E-mail: jig@radi.ac.cn
Website: www.cjig.cn
Tel: 010-64807995

中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS

中图法分类号: TN911.7　　**文献标识码**: A　　**文章编号**: 1006-8961(2017)03-0288-09

论文引用格式: Xiao Z J, Zhang H, Chen H, Gao T. Zero-watermarking based on boost normed singular value decomposition and cellular neural network [J]. Journal of Image and Graphics, 2017, 22(3): 0288-0296. [肖振久, 张晗, 陈虹, 高婷. 增强奇异值分解和细胞神经网络的零水印 [J]. 中国图象图形学报, 2017, 22(3): 0288-0296.] [DOI: 10.11834/jig.20170302]

增强奇异值分解和细胞神经网络的零水印

肖振久, 张晗, 陈虹, 高婷

辽宁工程技术大学软件学院, 葫芦岛　125105

摘　要: **目的**　针对奇异值分解算法存在的对角线失真、虚警错误等问题, 引入一个寻找最抗攻击缩放比例的参数, 提出基于增强奇异值分解的零水印算法。**方法**　首先将离散小波变换作用于原始图像, 对分离出的低频逼近子图进行不重叠分块, 对分块后的低频逼近子图作离散余弦变换得到低频系数矩阵, 再分别对每个块矩阵进行增强奇异值分解, 将得到的最大奇异值与最大奇异值均值作比较构成特征向量; 然后对水印图像进行 Arnold 变换和 Logistic 映射得到置乱加密后的水印图像; 最后将特征向量和置乱加密后的水印图像分别作为细胞神经网络的起始值和控制输入值, 通过设定细胞神经网络的反馈模板、控制模板以及阈值来确定具体的可逆逻辑运算。经过可逆逻辑运算处理后的细胞神经网络输出图像即为零水印的注册图像。将注册图像保存到认证中心以证明对图像作品的版权。**结果**　在 JPEG 压缩、噪声、滤波、旋转以及剪切等各种攻击下, 提取的水印和原始水印的归一化相关值都在 96% 以上, 算法平均运行时间为 2.389 s, 性能较高。**结论**　通过利用参数对奇异值矩阵进行调整的方法, 不仅增强了算法的鲁棒性, 而且解决了奇异值分解(SVD)出现的对角线失真和虚警错误问题。同时通过结合零水印的思想, 解决了传统水印算法需在载体图像中嵌入水印而导致的水印不可见性与鲁棒性之间的矛盾。

关键词: Arnold 变换; 增强奇异值分解; 细胞神经网络; 离散小波变换; 离散余弦变换; Logistic 映射; 零水印

Zero-watermarking based on boost normed singular value decomposition and cellular neural network

Xiao Zhenjiu, Zhang Han, Chen Hong, Gao Ting

College of Software, Liaoning Technical University, Huludao　125105, China

Abstract: **Objective** Numerous illegal pirating sites and programs have emerged with the rapid development of digital network technology because digital media can be easily copied and tampered with. Digital watermarking technology, which is an effective solution to image copyright protection, content authentication, integrity, and other issues, has become a crucial research topic in recent years. The singular values of images received via singular value decomposition (SVD) are strongly resistant to various attacks. Therefore, scholars have proposed various SVD-based watermarking methods. We proposed the novel boost normed singular value decomposition (BN-SVD) to solve the problems of diagonal distortion and false positives, which are caused by SVD. The method involves establishing a parameter to identify the optimum scaling factor for efficient robustness to improve existing SVD algorithms. Considering the inconsistencies between invisibility and robustness caused by embedding watermarks in original images by traditional watermarking algorithms, a novel zero-watermarking scheme

收稿日期: 2016-09-22; **修回日期**: 2016-11-30

基金项目: 国家自然科学基金项目(61540056)

第一作者简介: 肖振久(1968—), 男, 副教授, 2004 年于辽宁工程技术大学获计算机应用技术专业工学硕士学位, 主要研究方向为网络与信息安全、图像与视觉信息计算、数字水印。E-mail: 845585097@qq.com

Supported by: National Natural Science Foundation of China (61540056)

