一种改进的抗几何攻击的数字图像水印算法

李 健 叶有培 韩 牟
(南京理工大学计算机学院 南京 210094)

摘 要 利用奇异值分解的特性,提出了一种改进的基于奇异值分解的数字水印算法。该算法通过设定采样的起始和终止参数,对图像的频域幅度值进行有选择的部分采样。然后利用采样后的数据构造嵌入水印的数据矩阵,并对数据矩阵进行分块奇异值分解,获取一个由次大奇异值组成的数字序列。最后通过可调强度的加性方法,在次大奇异值上嵌入水印信息。依靠数据矩阵的采样构造方式和次大奇异值的几何攻击不变性实现了数字水印的抗几何攻击性。实验结果表明,该方法较传统方法而言有更高的灵活性和鲁棒性。

关键词 奇异值分解,数字水印,几何攻击
中图法分类号 TP391 **文献标识码** A

Improved Watermarking Algorithm for Digital Images Robust to Geometric Distortion

LI Jian YE You-pei HAN Mou
(School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract A novel digital watermarking algorithm based on singular value decomposition(SVD) was proposed. The data was collected in amplitude of image frequency domain through setting the start parameter and termination parameter of sampling. Data matrix for embedding watermarking was constructed by using these collection data. The algorithm made SVD on blocks of data matrix, and got a sub-maximum singular value sequence. Watermark was embedded via modifying the sub-maximum singular value. The modification method is a additive means, and intensity can be adjusted according to the image characteristics. The watermarking algorithm can resist geometric distortion depending on data matrix construction method and geometric attacks invariance of sub-maximum. The experimental results show that the method is more flexibility and robustness than traditional methods.

Keywords SVD, Digital watermarking, Geometric distortion

数字水印技术,是信息隐藏的一个重要分支,是一种专门解决互联网上多媒体信息安全问题的技术。它涉及了信息安全、多媒体信号处理和模式识别等多个学科。目前,数字水印已经成为多媒体版权认证和完整性保护的有效手段,但数字水印算法抗几何攻击的性能,严重制约了数字水印的使用范围。设计抗几何攻击的数字水印算法,成了数字水印技术研究的难点,也是数字水印技术实用化的一个瓶颈。

1 奇异值分解技术在数字水印中的应用

奇异值分解(SVD, Singular Value Decomposition)作为一种在变换域中寻找水印嵌入位置的策略,由 Liu[1] 等较早提出。Liu 在文章中,给出了基本的基于奇异值分解的水印嵌入方法。随后,在这个基础上,提出了很多改进方法。改进的思路大致可以分为3种方向:第一种方向,引入一些加密或其它的水印嵌入方法,与奇异值分解一起完成水印的嵌入过程,这种改进相对其它两种方案来说比较小,与原有嵌入方法比较接近[2]。第二种方向,最早提出的奇异值分解是在整个图像上进行的,从安全性或水印容量上来看都不能令人满意,于是提出了先对图像进行分块,然后在各个子块上进行奇异值分解的水印嵌入方法[3,4]。分块的奇异值分解,很好地改善了原有嵌入方法的性能,逐渐成了现在利用奇异值分解解决水印问题的一个主要步骤。第三种方向,将奇异值分解与其它频域变换相结合,获得鲁棒性更好的奇异值[5-7],DCT,DWT,DMWT 作为常用的频域构造方法,都已经应用到了与奇异值分解相配合的方法中。随着基于奇异值分解的水印嵌入算法的研究,奇异值本身具有的抗几何攻击特性引起了学者的注意。上海交通大学电子工程系的周波[8]就提出了一种依靠奇异值分解来抵抗几何失真的数字图像水印算法,并在文章中对奇异值的几何不变性进行了详细的证明。但他提出的方案,仍然沿用了传统的奇异值分解模式,这些模式很好地利用了奇异值在几何变换之后的稳定性,但为了提取水印而公开的中间文件包含了大量水印信息,降低了系统的安全性。

