中图法分类号: TN911.7　　**文献标识码:** A　　**文章编号:** 1006-8961(2019)01-0001-12

论文引用格式: Xiao Z J,Jiang D,Zhang H,Tang X L,Chen H. Adaptive zero-watermarking algorithm based on boost normed singular value decomposition [J]. Journal of Image and Graphics,2019,24(01):0001-0012. [肖振久,姜东,张晗,唐晓亮,陈虹. 增强奇异值分解的自适应零水印[J]. 中国图象图形学报,2019,24(01):0001-0012.] [DOI:10.11834/jig.180443]

增强奇异值分解的自适应零水印

肖振久,姜东,张晗,唐晓亮,陈虹

辽宁工程技术大学软件学院,葫芦岛　125105

摘　要: 目的　针对增强奇异值分解(BN-SVD)中引入最抗攻击缩放比例的参数β,需要进行大量的实验来获取且存在随机性的问题,提出一种增强奇异值分解的自适应零水印算法。方法　首先对原始图像进行不重叠分块,每一个子块都做斜变换处理,再分别对斜变换后得到的每一个块矩阵进行增强奇异值分解,依据每一个块矩阵的最大奇异值与整体最大奇异值均值的大小关系构成特征向量;对水印图像进行 Arnold 变换和混沌映射得到二次加密的水印图像;最后利用特征向量与二次加密后的水印图像做异或运算构造零水印;利用天牛须优化算法(BAS)中的适应度函数循环迭代自适应确定参数β,更好地解决奇异值分解(SVD)算法在水印的提取时存在的虚警率和对角线失真的问题。结果　仿真实验结果表明,在 JPEG 压缩、噪声、滤波、旋转、剪切以及混合攻击下,提取水印图像与原水印图像的归一化系数 NC 值均可达到 98% 以上,性能较好。结论　利用 BAS 算法自适应地确定 BN-SVD 中参数β,找到最佳抗攻击缩放比例,增强了图像的奇异值,降低了图像矩阵在受到攻击时的敏感性。有效地解决奇异值分解带来的对角线失真和虚警错误的问题,最终提高了算法的鲁棒性。

关键词: 自适应零水印;增强奇异值分解(BN-SVD);斜变换;天牛须优化算法(BAS);Arnold 变换;混沌映射

Adaptive zero-watermarking algorithm based on boost normed singular value decomposition

Xiao Zhenjiu, Jiang Dong, Zhang Han, Tang Xiaoliang, Chen Hong

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

Abstract: Objective Parameter β is the most commonly used anti-attack scaling ratio in boost normed singular value decomposition (BN-SVD). However, it requires numerous experiments to obtain and has randomness. Thus, an adaptive zero-watermarking algorithm based on BN-SVD was proposed. Using this parameter presents three advantages. First, the singular value of the image is enlarged, the sensitivity of the image to attacks is reduced, and the robustness of the algorithm is improved to some extent. Second, singular values are limited to a certain range. The diagonal distortion problem can be solved by equalizing the grayscale in the diagonal direction. Third, a singular value vector is specialized, and the corresponding relation between a singular value vector and an image is specialized to one, such that singular values can represent the features of the image. Thus, the problem of false alarm error is solved. **Method** First, the original image was divided into non-overlapping blocks. Then, slant transform (ST) was performed on each block matrix. BN-SVD was used on each block matrix after ST to achieve a maximum singular value, and a feature vector was created by comparing the maximum singular value with the average maximum singular value. The watermarked image was processed by Arnold transfor-

收稿日期: 2018-07-10;**修回日期:** 2018-08-13;**预印本日期:** 2018-08-20

基金项目: 国家自然科学基金青年科学基金项目(61401185)