based on BN-SVD is proposed. Zero-watermarking is defined by the registration and certification processes. In registration, an algorithm uses the major characteristics of a digital image to construct zero-watermarking registration information. The information is stored in a centralized authentication center. In certification, the watermark information is restored by using the digital images to be certified and the data stored in a centralized authentication center. **Method** First, a low-frequency approximation sub-graph was established from an original image that was decomposed by discrete wavelet transform (DWT) to non-overlapping image blocks. The low-frequency approximation sub-graph generated a low-frequency coefficient matrix via discrete cosine transform (DCT). BN-SVD was used to each block matrix to achieve a maximum singular value. A characteristic vector was created by comparing the maximum singular value with the average of the maximum singular value. The watermark image was disposed with Arnold transformation and Logistic map to obtain an encrypted and scrambling watermark image. Finally, the characteristic vector was set as an initial value and the scrambling encrypted watermark image as a controlling input value are both sent into a cellular neural network (CNN). By setting up a feedback template, the control template and threshold value of CNN determined the specific reversible logic operation. The output image was the registration image of zero-watermarking. The registration image was saved in the certification center to verify the copyright of the image. **Result** Experimental results indicated that all watermark images extracted by the proposed method do not exhibit diagonal marks when heterogenic attacks are imposed on original images. The proposed method overcame the diagonal distortion problem in the diagonal experiment. A one-to-one relation between the singular value vector and the image was established by introducing a parameter where different images have various singular value vectors. Therefore, the major characteristic of different images can be represented by different singular value vectors in a false-positive rate experiment. The normalized correlation between the extracted watermark image from BN-SVD and the original watermark image was below 50%. A low false-positive rate was observed. In the robustness experiment, we imposed various types of attacks, including JPEG compression, noise, filtering, rotating, and shear on the images. In the JPEG compression attack, the normalized correlation reached up to 99%. In the noise attack, the normalized correlation exceeded 97%. In the filter attack, the normalized correlation exceeded 98%. In the rotating attack, the normalized correlation was higher than 96%. In the shear attack, the normalized correlation exceeded 98%. These results indicated the need to improve high-shear attacks. **Conclusion** A parameter will be used to modify the singular values of a matrix, which enhances the robustness of the algorithm and eliminates the false-positive and diagonal distortion problems of SVD. Introducing CNN is advantageous because the attacker cannot determine specific parameters. Therefore, the attacker extract the watermark image by reversible logic operation to improve the security of the watermarking. The parallel image processing of CNN can be achieved with hardware, which makes the algorithm applicable in occasions with higher real-time requirement.

Key words: Arnold transform; boost normed singular value decomposition (BN-SVD); cellular neural network (CNN); discrete wavelet transform (DWT); discrete cosine transform (DCT); Logistic map; zero-watermarking

0 引 言

由于数字网络技术的迅速发展，数字媒体可以被轻易地复制和篡改，导致了大量非法盗版的出现[1-2]。数字水印技术作为一种有效解决图像版权、内容认证和完整性保护等问题的新型技术，近年来成为研究的热点[3]。

针对数字水印鲁棒性和透明性之间的矛盾，2003 年温泉等人[4]提出了零水印算法，其基本思想是将数字图像版权保护分为注册与认证两个过程，在注册过程中，算法主要利用数字图像的重要特征来构造水印，将其存放在集中认证中心，认证过程是利用待认证的数字图像与保存在集中认证中心的数据来恢复水印信息。

由于图像奇异值分解后的奇异值对各种攻击具有一定的抵抗能力，一部分学者提出了基于奇异值分解的水印方法。刘瑞桢等人[5]于 2001 年将奇异值分解理论首次应用于数字水印系统中，该方法将水印图像嵌入到载体图像的奇异值中。刘丽等人[6]提出了基于离散余弦变换(DCT)和奇异值分解(SVD)的 QR 码数字水印算法，能够很好地抵抗常见信号处理和图像处理的攻击，但在水印图像重建时存在着对角线失真问题。张飞艳等人[7]提出了 Contourlet-SVD 的稳健性数字水印算法，将水印信息以不同的强度值分别嵌入到能量最大方向子带

和能量最小方向子带的奇异值中，也取得了较好的效果，但是利用水印的提取算法，在与版权图像毫无关系的其他图像中也能提取出相似度很高的水印图像，表明水印算法存在严重的虚警错误。叶天语[8]提出基于方差的奇异值分解鲁棒零水印算法，对中值滤波有所改善，但抗剪切攻击的能力很弱。曲长波等人[9]提出了基于位平面理论和奇异值分解的鲁棒零水印算法，在抵抗噪声、滤波、剪切、JPEG 压缩方面都表现出一定的鲁棒性，但是提高效果不显著。为解决文献[6]存在的对角线失真和文献[7]存在的严重虚警错误问题，本文借鉴文献[10]，结合离散小波变换(DWT)和离散余弦变换(DCT)，从 DWT 扩展到 DWT-DCT 混合变换，提出了一种基于细胞神经网络应用 DWT-DCT 混合变换和 BN-SVD[11]的零水印算法。当对图像施加小的扰动时图像的奇异值无显著变化，说明图像的奇异值具有较好的稳定性[12]。对奇异值矩阵进行改进，增大奇异值并将其界定在一定范围内，使其稳定性更强。解决了水印提取时的对角线失真和虚警错误问题，提高了数字水印的鲁棒性。

1 算法的理论基础

1.1 奇异值分解

奇异值分解(SVD)是一种实现矩阵对角化的有效数值分析工具，广泛应用于图像处理领域。假设数字图像 I 大小为 $n\times n$，对其进行奇异值分解，则正交矩阵 $U_{n\times n}$、$V_{n\times n}$和对角矩阵 $S_{n\times n}$存在关系

$$\boldsymbol{A} = \boldsymbol{USV}^{\mathrm{T}} \tag{1}$$

式中，U 和 V 是正交矩阵，$S=\mathrm{diag}(\sigma_i)$是一个非对角元素均为 0 的矩阵，其对角线上的元素值 $\sigma_i(i=1,2,\cdots,r)$满足 $\sigma_1\geqslant\cdots\geqslant\sigma_r>0$。