针对这个问题,结合现有的基于奇异值分解的水印算法,本文提出了一种改进的基于奇异值分解的抗几何失真的数字图像水印算法。

到稿日期:2009-03-31 返修日期:2009-06-03 本文受国家自然科学基金项目(60472061)资助。
李 健(1979-),男,博士生,主要研究方向为信息安全与数字水印等,E-mail:li_jian7979@hotmail.com;叶有培(1944-),男,教授,博士生导师,主要研究方向为信息安全等;韩 牟(1980-),女,博士生,主要研究方向为信息安全等。

2 图像奇异值分解的分析和讨论

2.1 同一图像奇异值分解的分析

奇异值分解从分解的形式上主要有两个部分：一个是分解后的奇异值序列，另一个是分解得到的 U,V 矩阵。这两部分在图像的重构过程中都起到了一定的作用。下面以 Lena 图(512×512)在不同亮度下的 3 幅图像作为实验样本，分析同一图像奇异值分解。

按照式(1)分别对 3 幅图像进行奇异值分解，得到 3 幅图像的奇异值序列和 U,V 矩阵：

$$A=U\begin{bmatrix}\Sigma & o\\ o & o\end{bmatrix}V^H \tag{1}$$

其中，$\Sigma=\mathrm{diag}(\sigma_1,\sigma_2,\cdots,\sigma_r)$，而 $\sigma_i(i=1,2,\cdots,n,n\leqslant r)$ 为 A 的非零奇异值。

奇异值序列本身就是一个从大到小排序的有序序列，并且排在序列后面的奇异值要远远小于前面的，值小的奇异值权重也很小，所以实验只以前 100 个奇异值作为分析的目标数据。

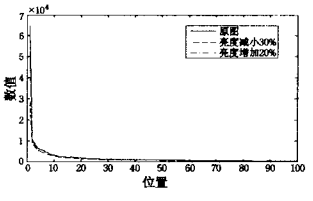

图 1 同一幅图像不同亮度下的奇异值

从图 1 可以看出，在 100 个奇异值中的前 10 个奇异值之后，奇异值的数值明显变小，所以下一步只对前 10 个奇异值进行详细的分析。

表 1 给出了前 10 个奇异值的具体数值。

表 1 不同亮度 Lena 图的前 10 个奇异值

位置	原图	亮度减小 30%	亮度增加 20%
1	64841	28905	72106
2	10620	9120	10475
3	8193	7055	8027
4	6490	5478	6433
5	5896	4989	5800
6	5562	4207	5480
7	4598	3926	4482
8	4101	3416	4020
9	3383	2900	3255
10	3181	2716	3147

从表 1 的数据可以看出，在奇异值序列中，亮度的变化主要反映在图像奇异值分解后的第一个奇异值上，后面 2～10 位的奇异值变化不大。图像的亮度变化，在图像的传播过程中很容易产生。即使同一图像出现不同的亮度形式，仍然应该认定为是同一幅图像。可见，如果使用空域的水印算法，尽管第一个奇异值要比后面的奇异值大很多，容易以大强度嵌入水印信息，但由于反映了大部分亮度信息，因此不适合在这一点上嵌入水印信息。

2.2 不同图像奇异值分解的分析

上一节讨论了同一幅图像在不同亮度下的奇异值分解的情况。本节沿用上一节的讨论方法，用 Lena，Baboon 和 Plane 3 幅图像做实验，给出具体的实验结果并进行分析。实验结果如图 2 所示和表 2 所列。