Supported by: Young Scientists Fund of National Natural Science Foundation of China(61401185)

mation and logistic mapping to obtain an encrypted and scrambled double-encrypted watermarked image. Finally, the zero watermark was constructed using the feature vector, and the double-encrypted watermarked image was used for XOR operation. During optimization, parameter β was determined by training and updating continuously through the BAS fitness function. Similar to genetic algorithm, particle swarm optimization, and so on, the proposed algorithm does not need to know the specific function form and gradient information. The optimization process can be realized independently, and its characteristics were single individual, less computation, and faster optimization speed. The algorithm was inspired by beetle search behavior. The biological principle is as follows: the beetle relies on the strength of the food smell to find food. Two antennae were randomly used to search nearby areas. When the antennae on one side detected a higher concentration of odors, the beetles turn in that direction. According to this simple principle, the beetle can effectively find food. **Results** Under JPEG compression, rotation, filtering, clipping, and other attacks, the normalized coefficients of the extracted watermarked images and the original watermarked exceeded 98%. Lena, Baboon, and Bridge were selected as the original grayscale image, and two different sizes of "Liaoning Technical University" were chosen as binary watermarking images. Several sets of experiments were conducted. In the experiment, a normalized correlation coefficient (NC) was used to analyze the similarity between the original watermark and the extracted watermark, and the optimal parameters β for the 16×16 pixels and 32×32 pixels watermarked images were found by the BAS optimization algorithm. The optimum parameter β values of the three gray images of Lena, Baboon, and Bridge were 0.298 3, 0.642 4, and 0.533 2 for the 16×16 pixels watermarked images and 0.737 0, 0.991 4, and 0.873 5 for the 32×32 pixels watermarked images. The experimental results revealed that with the increase in attack intensity and mixed attacks, the NC value of the watermark is affected. However, most NC values exceeded 0.99. The NC value of the watermark extracted after geometric attacks, such as clipping and rotation, was close to 1. Given that the original gray image was rotated, and some pixels were lost in the clipping process, the watermark generated was incomplete. A larger compression attack parameter corresponded to a larger NC value, indicating that the algorithm had better resistance to JPEG compression. For all kinds of noise attacks, the NC value of the extracted watermark can exceed 0.99. **Conclusion** BAS algorithm can be used to adaptively determine parameters β in BN-SVD. The optimal scale of scaling enhanced the singular value of the image and reduced the sensitivity of the image matrix when attacked. The problems of diagonal distortion and false alarm error caused by singular value decomposition were solved effectively, and the robustness of the watermarking algorithm was improved. Compared with other traditional optimization algorithms, the BAS algorithm presented the advantages of short training time, fast convergence speed, and good robustness. By integrating the concept of zero watermark, the contradiction between robustness and invisibility of the watermark is solved. Thus, the robustness of the watermarking algorithm was improved.

Key words: adaptive zero-watermarking; boost normed singular value decomposition (BN-SVD); slant transform (ST); beetle antennae search (BAS); Arnold transform; logistic map

0 引 言

由于通信技术、网络技术和计算机技术的飞速发展,数字媒体得到了广泛的应用。越来越多的数字媒体通过网络进行传输。然而,开放的网络环境和便捷的信息技术也给数字作品的信息安全和版权保护带来了日益严峻的问题。数字水印技术被认为是防止图像处理工具对图像数据进行非法修改和复制的最具潜力的技术之一,已经成为信息安全领域的一个研究热点[1-3]。

传统嵌入式水印算法都面临着算法透明性与鲁棒性的矛盾问题。文献[3]对水印图像与载体图像皆做了 Slant 变换处理,随机选取 m 个子块以强度 α 将水印信息嵌入到每个子块的 16 个中频位置。文献[4]作出改进将 Slant 变换与 LU 分解相结合,将图像分为 8×8 不重叠子块后分块进行 Slant 变换和 LU 分解将加密后的水印信息随机嵌入到上三角矩阵的第 1 行中。文献[3-4]中水印算法运算速度快、安全性高且都具有良好的不可见性。然而,水印算法对于压缩、噪声以及几何攻击的鲁棒性都较差。为了提高水印算法鲁棒性,一些学者提出基于奇异值分解(SVD)的水印算法。在文献[5]中,在对载体图像进行 Contourlet 变换后,对低频部分做块奇异值分解,其水印的主成分是通过修改块的最大奇异值的方式进行嵌入。算法具有较强的鲁棒性,虽然