奇异值分解存在以下缺陷：

1) 存在对角线失真问题。由于奇异值分解算法自身特性，使提取出来的水印往往会产生严重的对角失真。如果在带有水印标记的主图像被直接修改时，从被攻击的图像中提取的水印图像会产生对角线失真。

2) 存在虚警错误问题。对数字图像 I 进行 SVD，则存在正交矩阵 $U_{n\times n}$、$V_{n\times n}$，矩阵 $U_1V_1^{\mathrm{T}}$，$U_2V_2^{\mathrm{T}},\cdots,U_nV_n^{\mathrm{T}}$为矩阵空间的一组正交基，称为特征图像。因此，图像的奇异值向量所在的基空间是由图像本身内容所决定的，奇异值向量反映图像在不同特征图像下的亮度信息，相应的正交矩阵反映图像的几何结构。所以，图像与奇异值向量之间不存在一一对应的关系，即不同的图像可以有相同的奇异值向量，而图像的奇异值向量体现不出图像的结构特征。这就造成了当采用图像的奇异值向量嵌入水印信息时，在未嵌入水印信息或者其他随机图像中也可以提取出所需要的水印信息，增加了水印提取的虚警率，这使得算法的可靠性大大降低。

1.2 增强奇异值分解

为了克服上述两个问题，提出了一种改进的奇异值分解，将其命名为增强奇异值分解(BN-SVD)。此方法定义了一个参数 β，使在奇异值分解后获得的奇异值均匀化，解决了对角线问题并且增强了算法的鲁棒性。对大小为 $n\times n$ 的数字图像 I 进行增强奇异值分解，则存在正交矩阵 $U_{n\times n}$、$V_{n\times n}$和对角矩阵 $S_{n\times n}$使得

$$\boldsymbol{B} = \boldsymbol{U}*(\boldsymbol{S})^{\beta}*\boldsymbol{V}^{\mathrm{T}},\quad 0<\beta<1 \tag{2}$$

式中，矩阵 u_i 是矩阵 U 的左奇异矩阵，列矩阵 v_i 是矩阵 V 的右奇异矩阵。

增强奇异值分解实现途径如下：增强奇异值分解是在奇异值分解的基础上，对数字图像 I 进行奇异值分解后，对对角矩阵 $S_{n\times n}$做 β 次幂运算。处理不同的数字图像时，根据图像固有信息合理调整参数 β，使其达到最佳的抗攻击效果。

引入参数 β 的作用：

1) 寻找最佳抗攻击的缩放比例，放大图像奇异值，以减少受攻击时图像矩阵的敏感性，从而提高算法的鲁棒性；

2) 将奇异值限定在一定范围内，使对角线方向上的灰度均衡化，进而解决对角线失真问题；

3) 将奇异值向量特殊化，使其与图像存在一一对应关系，可代表图像特征，进而解决虚警错误问题。

1.3 细胞神经网络

细胞神经网络(CNN)是在 1988 年 Chua 和 Yang 等人提出的一种面向硬件实现的非线性神经网络模型，是由具有相同动力学性质的细胞组成的一个 2 维、3 维或 n 维有规则排列的处理器阵列。一个标准的 CNN 模型的结构，其基本单元称为细胞，第 i 行，第 j 列的细胞用 C_{ij}表示，细胞之间的连线表示所连接的细胞之间的相互作用。与 Hopfield

神经网络的全连接结构不同，CNN 的细胞是局部互连的，每一个细胞 C_{ij} 仅与它的邻域 $N_{ij}(r)$ 中的细胞相连，这些相连的细胞通过权重直接相互作用，而不直接相连的细胞则通过网络的连续动态动力学传输效应间接地相互作用[13]。

对一个 $M \times N$ 的 CNN 模型，其每一个细胞 $C_{ij}(1 \leqslant i \leqslant M, 1 \leqslant j \leqslant N)$ 都有一个恒定的外界输入 u_{ij}、一个阈值 t_{ij}、一个状态变量 x_{ij} 和一个输出 y_{ij}，各神经元运算的数学模型可以描述为

$$x_{ij} = -x_{ij} + \sum_{kl \in N_{ij}(r)} A_{kl} y_{kl} + \sum_{kl \in N_{ij}(r)} B_{kl} u_{kl} + t_{ij} \quad (3)$$
$$i = 1, \cdots, M; j = 1, \cdots, N$$

式中，x_{ij} 为细胞 C_{ij} 的当前状态，u_{kl} 和 y_{kl}，分别为各细胞的初始输入值和当前输出值；$N_{ij}(r)$ 表示细胞 C_{ij} 半径为 r 的邻域；C_{kl} 表示细胞 C_{ij} 的 r 邻域内的细胞；B_{kl} 表示邻域细胞 C_{kl} 的输入 u_{kl} 与细胞 C_{ij} 之间的连接权，称为控制模板；A_{kl} 表示邻域细胞 C_{kl} 的输出 y_{kl} 与细胞 C_{ij} 之间的连接权，称为反馈模板；t_{ij} 为 C_{ij} 内部的阈值电流。