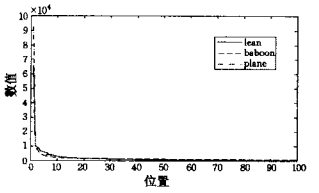

图 2 不同图像的前 100 个奇异值

由图 2 中曲线可以看出，3 幅不同图像的前 10 个奇异值有较大的不同，之后奇异值的差异逐渐缩小，并趋于基本相同。

表 2 3 幅图像的前 10 个奇异值

位置	Lena	Baboon	Plane
1	64841	66845	92341
2	10620	9554	10286
3	8193	6231	9244
4	6490	4390	6279
5	5896	3615	4918
6	5562	2954	4286
7	4598	2649	3834
8	4101	2421	3543
9	3383	2336	3213
10	3181	2177	3060

从表 2 可以看出，3 幅不同图像的前 10 个奇异值的确具有较大的差距。

与奇异值的分析类似，U,V 这两个矩阵在亮度变化中受到的影响可以通过以下的实验方法给出答案。

设 3 幅图像的奇异值分解形式为：

$$A_i=U_i\Sigma_iV_i^{\mathrm{T}}(i=1,2,3) \tag{2}$$

因为图像的像素信息都是实数，所以这里采用了奇异值分解的实数形式，其中 A_i 表示 3 幅不同亮度的 Lena 图像，U_i,V_i,Σ_i 分别代表 3 幅图像奇异值分解的矩阵和奇异值。利用不同的奇异值和 U,V 矩阵组合重构图像，重构公式如式(3)所示，并分析重构的图像 A_{mn}：

$$A_{mn}=U_m\Sigma_nV_m^{\mathrm{T}}(m,n=1,2,3,\text{且 } m\neq n) \tag{3}$$

从对重构图像的分析中发现，第一，尽管采用的是不同图像的奇异值序列，但是只要 U,V 矩阵不变，图像显示的内容不变，图像所显示的内容完全由图像奇异值分解的 U,V 矩阵决定。第二，完全不同的两幅图像(如图像 Lena 和 Plane)，奇异值分解后的奇异值很可能比较接近，这样重构出的图像与原图像很相似。

通过本小节对奇异值和 U,V 矩阵的实验分析发现，对直接在空域进行的奇异值分解，奇异值序列的前几个值(不包括第一个最大的奇异值)和 U,V 矩阵都具有一定的稳定性，符合嵌入水印信息的条件，但是 U,V 矩阵中的值过小，通常在(−1，+1)这个区间内，从数值上看，不能承受太大的变动。

2.3 基于奇异值分解的水印算法的分析

典型 SVD 方法的基本原理[1]是将水印嵌入到原始图像的奇异值中。在奇异值分解得到矩阵 Σ 后，把水印 $W\in R^{n\times n}$ 叠加到矩阵 Σ 上。然后对新产生的矩阵 $\Sigma+\alpha W$ 进行奇异值分解，得到分解后的 U_1,V_1 矩阵和奇异值矩阵 Σ_1。其中 $\alpha>0$，可以调节水印的嵌入强度。最后将矩阵 $U,\Sigma_1,V^{\mathrm{T}}$ 相乘，得到处理后包含水印信息的图像。如果用 A 代表原始图像，$\tilde{A}$ 代表嵌入水印后的图像，整个嵌入过程可以简单地表示为：

$$A\Rightarrow U\Sigma V^{\mathrm{T}} \tag{4}$$

$$\Sigma+\alpha W\Rightarrow U_1\Sigma_1V_1^{\mathrm{T}} \tag{5}$$

$$\tilde{A}\Leftarrow U\Sigma_1V^{\mathrm{T}} \tag{6}$$

在水印的检测过程中，如果待测图像是 A'，那么利用 U_1，Σ，V_1 就可以方便地提取出水印信息，提取的过程如下：

$$A'\Rightarrow U'\Sigma_1'V'^{\mathrm{T}} \tag{7}$$

$$D\Leftarrow U_1\Sigma_1'V_1^{\mathrm{T}} \tag{8}$$

$$W'\Leftarrow\frac{1}{\alpha}(D-\Sigma) \tag{9}$$

从水印的检测过程中可以看出，检测算法只涉及到待测图像的奇异值矩阵 Σ_1'，这种水印算法，会带来几个严重的问题。

第一，即使相差很多的图像，仍然能分解出比较接近的奇异值（$\Sigma_1'\approx\Sigma_1$），而基于这种相似的奇异值重构的水印图像，会被误判为含有水印信息。