在数值上达到了不可见性的标准,但具有明显的块效应。文献[6]提出了一种基于奇异值分解和离散小波变换的水印算法,具有良好的隐蔽性和稳健性,虽然针对对角线失真进行了改进但在水印重建时仍具有对角线失真的现象。文献[7]提出一种小波变换与奇异值分解(DWT-SVD)和果蝇优化算法(FOA)相结合的优化数字水印算法。但算法在水印提取阶段存在严重的虚警错误。文献[8]提出了一种基于奇异值分解和蜂群优化的鲁棒水印算法,嵌入强度的参数则采用蜂群优化算法来选取,自适应均衡水印算法的鲁棒性与透明性,但蜂群优化算法收敛速度慢,寻找最优解时间较长。在 2003 年,温泉等人[9]提出了零水印算法,解决水印算法鲁棒性与不可见性之间的矛盾。该类算法是利用原始载体图像的内部特征来构造零水印,并将其存放在集中认证中心,待认证时与保存的数据进行信息恢复,既保证了原始载体图像的完整性,又解决了水印算法鲁棒性与透明性的矛盾问题。文献[10]提出了基于位平面理论和奇异值分解的鲁棒零水印算法,在受到噪声、JPEG 压缩、滤波、剪切攻击方面,表现出较好的鲁棒性,但提升效果不明显。文献[11]提出了一种基于离散小波变换和奇异值分解的鲁棒双零水印算法。为解决水印鲁棒性与透明性的问题,文献[6]存在的对角线失真问题和文献[7]存在的严重虚警问题,本文借鉴文献[12]的思路,提出了一种基于斜变换(ST)和增强奇异值分解[13]的零水印算法。对奇异值矩阵作出改进,在一定范围内增强奇异值使其对角线方向上灰度更均衡,从而具有更好的鲁棒性。同时采用天牛须优化算法(BAS)来自适应确定参数 β。该算法的优势在于找到最优抗攻击的缩放比例,从而解决了水印算法提取时出现的虚警问题和对角线失真问题,进一步提高了水印算法的鲁棒性。

1　算法理论

1.1　斜变换

斜变换在信号处理中得到了广泛的应用,它是将原始信号从空域转换到频域。变换的思想是:根据图像信号的相关性,某行的亮度具有基本不变或线性渐变的特点,可以构造一个变化矩阵来反映行向量[14]的递增或递减特性。对于纹理图像,斜变换图像的质量与使用其他变换(如 Hadamard)编码得到的图像质量相比,具有优越性且误差更小,在能量压实方面具有次优性,可以有效提高水印的鲁棒性。类似于 Walsh-Hadamard 变换,斜变换具有计算简单、计算速度快的优点,是一种具有快速计算能力的正交变换。设 $\boldsymbol{I}$ 为原始图像像素矩阵,$\boldsymbol{S}$ 为斜矩阵,$\boldsymbol{J}$ 为 Slant 变换后的矩阵,则 Slant 变换过程可以表述为

$$\boldsymbol{J} = \boldsymbol{S} \times \boldsymbol{I} \times \boldsymbol{S}^{\mathrm{T}} \tag{1}$$

矩阵的阶数不同所对应的斜矩阵也不同,斜矩阵计算公式为

$$\begin{cases} \boldsymbol{S}_1 = \dfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\ \boldsymbol{S}_2 = \dfrac{1}{\sqrt{4}}\begin{bmatrix} 1 & 1 & 1 & 1 \\ \dfrac{3}{\sqrt{5}} & \dfrac{1}{\sqrt{5}} & -\dfrac{1}{\sqrt{5}} & -\dfrac{3}{\sqrt{5}} \\ 1 & -1 & -1 & 1 \\ \dfrac{1}{\sqrt{5}} & -\dfrac{3}{\sqrt{5}} & \dfrac{3}{\sqrt{5}} & -\dfrac{1}{\sqrt{5}} \end{bmatrix} \\ \boldsymbol{S}_n = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ a_n & b_n & 0 & -a_n & b_n & 0 \\ 0 & 0 & \boldsymbol{I}_{\frac{N}{2}-2} & 0 & 0 & \boldsymbol{I}_{\frac{N}{2}-2} \\ 0 & 1 & 0 & 0 & -1 & 0 \\ -b_n & a_n & 0 & b_n & a_n & 0 \\ 0 & 0 & \boldsymbol{I}_{\frac{N}{2}-2} & 0 & 0 & \boldsymbol{I}_{\frac{N}{2}-2} \end{bmatrix} \times \\ \quad \begin{bmatrix} \boldsymbol{S}_{n-1} & 0 \\ 0 & \boldsymbol{S}_{n-1} \end{bmatrix} \end{cases} \tag{2}$$