神经元的输出方程可以描述为

$$y(x_{ij}) = 0.5(|x_{ij} + 1| - |x_{ij} - 1|) \quad (4)$$

图像中的每一个像素与 CNN 中相同位置上的一个细胞相对应，每一个像素的灰度值对应于相同位置上细胞的输入 u_{ij}；对于标准 CNN，其输入 u_{kl}，状态 x_{ij}，与输出 y_{kl} 来的关系由反馈模板 A 与控制模板 B 以及阈值 t 来确定。CNN 不同的功能主要决定于模板参数的设计。设定不同的模板及阈值，CNN 并行处理器可以实现不同的图像处理功能。CNN 模板库中存在着大量的模板，例如 $\boldsymbol{A}$，$\boldsymbol{B}$ 均取 3×3 大小，假设图像 $\boldsymbol{P}_1$ 为起始值，假设图像 $\boldsymbol{P}_2$ 为控制输入值，当

$$\boldsymbol{A} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \boldsymbol{B} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, t = -1$$

时，获得的输出即为 $\boldsymbol{P}_1$ 和 $\boldsymbol{P}_2$ 相“与”。常见的简单模板可以完成图像“与”、“或”、“非”等操作，还可以组合模板来实现更复杂的图像处理过程[14]。使用细胞神经网络进一步提升了水印的安全性。

引入细胞神经网络的作用：一般的零水印算法大多采用将水印图像和特征向量做异或等可逆逻辑运算来进行水印检测密钥的生成。然而当算法受到攻击后，可直接通过逻辑逆运算得到水印图像，水印的安全性不高。本文采用细胞神经网络，通过反馈模板 $\boldsymbol{A}$ 与控制模板 $\boldsymbol{B}$ 以及阈值 t 来确定不同的逻辑运算，当攻击者无法确定 $\boldsymbol{A}$、$\boldsymbol{B}$、t 的具体设定参数时，就无法通过可逆逻辑运算提取出水印图像，提高了水印的安全性。

2　零水印算法设计

2.1　水印图像的预处理

水印图像的预处理采用 Arnold 变换进行一次加密。该变换的核心思想是通过改变像素点之间的位置关系来消除像素空间的相关性[15]，进而达到图像加密的效果，提高水印的安全性。

Arnold 变换是数学家 Arnold 在遍历理论的研究中提出的一类剪裁变换，俗称“猫脸变换”(cat mapping)[16]。2 维 Arnold 变换可写为

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ N) \quad (5)$$
$$x, y \in \{0, 1, \cdots, N-1\}$$

式中，(x, y) 是像素在原始图像的坐标，(x', y') 是变换后该像素在新图像的坐标，N 是数字图像矩阵的阶数，即图像的大小。

水印图像进行 Arnold 变换后，采用 Logistic 映射进行二次加密。混沌系统具有遍历性、初值敏感性和伪随机性等良好的特性，非常适合应用到图像加密领域。目前被广泛研究的 Logistic 映射是一种形式简单的 1 维混沌系统[17]，其定义为

$$x_{k+1} = \mu x_k (1 - x_k) \quad (6)$$
$$0 \leqslant \mu \leqslant 4, x_k \in (0, 1), k = 0, 1, 2, 3, \cdots$$

该系统对初值敏感，所生成的混沌序列具有非周期性和不收敛性，当参数范围在 3.569 945 6 $\leqslant \mu \leqslant$ 4 时，Logistic 映射处于混沌状态，进一步增强了水印安全性。

2.2　零水印的构造

零水印构造过程如图 1 所示。

选取 $N \times N$ 大小的灰度图像 $\boldsymbol{I}$ 为载体图像和 $(N/16) \times (N/16)$ 大小的二值图像 $\boldsymbol{W}$ 为水印图像。

零水印构造步骤如下：

1）将原始载体图像 $\boldsymbol{I}$ 进行一级 DWT，得其低频逼近子图 $\boldsymbol{P}$。

2）对所得到的低频逼近子图 $\boldsymbol{P}$ 进行分块，分割为 $(N/16) \times (N/16)$ 个 8×8 大小互不重叠图像子

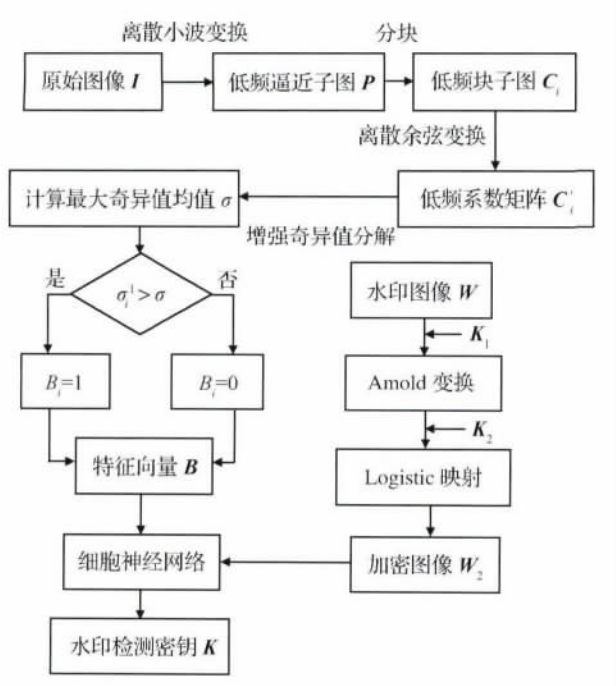

图 1　零水印构造图

Fig. 1　Zero watermark structure diagram

块 $C_i(i=1,2,\cdots,(N/16)\times(N/16))$。

3）对分块后的低频逼近子图 C_i 进行 DCT，进行 ziazag 扫描，提取每块 64 个系数中的前 16 位，然后反 zigzag 扫描，生成一个 4×4 的低频系数矩阵 $C'_i(i=1,2,\cdots,(N/16)\times(N/16))$。

