中能对原始图像的剪切、旋转、行列镜像等几何攻击具有比较好的稳健性。

根据 HVS 水印策略,人眼对 YUV 彩色空间中亮度分量 Y 的敏感性低于 RGB 彩色空间中各个颜色分量的敏感性,这样将水印信息嵌入到 Y 分量中具有较高的鲁棒性。因为一般的彩色图像都是用 RGB 彩色空间来表示,所以首先要将彩色图像由 RGB 模式转换到 YUV 模式以得到亮度 Y 分量。YUV 彩色空间与 RGB 空间的转换关系式(1)

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.148 & -0.289 & 0.437 \\ 0.615 & -0.515 & -0.100 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{1}$$

Y 表示亮度,U,V 用来表示色差,R,G,B 分别表示红色、绿色、蓝色分量值。

1 图像置乱

图像置乱作为一种图像加密技术,成为数字图像加密的重要手段之一。所谓图像置乱技术是指将一幅图像的像素的空间位置重新进行排列,将原始图像变换成杂乱无章的新图像。如果不知道所使用的置乱方法和密钥,就很难恢复出原始图像。置乱变换有两个重要特点:(1) 置乱变换一般都有周期性,先是越来越乱,而后当迭代到一定次数之后就会恢复到原图。(2) 置乱变换只是令像素的空间位置发生了变换,而像素的值不变。

收稿日期:2010-03-28

作者简介:石红芹(1970—),女,硕士,讲师,主要研究方向为数字水印、网络信息安全。

1.1 Fibonacci 变换

Fibonacci 数列是数学中很重要的数列，由于它具有许多重要的应用，所以一直受到人们的青睐。Fibonacci数列的定义如下

令：$F_1=1$，$F_2=1$，一般地公式(2)为Fibonacci 数列

$$F_n=F_{n-2}+F_{n-1}\quad n\geqslant 3 \tag{2}$$

Fibonacci 变换的公式见(3)

$$S_k=(kF_n+r)\bmod F_{n+1} \tag{3}$$

F_n、F_{n+1}是Fibonacci 数列中的两个相邻数，其中 $k=0,1,2,3,\cdots F_{n+1}-1$；$r=0,1,2,3,\cdots F_{n+1}-1$。这里 r 可作算法中密钥的一部分。由定义可以看出，该变换可将数列$\{Q\}=(0,1,2\cdots,F_{n+1}-1)$变换成另一个新数列$\{S\}=(S_0,S_1,S_2,\cdots S_{F_{n+1}-1})$且可以证明$\{S\}$是$\{Q\}$的一个伪随机置换[4]。考虑到 Fibonacci 变换置乱度计算量小，置乱的周期短，速度快。故而对彩色载体图像用 Fibonacci 变换。图 1 为载体图像，图 2为经过 Fibonacci 置乱变换的载体图像。

1.2 Arnold 变换

Arnold 变换是将图像看作平面区域上的二元函数 $Z=F(x,y)$，$(x,y)\in R$，通常区域 R 是一个矩形。对 R 中的任意点相对应的函数值代表图像的信息 (如灰度值等)。

图像的离散 Arnold 变换即为式(4)

$$\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}1&1\\1&2\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}\pmod N \tag{4}$$

式中：(x,y)表示该图像矩阵的某个元素未变换时的位置，(x',y')表示变换后新的位置。通过变换水印图像由清晰到模糊，提取水印后，可以利用 Arnold 变换的周期性，重新得到原图像. 表 1 为部分不同尺寸的图像经 Arnold 变换的周期表：

表 1　Arnold 变换的周期

图像大小	变换周期
32×32	24
64×64	48
128×128	96
256×256	192

因 Arnold 变换具有算法简单，运算快和具有周期性等特点故对水印的加密采用二维 Arnold 变换。图 3 为水印图像，图 4 为经过 Arnold 置乱变换的水印图像。

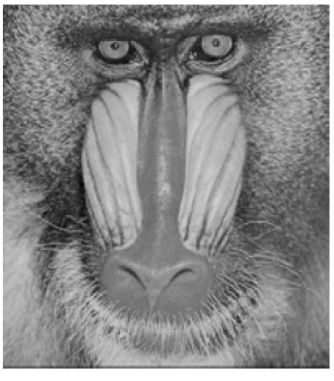

图 1　载体图像

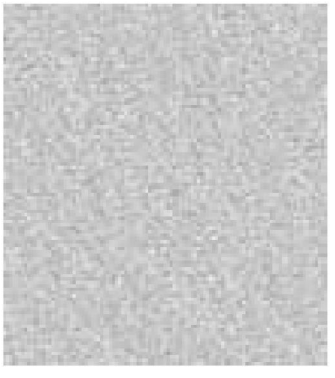

图 2　置乱后的载体图像

图 3　水印图像图

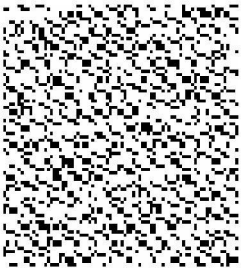

图 4　置乱后的水印图像

2　图像的奇异值分解

奇异值分解是线性代数中一种重要的矩阵分解，在信号处理、统计学等领域有重要应用。数字图像可以被视为有许多非负标量组成的矩阵，奇异值分解(singular value decomposition，SVD)是一种将矩阵进行对角化的数值技术，已被广泛应用与图像编码和其他信号处理技术中。从图像处理的角度来看，奇异值分解有如下的特性：一幅图像的奇异值具有相当好的稳定性，也就是说，当图像受到轻微的扰动时，它的奇异值