式中,$\boldsymbol{I}_{\frac{N}{2}-2}$ 是 $\left(\dfrac{N}{2}-2\right)$ 阶的单位矩阵。a_n,b_n 的计算公式为

$$\begin{cases} a_{n+1} = \left(\dfrac{3N^2}{4(N^2-1)}\right)^{1/2} \\ b_{n+1} = \left(\dfrac{N^2-4}{4(N^2-1)}\right)^{1/2} \end{cases}, N = 2^n \tag{3}$$

Slant 逆变换为

$$\boldsymbol{I} = \boldsymbol{S}^{\mathrm{T}} \times \boldsymbol{J} \times \boldsymbol{S} \tag{4}$$

1.2　奇异值分解(SVD)

奇异值分解是矩阵对角化的有效数值分析工具,被广泛地应用于图像处理领域。假设数字图像 $\boldsymbol{A}$ 的大小为 $N \times N$,对其进行奇异值分解,则存在正

交矩阵 $\boldsymbol{U}_{N\times N}$、$\boldsymbol{V}_{N\times N}$和对角矩阵 $\boldsymbol{S}_{N\times N}$使得

$$\boldsymbol{A} = \boldsymbol{U}\times\boldsymbol{S}\times\boldsymbol{V}^{\mathrm{T}} \tag{5}$$

式中，$\boldsymbol{U}$ 和 $\boldsymbol{V}^{\mathrm{T}}$ 分别是左奇异值矩阵和右奇异值矩阵且二者都是正交矩阵 $\boldsymbol{U}\times\boldsymbol{U}^{\mathrm{T}}=1$，$\boldsymbol{V}=\boldsymbol{V}^{-1}$，而 $\boldsymbol{S}=\mathrm{diag}(\lambda_i)$ 是一个除对角元素外其他值都是 0 的矩阵，其对角线上的元素值为 $\lambda_i(i=1,2,\cdots,r)$ 且 $\lambda_1\geqslant\cdots\geqslant\lambda_r>0$。$r$ 为矩阵 $\boldsymbol{A}$ 的秩。

当对图像施加较小的扰动时不会对图像的奇异值造成过大的影响，其拥有较好的稳定性。经过奇异值分解后，对应的正交矩阵表示图像的几何结构，奇异矩阵表示图像的亮度信息。图像与奇异值向量间并无一一对应关系，意味着不同的图像其奇异值向量可以为相同的，而两幅图像结构并不相同。这就会导致在运用奇异值向量进行水印信息嵌入时，可能在并未嵌入水印信息的图像中提取出水印信息，造成水印提取时的虚警问题。且由于奇异值分解的自身特性，在提取水印时会产生较为严重的对角线失真问题。

1.3 增强奇异值分解

增强奇异值分解(BN-SVD)是在奇异值分解的基础上引入一个参数 β，其作用为使奇异值分解后得到对角线方向上的灰度均衡化。假设数字图像 $\boldsymbol{B}$ 大小为 $N\times N$，对其进行增强奇异值分解，则存在正交矩阵 $\boldsymbol{U}_{N\times N}$、$\boldsymbol{V}_{N\times N}$和对角矩阵 $\boldsymbol{S}_{N\times N}$使得

$$\boldsymbol{B} = \boldsymbol{U}\times(\boldsymbol{S})^{\beta}\times\boldsymbol{V}^{\mathrm{T}},0<\beta<1 \tag{6}$$

式中，矩阵 $\boldsymbol{U}$ 是矩阵 $\boldsymbol{B}$ 的左奇异矩阵，列矩阵 $\boldsymbol{V}^{\mathrm{T}}$ 是矩阵 $\boldsymbol{B}$ 的右奇异矩阵。

增强奇异值矩分解是将数字图像 $\boldsymbol{B}$ 进行奇异值分解后的对角矩阵 $\boldsymbol{S}_{N\times N}$做 β 次幂运算。在处理不同的数字图像时，可以根据图像自身固有的信息对参数进行合理的调整，以达到最佳的抗攻击效果。