4）对每个图像子块 C'_i 进行 BN-SVD，即 $L_i = U_i(S_i)^{\beta}V^{\mathrm{T}}(0<\beta<1)$。式中 U_i 和 V_i 为正交矩阵，S_i 为对角阵，$\sigma_i^k(k=1,2,\cdots,r)$ 为第 i 个低频系数矩阵 C'_i 的奇异值。从对角矩阵 S_i 中提取第 1 个奇异值，共提取出 $(N/16)\times(N/16)$ 个最大奇异值，记作 $\sigma_i^1(i=1,2,\cdots,(N/16)\times(N/16))$。

5）求 $(N/16)\times(N/16)$ 个最大奇异值的均值，$\sigma=\mathrm{mean}(\sigma_i^1)$ 根据与 σ_i^1 的大小关系产生特征向量 B，即

$$B_i=\begin{cases}1 & \sigma_i^1>\sigma\\ 0 & \text{其他}\end{cases}\tag{7}$$

6）对水印图像 W 进行 Arnold 置乱，得到水印图像 W_1 和密钥 K_1，然后对水印图像 W_1 进行 Logistic 映射，得到水印图像 W_2 和密钥 K_2。

7）将特征向量 B 作为细胞神经网络的起始值，置乱加密后的水印图像 W_2 作为细胞神经网络的控制输入值，设定反馈模板 A 与控制模板 B 以及阈值 t，经过一定的可逆运算处理后的输出图像即为代表原始载体图像版权信息的水印检测密钥 K。

最后，将原始图像载体检测密钥 K 和相应的时间戳注册到认证中心以证明对图像作品的版权。

2.3　零水印的检测

零水印检测过程如图 2 所示。

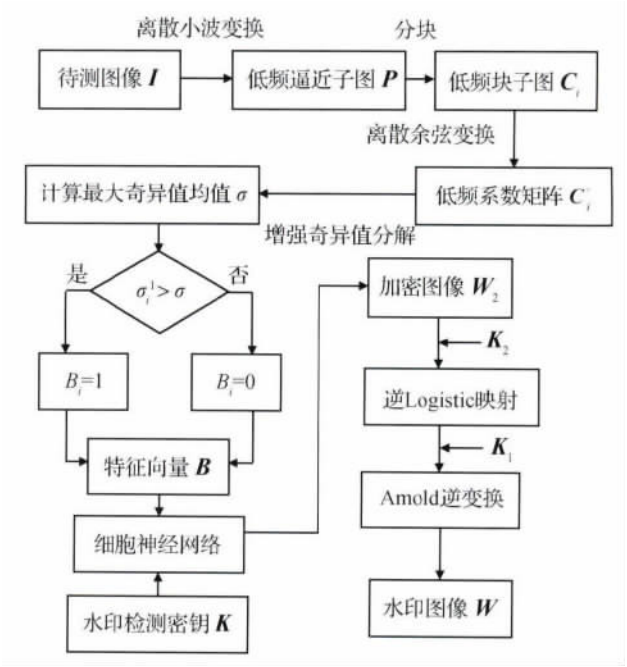

图 2　零水印检测图

Fig. 2　Zero watermark detection diagram

选取 $N\times N$ 大小的灰度图像 I' 为载体图像和 $(N/16)\times(N/16)$ 大小的二值图像 W 为水印图像。

零水印检测步骤如下：

对待测图像 I' 进行上述零水印构造步骤 1）—5）操作。然后将得到的特征向量作为细胞神经网络的起始值，代表原始载体图像版权信息的水印检测密钥 K 作为细胞神经网络的控制输入值，反馈模板 A 与控制模板 B 以及阈值 t 为构造零水印时设定的模板参数。经过一定的可逆运算处理后输出置乱加密后的水印图像 W_2。

最后，利用密钥 K_1、K_2 对置乱加密后的水印图像 W_2 进行逆 Logistic 映射和 Arnold 逆变换得到原始水印图像 W。

3　仿真实验及结果分析

3.1　实验环境及参数说明

为了验证本文算法的有效性和可行性，采用 Matlab R2014a 的实验平台。选取如图 3（a）—（c）3 幅灰度图像作为原始载体图像，其大小为 512×512

像素，图像 Lena 有较小的细节，纹理信息少；图像 Plane 的细节信息和纹理信息相对较复杂；图像 Bridge 的细节信息比较均匀，纹理信息比较多；选取相对复杂的“辽宁工大”作为有意义的二值水印如图 3(d)，其大小为 32×32 像素。为达到较好的置乱效果，Arnold 置乱次数 $n = 20$；Logistic 映射参数 $\mu = 3.654$ 和初值 $x_0 = 0.54$，仿真过程中采用归一化互相关(NC)函数来评价提取的水印与原水印的相似度，即

$$NC(x_1, x_2) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} x_1(i,j)\,x_2(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} x_1(i,j)^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} x_2(i,j)^2}} \tag{8}$$