不会发生剧烈的改变，从线性代数的角度来看，一幅数字图像可以看成是由一个许多非负标量项组成的矩阵。用 $X\in \boldsymbol{R}^{N\times N}$ 表示一个图像矩阵，其中 $\boldsymbol{R}$ 表示实数域，则 X 的奇异值分解定义如式(5)

$$X=USV^{\mathrm{T}} \tag{5}$$

式中：$U\in R^{N\times N}$ 和 $V\in R^{N\times N}$ 均为正交阵，$S\in R^{N\times N}$ 为对角阵。其对角线上的元素满足式(6)

$$\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_r\geqslant\lambda_{r+1}=\cdots=\lambda_N=0 \tag{6}$$

式中：r 为 X 的秩，$\lambda_i(1\leqslant i\leqslant N)$ 由分解惟一确定，它称之为X的奇异值。图像SVD分解，其奇异值所表现的是图像内在的代数特性而非视觉特性，它可以作为图像特征之一。奇异值的稳定性非常好，当图像被施加小的扰动时，图像的奇异值不会有大的变化。文献[5]给出了SVD分解运用于水印嵌入算法的理论分析。

3 水印的嵌入与水印的提取

3.1 水印的嵌入

本文选取的载体图像为 $M\times M$ 的彩色图像Baboon，水印为 $N\times N$ 的二值图像Cameraman。因为当载体图像较大的时候进行奇异值分解的时间较长，故可先将其分块后再分别对每块进行SVD分解。具体的水印嵌入过程描述如下：

步骤1：将原始水印图像进行二维Arnold置乱得待嵌入的水印图像，迭代的次数k就是一个密钥。应用公式(7)，对置乱水印图像进行奇异值分解。

$$X=U_WS_WV_W^{\mathrm{T}} \tag{7}$$

其中 T 为共轭转置。

步骤2：将彩色载体图像由RGB模式转换为YUV模式后对Y分量进行Fibonacci置乱变换，置乱参数 r 可以作为密钥。

步骤3：对置乱后的载体图像进行8×8分块，对每一块进行奇异值分解，得到公式(8)

$$X^j=U_k^jS_k^jV_k^{\mathrm{T}}\qquad j=1,2,\cdots,64 \tag{8}$$

其中：j 代表各个分块，$\lambda_i^j(i=1,2,\cdots,N)$ 为 S^j 的奇异值元素。

步骤4：利用公式(9)修改各个分块的奇异值，嵌入水印图像的奇异值到各个分块中。

$$\lambda_i^*=\lambda_i^j+\alpha_j\lambda_{wi} \tag{9}$$

其中 $i=1,2,\cdots,N$，$j=1,2,\cdots,64$，α_j 为嵌入因子。

步骤5：利用修改后的各分块的奇异值集，由公式(10)进行重构，逆Fibonacci变换，再由YUV模式转换为RGB模式，得到嵌入水印后的载体图像。

$$X^{*j}=U_k^jS_k^{*j}V_k^T\qquad j=1,2,\cdots,64 \tag{10}$$

3.2 水印的提取

水印提取是水印嵌入的逆过程，在水印图像的加密域进行。具体提取过程如下：

步骤1：对含水印图像进行彩色空间模式变换，由RGB转换为YUV模式后进行Fibonacci置乱变换后，提取 Y 分量进行8×8分块。

步骤2：由公式(8)对各分块进行奇异值分解，再利用公式(11)从各分块中提取水印图像的奇异值。

$$\lambda_{wi}^j=(\lambda_i^{*j}-\lambda_i^j)/\alpha_j \tag{11}$$

其中：$i=1,2,\cdots,n$，$j=1,2,\cdots,64$。

步骤3：利用公式(7)，提取出置乱水印图像，再经利用Arnold反置乱技术和提供的密钥(置乱次数k和加密者的密钥)解密提取出来的信息，即得到可能已经失真的图像水印。

4 实验结果与仿真

本实验采用512×512的彩色图像Baboon，水印为128×128的二值图像Cameraman，为了客观地验证本

算法的性能，这里引入两个指标：归一化相关系数 NC：原始水印和提取出的水印之间的相似度可以通过相关性检验来衡量；峰值信噪比 PSNR：用来客观反映图像视觉特性的指标，嵌入水印的图像可以用 PSNR 验证水印的不可见性。图 5 为水印图像受到攻击时的部分测试结果图。