第二，检测过程使用 U_1，V_1 进行含水印信息图像的重构，即使奇异值矩阵有很大差别，重构的图像仍然与原图像比较相似，这种情况同样会被误判为含有水印信息。

第三，这种水印算法很容易被破解。如果对一幅含水印的图像进行奇异值分解，得到奇异值矩阵 Σ，Σ 是一个合法的、可以检测出水印的奇异值矩阵。然后对非授权的图像进行奇异值分解，得到矩阵 U_1，V_1，Σ_1，再利用 U_1，V_1 和 Σ 重构图像，把重构的图像作为合法图像发布出去。这样一来，非授权的用户都可以随意制作带有版权水印的图像，这个过程可以简单表示为：

$$A\Rightarrow U\Sigma V^{\mathrm{T}} \tag{10}$$

$$B\Rightarrow U_1\Sigma_1V_1^{\mathrm{T}} \tag{11}$$

$$B'\Leftarrow U_1\Sigma V_1^{\mathrm{T}} \tag{12}$$

其中，A 表示含水印的合法图像，B 代表不含水印的非法图像，B'就是合成的含水印的非法图像。

第一、第二个问题只是降低了这种 SVD 水印算法的准确度，而第三个问题的存在，彻底消除了这种算法的可行性。随后很多学者基于这种算法进行了一些改进，但不同程度上还是存在以上 3 个问题。要想彻底解决，必须消除对 U，V 矩阵的依赖，只利用矩阵的奇异值嵌入和提取信息。下面就按照这个思路，提出了一种新的基于奇异值分解的抗几何失真的数字图像水印算法。

3 水印算法的实现

从以上的分析可以发现，由于奇异值分解本身带有的特性，直接在整幅图像的空域上进行奇异值分解，依靠奇异值嵌入水印信息效果并不好。为了增加水印算法的安全性，并提高水印容量，可以采用变换域中分块的方法，文献[9]就是采用了这种思想。但是图像分块之后，原有的抗几何攻击性就降低了，所以文献中增加了对图像平移和旋转的校正方法，以此消除平移和旋转的影响。而 DFT 变换域本身就具有很好的循环平移不变性和旋转性，利用 DFT 变换和分块 SVD 相结合的方法，可以有效解决水印嵌入安全性和抗几何攻击的问题。

3.1 构造数据矩阵

构造数据矩阵的第一步是对整幅图像进行 DFT 变换，得到图像的 DFT 变换域。并对变换后的数据进行中心化操作，将变换域的零频域置于中心区域，然后计算幅值，产生图像中心化的幅度谱。中心化的幅度谱天然分成 4 个象限，并且满足对称性，如式(13)所示：

$$X_{i,j}=X_{N-i+1,N-j+1}(i,j\leqslant N) \tag{13}$$

其中，$X_{i,j}$ 表示中心化幅度谱中坐标为(i,j)的点，整个幅度谱大小为 $N\times N$。

DFT 变换的对称性减少了可嵌入水印信息嵌入点的数量，但为抵抗旋转攻击提供了途径。实验发现，虽然图像在攻击前后保持了原有的象限，但无法恢复旋转图像和原图像之间的象限同步，即无法确认旋转后的象限对应原图像的第几个象限。针对这个问题，本文提出了一种分象限采样的方法。

任意选择一个象限作为采样的起始象限，采集该象限选定区域内的信息（采样方法在下面详细说明），得到一个数据集合 A。完成该象限的数据采集后，按照顺时针顺序，选择下一个象限，继续进行一次数据的采集，同样可以得到一个数据集合，假设为 B。根据正对称的条件可以知道，其它对称的两个象限，数据也必然为 A 和 B。那么，不论怎样旋转，顺时针方向的两个连续象限，采样后得到的肯定是数据集合 A 和 B。以这两个数据集合上下叠加组成的矩阵，结果只有两种形式，如图 3 所示。