式中，x_1、x_2 分别表示初始水印和提取出的水印。

3.2　实验结果

3.2.1　对角线问题实验测试

文献[6]对原始图像施加攻击实验后，所提取的水印图像上有明显的对角线痕迹如图 4(b)所示。

对待测图 3(a)分别施加不同类别的攻击，实验后采用 BN-SVD 提取水印如图 5 所示，从图 5(a)—(f)可以看出，水印图像无明显对角线痕迹。实验表明本算法克服了对角线失真问题。

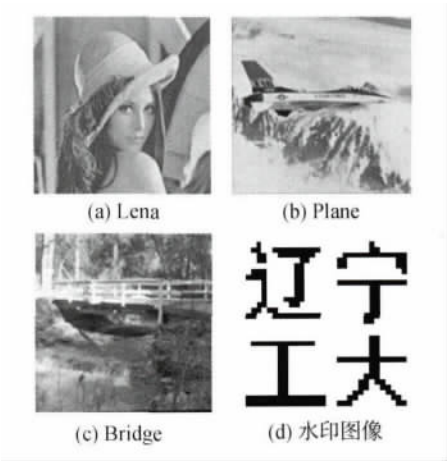

图 3　原始图像和水印图像

Fig. 3　Original and watermark images ((a) Lena; (b) Plane; (c) Bridge; (d) watermark image)

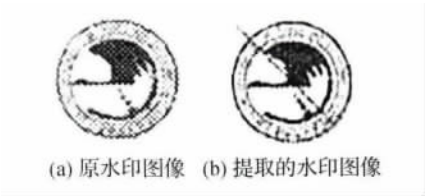

图 4　原水印图像和受攻击后提取的水印图像

Fig. 4　Original watermark image and attacked extract watermark images ((a) original watermark image; (b) extraction of watermark image)

图 5　受攻击后的原始图像和提取的水印图像

Fig. 5　Attacked original and extract watermark images ((a) compression strength = 20; (b) median filter 3×3; (c) intensity of gaussian noise = 0.05; (d) intensity of salt & pepper noise = 0.05; (e) shear picture 1/4; (f) rotate 1 degree)

3.2.2 虚警率问题实验测试

首先通过原始图像图6(a)和原始水印图6(b)构造水印密钥,然后对与原始图像相似度较高的伪随机图像分别用BN-SVD算法和SVD算法提取图像特征向量与水印密钥进行可逆逻辑运算,提取出水印图像。由图6(c)可知,当伪随机图像采用SVD算法提取水印图像时,也可以提取出正确的水印图像(明文),虚警率高。由图6(d)可知,当采用BN-SVD算法提取水印图像时,在无法确定参数β的值的情况下,就无法提取出正确的水印图像(密文),降低了算法的虚警率。引入参数β后,奇异值向量与图像便存在了一一对应关系,即不同的图像存在不同的奇异值向量,因此图像的奇异值向量便可体现图像的特征,解决了虚警错误问题。

图6 采用2种算法提取的水印图像

Fig. 6 Using two kinds of algorithms to extract watermark images ((a) original images; (b) original watermark images; (c) SVD algorithm; (d) BN-SVD algorithm)

为验证上述虚警率问题,表1给出了分别采用BN-SVD算法和SVD算法进行上述实验后所提取的水印图像和原始水印图像的NC值对比。

由表1可知,采用BN-SVD算法提取出的水印图像和原始水印图像的归一化相关值在0.5以下,说明本文算法虚警率较低。

表1 两种算法的NC值对比

Table 1 Two algorithms of NC value contrast

图像	BN-SVD算法	SVD算法
Lena	0.357 8	0.996 2
Plane	0.337 4	0.994 9
Bridge	0.315 9	0.989 9

3.2.3 BN-SVD和SVD的鲁棒性对比实验

为验证采用BN-SVD算法具有较强的鲁棒性,对待测图3(a)—(c)分别施加不同类别的攻击实验,包括JPEG压缩、噪声攻击、滤波攻击、旋转攻击和剪切攻击。表2给出了3幅待测图像在经受攻击

表2 待测图像受攻击BN-SVD和SVD提取水印NC值对比

Table 2 Under attacked test image BN-SVD and SVD extracted watermark NC value contrast

攻击方式	参数	算法	Lena	Plane	Bridge
JPEG压缩	20	SVD	0.996 2	0.987 4	0.997 5
		BN-SVD	0.998 7	0.996 2	0.998 7
滤波	3×3中值滤波	SVD	0.992 4	0.997 5	0.993 7
		BN-SVD	1	0.996 2	0.998 7
噪声	椒盐噪声0.05	SVD	0.988 6	0.989 9	0.993 7
		BN-SVD	0.992 4	0.991 2	0.993 7
	高斯噪声0.05	SVD	0.973 5	0.973 5	0.978 5
		BN-SVD	0.991 2	0.988 6	0.987 4
旋转	向右1°	SVD	0.962 1	0.958 3	0.965 9
		BN-SVD	0.986 1	0.969 7	0.977 3
剪切	左上角1/64	SVD	0.957 1	0.982 3	0.973 5
		BN-SVD	1	0.983 6	0.988 6