图 5　水印图像部分攻击测试结果

本文算法与常用的鲁棒性较好的小波域置乱水印算法[6]和基于改进型的 SVD 算法[7]作比较，用水印图像常常遇到的攻击手段对无置乱、水印置乱、原图置乱和本文采用的双置乱算法进行攻击，观察它们的 NC 值。实验结果的比较如表 2。

表 2　不同置乱方式下的抗攻击实验 NC 值比较

比较方式	无置乱 $PSNR=42.377$	水印置乱 $PSNR=42.216$	原图置乱 $PSNR=42.353$	双置乱 $PSNR=42.382$
JPEG 压缩 $QF=30$	0.915 2	0.918 7	0.917 1	0.904 4
JPEG 压缩 $QF=20$	0.576 6	0.595 1	0.766 2	0.765 4
5×5 高斯低通滤波	0.949 3	0.961 5	0.974 1	0.977 7
中值滤波(5×5)	0.938 4	0.875 4	0.884 6	0.879 5
椒盐噪声(0.005)	0.812 1	0.817 9	0.816 2	0.814 2
剪切(1/4)	0.997 3	0.995 9	0.972 3	0.976 5
剪切(1/2)	0.991 8	0.990 8	0.985 4	0.986 4
旋转(20 度)	0.808 5	0.844 5	0.858 7	0.863 5
旋转(45 度)	0.759 5	0.803 6	0.811 1	0.819 6
放缩(1/2)	0.801 9	0.765 1	0.764 8	0.766 8
放缩(2 倍)	0.998 9	0.999 9	0.999 9	0.999 9

5　结论

由以上各个实验可以看出，本文采用的水印嵌入策略，很好地满足了数字水印的不可见性，在人类视觉系统中图像明显改变的攻击下，也表现了不错的鲁棒性，本算法的创新之处就在于采用了水印和彩色载体图像的双置乱，不但较好地保证了算法的安全性，而且在抗几何变换攻击上也具有良好的性能。

参考文献：

[1] 李斌，王新伟．关于 SVD 图像水印算法的分析和改进[J]．华东师范大学学报，2007，13(1)：100-106.
[2] 王淑琴，张金海，王卫民．一种基于奇异值分解的自适应水印算法[J]．计算机仿真，2008，25(8)：109-112.
[3] 徐超汉，柯宗贵．计算机网络安全实用技术[M]．北京：电子工业出版社，2005.
[4] 堪志鹏，邹建成．一种基于 Fibonacci 变换的视频置乱技术[J]．北方工业大学学报，2007，19(3)：6-10.
[5] 李学斌，俞登峰，程亮．基于奇异值分解的零水印算法[J]．计算机工程，2009，35(11)：163-165.
[6] 杨卫民，谭骏珊，金正．基于奇异值分解的彩色图像水印算法[J]．计算机工程与设计，2008，29(23)：6 151-6 153.
[7] 张遂生，袁正道．基于奇异值分解的数字水印改进方案[J]．南京师范大学学报，2008，8(4)：141-144.

(下转第 67 页)

Verifiable Dynamic Multi-secret Sharing Scheme

Zhao Liping，Tang Wenliang

(School of Software Engineering，East China Jiaotong University，Nanchang 330013，China)

Abstract：The paper proposes a new verifiable multi-secret sharing scheme of dynamic threshold. The security of the proposed scheme is based on Shamir's secret sharing scheme and the ECIES cryptosystem，and the difficulty in solving the elliptic curve discrete logarithm. In the scheme，the secret will change periodically and the dealer will periodically publish some of the information to increase the robustness of system. The dealer could adjust the threshold value depending on the secure level of different secret. In addition，the efficient solutions against multiform cheating of any participant are proposed，and the participants can verify the information which they have received. Each participant uses his own private secret during different time periods to reconstruct the corresponding shared secrets without revealing their own private information. Public information is renewed periodically in the scheme，which will not influence new secret sharing.

Key words：threshold；elliptic curve；secret sharing；multi-secret

（责任编辑　刘棉玲）

（上接第 47 页）

A Watermarking Algorithm for Color Images Based on Double Scrambling and SVD

Shi Hongqin，Lv Fangliang

(School of Software，East China Jiaotong University，Nanchang 330013，China)

Abstract：A secure watermarking algorithm based on watermark and the double carrier scrambling is proposed. Firstly，the carrier image is transformed from RGB color space into YUV color space. After scrambling Fibonacci transformation，the Y component is divided into 8×8 blocks and singular value decomposition for each block is conducted. Through Arnold，the binary image is embedded into singular value of each block of Y component. Simulating experiments show that the algorithm has better robustness for JPEG compression，cropping，rotation，filtering，and geometric attacks.

Key words：singular value decomposition；color space convert；double scrambling transform

（责任编辑　王建华）