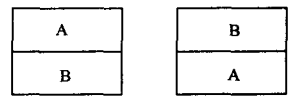

图 3 两象限数据组合形式

在水印的检测过程中，如果按照一种形式提取不出水印，那么只需要交换两个象限的上下顺序，检测另一种形式下是否存在水印，就可以做出判断。这样，通过增加部分计算量，就能够完全消除旋转攻击带来的影响。

而每一个象限的采样顺序，要根据 DFT 变换域数据的特点，尽量将靠近低频区的、比较大的数据和靠近高频区的比较小的数据交叉存放。这样，在后续步骤的分块 SVD 分解中，可以将能量均匀地分布于每一个子块中。所以，这里不采用一般的环形采样方法，提出一种沿半径方向的类之字形采样方式。采样时，从设定的起始距离开始，顺半径方向顺序采样，直到采集到满足终止距离的点；然后返回到下一个起始距离点，开始另一个平行于半径方向的采样，直到全部采集完。

图 4 以 6×6 的矩阵为例（右下角为测算距离的中心点），标出了采样点的采样先后顺序。其中起始距离 $d_1=3$，终止距离 $d_2=5$。

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

图 4 采样顺序

3.2 起始距离和终止距离的确定方法

d_1 和 d_2 的数值受水印大小、原始图像大小及分块奇异值分解的分块参数影响，所以要综合考虑这 3 方面的情况，以确定 d_1 和 d_2 的大小。假设水印的长度为 I，在这里将水印统一表示成一维序列的形式。其它形式的水印，例如图像水印 T（大小为 $M_w\times N_w$），可以顺序扫描成 $1\times I(I=M_w\times N_w)$ 的一维序列形式。图像的大小表示为 $N\times N$，分块奇异值分

解的分块参数为 M，M 通常等于 4 或 8，表示将采样后的数据矩阵按照 4×4 或 8×8 不重叠地分块。

一般情况下，为了将采样的区域置于 DFT 变换频谱图的中频区域，应选择 $N/4 \leqslant d_1 < d_2 < N/2$ 的范围。并且，d_1 和 d_2 必须满足式(14)，其中 τ 表示在分块奇异值分解之后，每个块中准备嵌入水印信息的奇异值个数，根据分块大小的不同，可以选择 1 或 2，如果选择更大的分块参数，τ 相应的选择范围也更大。

$$\frac{\pi\tau(d_2^2-d_1^2)}{2} \geqslant I \times M^2 \tag{14}$$

3.3 水印嵌入步骤

设要嵌入水印信息的原始图像为 $G(N\times N)$。在这里，选用一幅图像作为水印，待嵌入的水印图像表示为 $F(N_w \times N_w)$。

具体的嵌入步骤如下。

Step1 对原始图像 $G(N\times N)$ 做 DFT 变换，计算原始图像的幅度谱。

Step2 对图像的幅度谱进行中心化操作。将变换域的零频域移到图像的中心位置，得到中心化幅度谱矩阵 $G_c(N\times N)$。

Step3 根据 3.2 节提出的方法确定参数 d_1 和 d_2 的大小，并选定参数 M 和 τ。在这里，选择 $M=4$，$\tau=1$。将采样系数重组成矩阵 $S(S\in G_c(N\times N)$，一般为方阵)。

Step4 将重组后的系数矩阵 S 分割为 K 个互不覆盖的 4×4 子块，记为 $S_k(x,y)$，$k=1,2,3,\cdots,K$，即

$$S=\bigcup_{k=1}^{K} S_k(x,y) \quad 1\leqslant x\leqslant 4, 1\leqslant y\leqslant 4 \tag{15}$$