后分别用 BN-SVD 和 SVD 所提取的水印 NC 值。

从表 2 可以看出，与使用 SVD 相比，使用 BN-SVD 所提取的水印 NC 值得到显著提高，足以说明 BN-SVD 水印算法的鲁棒性明显优于 SVD 水印算法的鲁棒性。

3.2.4　本文算法与文献 [9,11] 的对比实验

1) 鲁棒性对比实验。为了更好地检测本算法具有较好的鲁棒性，选择 Lena 图像为原始载体图像，对其进行不同类别的攻击实验，将受攻击后所提取出的水印 NC 值与文献 [9,11] 实验结果进行对比，其对比结果如表 3 所示。

表 3　本文算法与文献 [9,11] 的 NC 值对比

Table 3　The method and literature [9,11] NC value contrast

攻击方式	参数	文献 [9]	文献 [11]	文本算法
JPEG 压缩	20	0.972 1	0.998 2	0.998 7
	10	0.966 1	0.992 5	0.996 2
滤波	3×3 中值滤波	0.992 2	1	1
	5×5 中值滤波	0.986 6	0.995 7	0.996 2
噪声	椒盐噪声 0.01	0.999 2	0.997 5	1
	椒盐噪声 0.02	0.998 4	0.995 6	0.997 5
	高斯噪声 0.001	0.980 1	0.9971	1
	高斯噪声 0.002	0.975 1	0.996 7	0.998 7
旋转	向右 1°	0.985 4	0.984 8	0.986 1
	向左 1°	0.985 7	0.986 1	0.986 0
剪切	左上角 1/16	0.998 5	0.998 9	1
	左上角 1/4	0.986 4	0.987 3	0.998 7

由表 3 可得，待测图像受到 JPEG 压缩攻击、中值滤波攻击、噪声攻击、旋转攻击以及剪切攻击后所提取出的水印图像 NC 值都要高于文献 [9,11]，说明本文算法的鲁棒性明显优于文献 [9,11]。

2) 运行时间对比实验

为了更加全面地检测算法的性能，选择 Lena 图像作为原始载体图像，对其进行不同类别的攻击实验，将本文算法实验运行时间与文献 [9,11] 的实验运行时间进行对比，对比结果见表 4。

表 4　本文算法与文献 [9,11] 的运行时间对比

Table 4　The method and literature [9,11] run time contrast

/s

攻击方式	文献 [9]	文献 [11]	本文算法
JPEG 压缩	2.450	2.610	2.439
滤波	2.576	2.720	2.627
噪声	2.428	2.637	2.567
旋转	2.262	2.130	2.008
剪切	2.514	2.519	2.306

由表 4 可得，在受到“JPEG 压缩”、“旋转”、“剪切”攻击时，本文算法的运行时间优于文献 [9,11] 算法；而在“滤波”和“噪声”的攻击下，本文算法的运行时间介于文献 [9] 与文献 [11] 算法之间。

综合以上实验结果，本文算法不仅解决了传统奇异值分解所存在的对角线失真和严重的虚警错误问题，对各种攻击的鲁棒性都有所提高，特别是在抗剪切攻击能力的提升高较为明显，突显本文算法的优势。

4　结　论

本文分析了传统奇异值分解水印算法中存在的提取水印图像时出现的对角线失真和虚警错误问题，提出了一种应用 DWT-DCT 混合变换，基于细胞神经网络和 BN-SVD 的零水印算法，零水印的注册图像由细胞神经网络的输出生成。实验结果证明，本文算法本质上解决了水印图像的对角线失真和虚警错误问题，并且在经过滤波、噪声、压缩以及剪切等常见攻击后，提取出的水印 NC 值均达到 96% 以上，有效提高了算法的鲁棒性。细胞神经网络并行处理图像可硬件实现，使得该算法可以应用于实时性要求较高的场合。但算法在运行时间和复合型几何攻击方面有待提高。在今后的研究中，希望能在抵抗更大强度的常见攻击以及复合型几何攻击方面进一步探索。

参考文献(References)

[1] Yin H, Lin C, Qiu F, et al. A survey of digital watermarking [J]. Journal of Computer Research and Development, 2005, 42(7): 1093-1099. [尹浩, 林闯, 邱锋, 等. 数字水印技术综述 [J]. 计算机研究与发展, 2005, 42(7): 1093-1099.]

[2] Yi K X, Shi J Y, Sun X. Digital watermarking techniques: an introductory review [J]. Journal of Image and Graphics, 2001, 6(2): 11-17. [易开祥, 石教英, 孙鑫. 数字水印技术研究进展 [J]. 中国图象图形学报, 2001, 6(2): 11-17.] [DOI: 10.11834/jig.20010229]

[3] Zou X X. Research on multimedia digital watermarking techniques [D]. Beijing: Chinese Academy of Sciences (Institute of

Computing Technology), 2003. [邹潇湘. 多媒体数字水印技术研究[D]. 北京: 中国科学院研究生院, 2003.]