BN_SVD 分解的优点如下：

1)将图像奇异值进行放大，降低了图像矩阵在受到攻击时的敏感性，一定程度上提高了算法的鲁棒性。

2)奇异值被限定在一定的范围内，均衡化对角线方向上的灰度，可以解决对角线失真的问题。

3)将奇异值向量特殊化，使其与图像存在一一对应关系，使得奇异值可代表图像的特征，进而解决了其存在的虚警错误问题。

1.4 自适应天牛须优化算法

天牛须搜索(BAS)算法[15]又叫甲虫触角搜索算法，2017 年李帅等人[16]提出了一种新的基于甲虫觅食原理的优化算法，适用于多种优化函数。该算法相似于遗传算法、粒子群优化等算法，不需要知道具体的函数形式和梯度信息。优化过程可以独立实现，其特点如下：个体单一，运算量减小并且加快寻优速度。该算法受甲虫搜索行为启发。其生物原理[17]为：天牛是根据食物气味的强弱来寻找食物的，天牛随机使用两个触角在附近地区进行搜寻，当一侧的触角探测到更高浓度的气味时，天牛就会转向方向，依据这一简单原理天牛就可以有效找到食物。

算法步骤如下：

1)初始化最大迭代次数 MAX，随机初始化天牛气味强度 X 和天牛须朝向的随机向量 d 并做归一化处理

$$\boldsymbol{d}' = \frac{rands(k,1)}{\|rands(k,1)\|} \tag{7}$$

式中，$rands()$为随机函数；k 表示空间维度。

2)赋予天牛个体左右两须利用气味强度搜寻并朝向食物的空间坐标

$$\begin{cases}\boldsymbol{X}_{\mathrm{R}}^{t} = \boldsymbol{X}^{t}+d_0\times\boldsymbol{d}'/2\\ \boldsymbol{X}_{\mathrm{L}}^{t} = \boldsymbol{X}^{t}-d_0\times\boldsymbol{d}'/2\end{cases} \tag{8}$$

式中，在第 t 次迭代时，天牛右须位置坐标为 X_{R}^{t}；天牛左须位置坐标为 X_{L}^{t}；天牛质心坐标 X^{t}；两须之间的距离 d_0。

3)迭代更新天牛的位置

$$\boldsymbol{X}^{t+1} = \boldsymbol{X}^{t}-\delta^{t}\times\boldsymbol{d}'\times\mathrm{sgn}(f(\boldsymbol{X}_{\mathrm{R}}^{t})-f(\boldsymbol{X}_{\mathrm{L}}^{t})) \tag{9}$$

式中，δ^{t} 表示在第 t 次迭代时的步长因子。

4)由于无法得知气味强度的位置，先将气味强度测定值设定为 X。在本实验中 X 的横坐标为参数 β，取值范围为 [0,1]，所以对该值进行分段约束

$$\boldsymbol{X} = \begin{cases}(1,0) & |\boldsymbol{X}^{t+1}|>1\\ (0,0) & |\boldsymbol{X}^{t+1}|<0\\ \boldsymbol{X}^{t+1} & \text{其他}\end{cases} \tag{10}$$

5)通过天牛的左右须坐标(X_{L}^{t}，X_{R}^{t})利用式(9)确定当前天牛的空间位置和气味强度测定函数 f(即适应度函数)来求出天牛个体位置的气味强度，即