并对每块系数矩阵 $S_k(x,y)$ 分别进行奇异值分解，得到每一个子块的奇异值矩阵 $\Sigma_k(k=1,2,3,\cdots,K)$，其中

$$\Sigma_k=\begin{bmatrix}\sigma_1 & & & \\ & \sigma_2 & & \\ & & \sigma_3 & \\ & & & \sigma_4\end{bmatrix} \tag{16}$$

Step5 将水印图像逐行扫描成一个一维的序列。这里选用了一个正方形的水印图像 $F(N_w\times N_w)$，扫描后长度为 I $(I=N_w\times N_w)$，记为 $W=\{w_i, 1\leqslant i\leqslant I\}$。

Step6 利用各块的第二个奇异值来嵌入水印信息，即

$$\tilde{\sigma}_{i,2}=\sigma_{i,2}+\alpha_i w_i \quad (i=1,2,3,\cdots I, I\leqslant K) \tag{17}$$

其中，$\sigma_{i,2}$ 表示第 i 个子块的奇异值矩阵中的第二个奇异值，α_i 表示水印的嵌入强度，w_i 是水印序列中第 i 个水印信息。如果水印序列的值不适合直接代入，也可以先进行一次映射，这里统一用 w_i 表示。$\tilde{\sigma}_{i,2}$ 表示嵌入水印信息后的第 i 个子块的奇异值矩阵中的第二个奇异值。

Step7 将 $\tilde{\sigma}_{i,2}$ 带回到子块矩阵 Σ_i 中，进行 SVD 重构，得到嵌入水印后的采样矩阵 $\tilde{S}$。

Step8 将 $\tilde{S}$ 中的数据按照采样位置回填到原来的幅度谱中。由于 DFT 系数具有共轭对称性，回填完数据后，需要按照式(13)，在对称点进行同样的修改。

Step9 进行逆离散傅立叶变换，生成嵌入水印后的图像 $\tilde{G}(N\times N)$。

Step10 保存嵌入过程的中间文件，其中包括采样起始距离和终止距离参数 d_1 和 d_2、分块大小参数 M(这里是 4)、嵌入强度 α_i 和 I 个奇异值矩阵的第二个分量 $\sigma_{i,2}(i=1,2,3,\cdots I)$，作为提取水印时候的参数。并发布含水印的图像。

3.4 水印提取算法

水印的提取过程是加入水印过程的逆过程，利用中间文件的参数，将待测图像分块，提取次大奇异值，然后提取水印信息，并进行比较。设待验证的图像为 G'，水印提取步骤如下。

Step1 对图像 G' 进行 DFT 变换，计算幅度谱，并对幅度谱中心化。

Step2 根据采样起始距离和终止距离参数 d_1 和 d_2 确定采样范围，采样并按照分块参数 M 分块。

Step3 对各个分块进行奇异值分解，得到每块奇异值分解的次大值 $\sigma'_{i,2}(i=1,2,3,\cdots,I)$，并提取第 i 块中包含的水印信息 w_i'，即

$$w_i'=(\sigma'_{i,2}-\sigma_{i,2})/\alpha_i \tag{18}$$

Step4 将得到的 $W'(W'=\{w_i', i=1,2,3,\cdots,I\})$ 序列重新排序，变成二维图像 $F'(N_w\times N_w)$。

Step5 利用式(19)计算原始水印 F 和提取水印 F' 之间的标准相关系数 NC。

$$NC=\frac{\sum_{i=1}^{N_w}\sum_{j=1}^{N_w}(F'(i,j)-\bar{F}')(F(i,j)-\bar{F})}{\sqrt{\sum_{i=1}^{N_w}\sum_{j=1}^{N_w}(F'(i,j)-\bar{F}')^2}\sqrt{\sum_{i=1}^{N_w}\sum_{j=1}^{N_w}(F(i,j)-\bar{F})^2}} \tag{19}$$