[4] Wen Q, Sun T F, Wang S Y. Concept and application of zero-watermark[J]. Acta Electronica Sinica, 2003, 31(2): 214-216. [温泉, 孙锬锋, 王树勋. 零水印的概念与应用[J]. 电子学报, 2003, 31(2): 214-216.] [DOI: 10.3321/j.issn:0372-2112.2003.02.015]

[5] Liu R Z, Tan T N. SVD based digital watermarking method[J]. Acta Electronica Sinica, 2001, 29(2): 168-171. [刘瑞祯, 谭铁牛. 基于奇异值分解的数字图像水印方法[J]. 电子学报, 2001, 29(2): 168-171.] [DOI: 10.3321/j.issn:0372-2112.2001.02.007]

[6] Liu L, Zhou Y J, Zhang B, et al. Digital watermarking method for QR code images based on DCT and SVD[J]. Infrared and Laser Engineering, 2013, 42(S2): 304-311. [刘丽, 周亚建, 张斌, 等. 基于DCT和SVD的QR码数字水印算法[J]. 红外与激光工程, 2013, 42(S2): 304-311.] [DOI: 10.3969/j.issn.1007-2276.2013.z2.005]

[7] Zhang F Y, Quan H L, Lin L Y, et al. Robust digital watermark algorithm in Contourlet domain based on singular value decomposition[J]. Application Research of Computers, 2012, 29(4): 1402-1404, 1408. [张飞艳, 全桓立, 林立宇, 等. 基于奇异值分解的Contourlet域稳健性数字水印算法[J]. 计算机应用研究, 2012, 29(4): 1402-1404, 1408.] [DOI: 10.3969/j.issn.1001-3695.2012.04.056]

[8] Ye T Y. A robust zero-watermarking algorithm using variance in singular value decomposition domain[J]. Acta Photonica Sinica, 2011, 40(6): 961-966. [叶天语. 基于方差的奇异值分解域鲁棒零水印算法[J]. 光子学报, 2011, 40(6): 961-966.] [DOI: 10.3788/gzxb20114006.0961]

[9] Qu C B, Wang D F. Robust zero watermarking algorithm based on bit plane theory and singular value decomposition[J]. Journal of Computer Applications, 2014, 34(12): 3462-3465, 3506. [曲长波, 王东峰. 基于位平面理论和奇异值分解的鲁棒零水印算法[J]. 计算机应用, 2014, 34(12): 3462-3465, 3506.] [DOI: 10.11772/j.issn.1001-9081.2014.12.3462]

[10] Ning G Q, Liu Y Y, Li F T, et al. A robust digital image watermarking algorithm based on DWT-DCT transformation[J]. Electronic Design Engineering, 2009, 17(11): 67-69. [宁国强, 刘媛媛, 李凤堂, 等. 一种基于DWT-DCT变换强鲁棒性的数字水印算法[J]. 电子设计工程, 2009, 17(11): 67-69.] [DOI: 10.3969/j.issn.1674-6236.2009.11.026]

[11] Rao Y R, Nagabhooshanam E. A novel image zero-watermarking scheme based on DWT-BN-SVD[C]//Proceedings of 2014 International Conference on Information Communication and Embedded Systems. Chennai: IEEE, 2014: 1-6. [DOI: 10.1109/ICICES.2014.7034073]

[12] Gupta A K, Raval M S. A robust and secure watermarking scheme based on singular values replacement[J]. Sādhanā, 2012, 37(4): 425-440. [DOI: 10.1007/s12046-012-0089-x]

[13] Ren X X. Research on application of cellular neural networks to image encryption[D]. Chongqing: Chongqing University, 2012. [任晓霞. 细胞神经网络在数字图像加密方面的应用研究[D]. 重庆: 重庆大学, 2012.] [DOI: 10.7666/d.y2154353]

[14] Zhao J, Qun Z G. Zero digital watermarking algorithm based on CNN and NSCT[J]. Science Technology and Engineering, 2013, 13(5): 1368-1372. [赵杰, 屈正庚. 基于CNN和NSCT的零水印算法[J]. 科学技术与工程, 2013, 13(5): 1368-1372.] [DOI: 10.3969/j.issn.1671-1815.2013.05.052]

[15] Wu C M. An improved discrete arnold transform and its application in image scrambling and encryption[J]. Acta Physica Sinica, 2014, 63(9): #090504. [吴成茂. 离散Arnold变换改进及其在图像置乱加密中的应用[J]. 物理学报, 2014, 63(9): #090504.] [DOI: 10.7498/aps.63.090504]

[16] Tang Z J, Zhang X Q. Secure image encryption without size limitation using Arnold transform and random strategies[J]. Journal of Multimedia, 2011, 6(2): 202-206. [DOI: 10.4304/jmm.6.2.202-206]

[17] Song W, Hou J J, Li Z H, et al. A novel zero-bit watermarking algorithm based on Logistic chaotic system and singular value decomposition[J]. Acta Physica Sinica, 2009, 58(7): 4449-4456. [宋伟, 侯建军, 李赵红, 等. 一种基于Logistic混沌系统和奇异值分解的零水印算法[J]. 物理学报, 2009, 58(7): 4449-4456.] [DOI: 10.3321/j.issn:1000-3290.2009.07.013]