$$f(\boldsymbol{X}) = f(\boldsymbol{X}^{t+1}) \tag{11}$$

本文提出自适应算法的关键在于寻求最优参数 β。在此过程中，实现适应度函数 f 的循环迭代从而影响水印的鲁棒性，算法流程如图 1 所示。

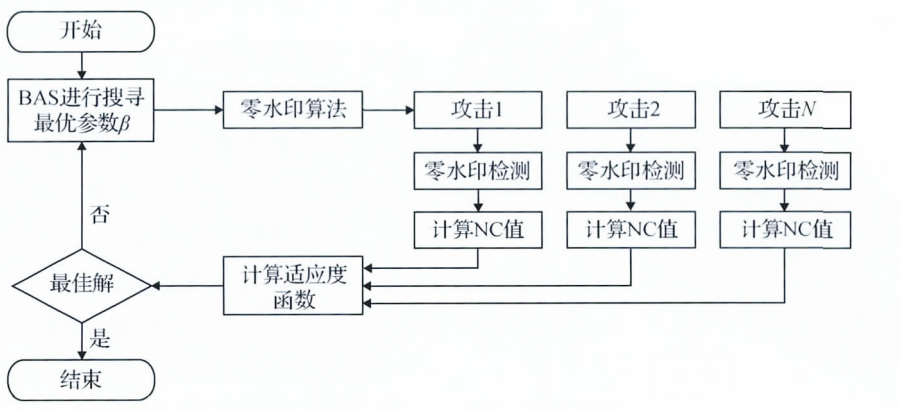


图 1　BAS 搜寻最优解的流程

Fig. 1　The flow of BAS search for optimal solution

适应度函数(fitness function)是评价每个候选方案实现自适应的直接依据。在天牛须优化算法中,适应度函数的选择是该算法实现的重要环节。本仿真实验中,分别使用了 32×32 像素与 16×16 像素两组不同大小的水印图像,对多组实验进行了比较,并分别对两组目标函数 f 进行迭代寻求最优参数 β,使其达到更强的鲁棒性。

6)找出天牛须中最新的气味强度 f 及位置 $\vec{X}$,即

$$[f,\vec{X}] = \max(\vec{X}) \tag{12}$$

7)寻找最强的气味强度 f_{best} 的位置 $\vec{X}_{\text{best}}$,并奔向该位置

$$\begin{cases} f = \max(f_{\text{best}}) \\ X = \max(X_{\text{best}}) \end{cases} \tag{13}$$

8)重复执行步骤 2)—6),迭代优化来寻找最优解,在每次迭代结束时,判断气味,如果气味强度优于前一次则执行步骤 7),当执行最大迭代次数 MAX 则结束整个过程,得到最优结果 X 的横坐标即参数 β。

2　算法实现

2.1　水印图像预处理

为了进一步提高安全性,本文采用 Arnold 置乱和 Logistic 混沌映射的双重置乱来实现对水印图像的预处理。

Arnold 变换[18] 俗称猫脸映射是一种从规则位置到随即位置的映射,是一种传统的混沌系统。本文选择 Arnold 置乱对图像进行第 1 次加密。

对一幅大小为 $M \times M$ 的图像,Arnold 置乱定义为

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{14}$$

$$x,y \in \{0,1,\cdots,N-1\}$$

式中,前后像素点的位置分别由 (x,y) 和 (x',y') 表示。x、y、N 为正整数,N 代表图像矩阵的阶数,mod 为取余运算。其变换的实质是通过像素位置的置换,来减弱相邻像素之间的关联性,提高了图像安全性。此外该置乱具有周期性,即经过有限次的迭代便可恢复出原始图像。

Logistic 映射[19-20] 具有遍历性高、伪随机性强、对初值高敏感等优点,在保密通信领域、图像加密领域中应用十分广泛,是一种形式简单的 1 维混沌系统。其定义为

$$x_{i+1} = \mu x_i(1 - x_i)$$

$$x_i \in (0,1),\mu \in [0,4] \tag{15}$$

式中,μ 为 Logistic 混沌系统的控制参数,x_i 为映射的混沌序列。当 $x_i \in (0,1)$ 时,Logistic 映射工作处于混沌状态,也就是说,有初始条件 x_0 在 Logistic 映射作用下产生的序列是非周期性的、不收敛的,而在此范围之外,生成的序列必将收敛于某一个特定的值,当 $3.569\ 456 < \mu \leqslant 4$ 时,特别是比较靠近 4 时,迭代生成的值处于一种随机分布的状态,而在其他处取值时,再经过一定次数的迭代之后,生成的值将收敛于一个特定的数值。