Step6 设定相关系数的参考门限 P。如果相关系数大于参考门限，则表明包含水印，反之则还需要返回 Step2，重新提取一次水印信息。Step2 中采样数据的重组方法在 3.1 节中已有详细介绍。再次进行水印检测后，如果还判定为不包含水印，则可以认定该检测图像不包含匹配的水印信息。

4 实验与分析

为了检验本方法的性能，使用 512×512 的 Baboon 图像作为测试图像，图 5 作为有意义的图像水印进行了测试。

图 5 水印图像(32×32)

测试中，主要测试水印算法在不同攻击下表现的性能，检验算法抵抗不同几何攻击的能力，测试结果以提取出的水印与原水印图像之间的标准化相关系数作为比较的指标。由于篇幅有限，这里只给出嵌入水印后的结果图，如图 6 所示。

图 6 嵌入水印后的结果图

其它攻击下的测试结果如表 3 所列。

表 3 攻击测试结果

攻击类型	NC	攻击类型	NC
无攻击	0.9999	平移	0.8012
旋转 45°(带剪切)	0.6834	循环平移	0.8635
旋转 45°(不带剪切)	0.8322	添加高斯噪声	0.8668

缩小 20%	0.7921	添加椒盐噪声	0.8579
放大 25%	0.8661	添加乘性噪声	0.8645
条状剪切	0.8532	中值滤波	0.6452
块状剪切	0.8379	维纳滤波	0.6673

从表 3 的测试结果中可以看出，嵌入水印之后，无任何攻击的情况下，提取出的水印相关系数为 0.9999，基本与原图相同。之后对图像进行了常见的几何攻击，包括不同形式的旋转、缩放、剪切和平移，以及一些加噪、滤波处理。从测试结果中可以发现，带剪切的旋转效果明显弱于不带剪切的旋转结果；缩小的结果弱于放大的结果，这些都是由于一些几何攻击在攻击过程中丢失了部分原始数据而造成的。鉴于随着数据的丢失，图像的实际意义也会跟着下降，失去使用价值，所以实验结果还是可以接受的。

结束语 本文从构造几何攻击不变域抵抗几何攻击的思路出发，提出了一种改进的基于奇异值分解的抗几何攻击的数字图像水印算法。

通过对图像奇异值分解的特性进行分析和研究，提出了以奇异值矩阵中次大值点作为水印的最优嵌入位置。并改进现有的分块奇异值分解嵌入方法，提出了一套在 DFT 变换域的类之字形采样方案，详细设计了采样起始和终止位置、采样顺序及数据矩阵的构建方式，有效提高了水印系统的安全性，并解决了分块后无法抵抗旋转攻击的问题，降低了水印检测过程的复杂度。并且，本方案与原有的奇异值分解方法相比，彻底消除了对 U,V 矩阵的依赖，抗干扰能力更强。实验证明，本文提出的水印算法，对于抵抗常见的几何攻击是有效的。

参 考 文 献

[1] Liu R Z, Tan T N. An SVD-based watermarking scheme for protecting rightful ownership[J]. IEEE Transaction on Multimedia, 2002, 4(1): 121-128

[2] Shieh Jieh-Ming, Lou Der-Chyuan, Chang Ming-Chang. A semi-blind digital watermarking scheme based on singular value decomposition[J]. Computer Standards and Interfaces, 2005, 28(4): 428-440

[3] Zhang Zhi-Ming, Wang Lei. A novel SVD watermarking method with turbo code enhanced robustness[C]// Proc. of the Intl. Computer Congress 2004 on Wavelet Analysis and its Applications, and Active Media Technology. v1, 2004

[4] 吕英华，王巍，孔俊，等. 基于 SVD 和神经网络的鲁棒水印算法[J]. 计算机科学，2005，32(12)：232-235

[5] Ganic E, Eskicioglu A M. Robust DWT-SVD domain inage watermarking: embedding data in all frequencies[C]// Proc. of the 2004 Multimedian and Security Workshop on Multimedian and Security. 2004: 166-174