两种加密方法的结合,使水印的鲁棒性和安全性有所提升,实现更好的加密效果。

2.2　零水印构造方案

零水印构造图如图 2 所示。

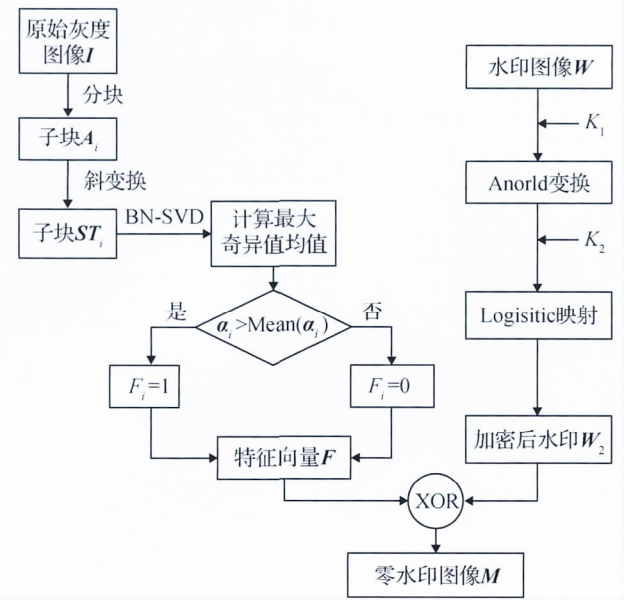


图 2　零水印构造图

Fig. 2　Zero watermark structure diagram

选取大小为 $M \times M$ 的灰度图像 $\boldsymbol{I}$ 作为原始图像，大小为 $(M/16) \times (M/16)$ 的二值化图像 $\boldsymbol{W}$ 作为水印图像。零水印图像具体构造流程如下：

1）对原始灰度图像 $\boldsymbol{I}$ 进行 8×8 分块，生成不重叠子块：$\boldsymbol{A}_i(i = 1,2,\cdots,(M/16) \times (M/16))$，并对 $\boldsymbol{A}_i$ 进行斜变换处理，得到子块记作：$\boldsymbol{ST}_i(i = 1,2,\cdots,(M/16) \times (M/16))$。

2）对 $\boldsymbol{ST}_i$ 进行增强奇异值分解，即 $\boldsymbol{ST}_i = \boldsymbol{U}_i \times (\boldsymbol{S}_i)^{\beta}\boldsymbol{V}_i^{\mathrm{T}}(0 < \beta < 1)$，得到正交矩阵 $\boldsymbol{U}_i$、$\boldsymbol{V}_i$ 和对角矩阵 $\boldsymbol{S}_i$。参数 β 用 1.4 节天牛须搜索找到最优。

3）从对角矩阵 $\boldsymbol{S}_i$ 中取出第一个奇异值共有 $(M/16) \times (M/16)$ 个，记作 $\alpha_i(i = 1,2,\cdots,(M/16) \times (M/16))$。

4）求 $(M/16) \times (M/16)$ 个最大奇异值的平均值 $\mathrm{mean}(\boldsymbol{\alpha}_i)$。依据 $\boldsymbol{\alpha}_i$ 和 $\mathrm{mean}(\boldsymbol{\alpha}_i)$ 的大小关系构成一个特征向量 $\boldsymbol{F}$，即

$$F_i = \begin{cases} 1 & \boldsymbol{\alpha}_i > \mathrm{mean}(\boldsymbol{\alpha}_i) \\ 0 & \text{其他} \end{cases} \tag{16}$$

5）最后将原始二值水印图像 $\boldsymbol{W}$ 作 K_1 次 Arnold 置乱，获得置乱后水印图像 $\boldsymbol{W}_1$。随之对水印图像 $\boldsymbol{W}_1$ 进行 Logistic 映射，得到二次加密后水印图像 $\boldsymbol{W}_2$ 和密钥 K_2。

6）将特征向量 $\boldsymbol{F}$ 与置乱后的水印图像 $\boldsymbol{W}_2$ 进行异或运算（XOR），生成零水印图像 $\boldsymbol{M}$，即

$$\boldsymbol{M} = \mathrm{XOR}(\boldsymbol{F},\boldsymbol{W}_2) \tag{17}$$

2.3　零水印检测

零水印检测图如图 3 所示。

水印的检测即为水印构造的逆过程。选取载体灰度图像 $\boldsymbol{I}'$，大小为 $M \times M$。

零水印检测步骤如下：

1）对原始灰度图像 $\boldsymbol{I}'$ 进行 8×8 分割，得到 $(M/16) \times (M/16)$ 个大小互不重叠的子块 $\boldsymbol{A}'_i(i = 1,2,\cdots,(M/16) \times (M/16))$，随之对其进行 Slant 逆变换，得到子块记作：$\boldsymbol{ST}'_i(i = 1,2,\cdots,(M/16) \times (M/16))$。