[6] 刘峰，孙林军. 一种基于 DCT 和 SVD 的数字图像水印技术[J]. 计算机应用，2005，25(8)：1944-1946

[7] 黄松，张伟，陈军，等. 一个基于 DWT 的自适应数字水印算法[J]. 计算机科学，2006，33(7)：155-157

[8] 周波，陈健. 基于奇异值分解的抗几何失真的数字水印算法[J]. 中国图像图形学报，2004，9(4)：507-509

[9] 李海峰，王树勋，温泉，等. 基于分块 SVD 和 Zernike 矩的鲁棒图像水印[J]. 模式识别与人工智能，2005，18(3)：359-365

(上接第 122 页)

应像素的计算，不会对互换集有太大影响，但可以显著提高计算时间性能。

3) 用互换集对 lena 图像进行像素互换，进行了互换前后的图像块广义概率分布比较实验，验证了互换前后的图像块广义概率分布不发生变化。由于 $\delta=1$，互换前后的图像在视觉上没有任何变化。将 lena 图像第 1 图像块 EXC 集合的 1653 个互换对都进行像素位置互换，这是图像块失真的极限，对应的峰值信噪比为

$$PSNR=-10\lg\left\{\frac{1}{255^2MN}\sum_{m=1}^{M}\sum_{n=1}^{N}[d(m,n)]^2\right\}$$

$$=-10\lg\left\{\frac{2\times1653}{255^2\times64\times64}\right\}=112.97\text{dB}$$

人眼只能判别出 $PSNR\leqslant38$dB 失真的图像[5]，所以人眼无法判断出互换所产生的图像失真。

为了使以后的研究者能进行数据比较，将 lena 图像第 1 图像块的前几个互换对的数据按顺序给出，如表 2 所列。

表 2 互换对的数据表

互换对	像素	依赖像素数	变化符号集
x(1,45) x(14,46)	x(1,45)=3	1,0,1	{1} - - -
	x(14,46)=4	0,1,2	- {6} - {3}
x(1,52) x(2,47)	x(1,52)=1	1,0,1	- - - -
	x(2,47)=2	0,1,2	- - - {1}
x(1,58) x(54,56)	x(1,58)=123	1,0,1	- - - -
	x(1,52)=122	1,1,0	{120} - - -

依赖像素数的 3 个值依次对应 x_{-1},x,x_{+1} 的依赖像素个数。变化符号集的 4 个值依次对应 $X_{+1}^{+},X_{+1}^{\pm},X_{-1}^{-},X_{+1}^{-}$。

结束语 通过对图像相邻像素的相关性进行分析，给出了基于广义信息熵的安全约束条件，改善了基于香农信息熵的信息隐藏安全模型的不足之处。所提出的信息隐藏的安全约束条件和方法，具有理论和实际的意义。但所提出的广义信息熵是否是理论上最佳的，还有待进一步研究。另外，δ 值的确定与图像的视觉感知模型有关，目前还没能在理论上解决，只能通过实验来确定。

参 考 文 献

[1] Cachin C. An information-theoretic model for steganography[C]// Proceeding of Second International Workshop on Information Hiding. Lecture Notes in Computer Science. 1998: 306-318

[2] Mittelholzer T. An information-theoretic approach to steganography and watermarking[C]// Preliminary Proceedings of the Third Inter-national Information Hiding Workshop. Dresden, Germany, 1999: 1-15

[3] 林代茂，胡岚，郭云彪，等. 广义信息隐藏技术的安全问题[J]. 中山大学学报，2004，43(2)：14-16

[4] 鲁晨光. 广义熵和广义互信息的编码意义[J]. 通信学报，1994，15(6)：37-44

[5] Petitcolas F A P, Anderson R J. Evaluation of Copyright Marking Systems[C]// Proc. IEEE Multimedia Systems. Italy: Florence, June 1999: 574-579