2）对每一个子块 $\boldsymbol{ST}_i$ 进行增强奇异值分解（BN-SVD），得到对角矩阵 $\boldsymbol{S}'_i$。

3）取对角矩阵 $\boldsymbol{S}'_i$ 中第 1 个奇异值共 $(M/16) \times (M/16)$ 个记作：$\boldsymbol{\alpha}'_i(i = 1,2,\cdots,(M/16) \times (M/16))$。求取平均值 $\mathrm{mean}(\boldsymbol{\alpha}'_i)$。根据 $\boldsymbol{\alpha}'_i$ 和 $\mathrm{mean}(\boldsymbol{\alpha}'_i)$ 的大小关系得到特征向量 $\boldsymbol{F}'$。

4）将零水印图像 $\boldsymbol{M}$ 与步骤 3）中得到的特征向量 $\boldsymbol{F}'$ 进行异或运算，得到加密置乱后的水印图像 $\boldsymbol{W}_2$，即

$$\boldsymbol{W}_2 = \mathrm{XOR}(\boldsymbol{M},\boldsymbol{F}') \tag{18}$$

5）最后对水印图像 $\boldsymbol{W}_2$ 进行逆 Logistic 映射和 K_1 次 Arnold 逆置乱得到原始水印图像 $\boldsymbol{W}$。

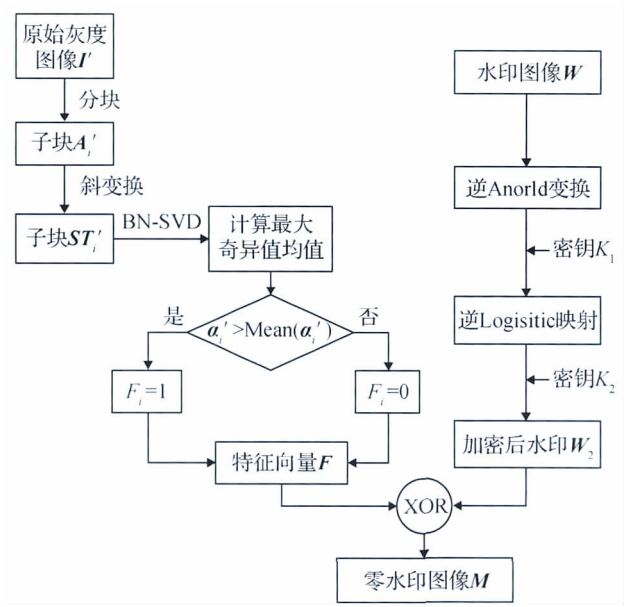


图 3　零水印检测图

Fig. 3　Zero watermark detection diagram

3　仿真实验与分析

为了验证本文算法是否具有较高的鲁棒性,采用 MATLAB 2016a 实验平台,选取如图 4(a)—(c)标准灰度测试图像作为原始灰度图像,其大小 512×512 像素。图像 Lena 纹理信息较少,但有较小的细节;图像 Baboon 细节与纹理信息都相对复杂;图像 Bridge 细节与纹理都相对均匀;选取如图 4(d)所示 32×32 像素的二值图像“辽宁工大”为水印图像,图 4(e)所示为 16×16 像素的二值图像“辽宁工大”为水印图像。设置天牛须优化算法的迭代次数为 40,实验中,分别对 3 幅原始灰度图像进行了以下 9 种攻击:1)3×3 中值滤波;2)JPEG 压缩;3)剪切;4)旋转;5)高斯滤波;6)高斯噪声;7)椒盐噪声;8)缩放;9)混合。仿真实验采用归一化相关(NC)函数来评价提取的水印与原水印的相似度,即

$$NC(x_1,x_2)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}x_1(i,j)x_2(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(x_1(i,j))^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(x_2(i,j))^2}} \tag{19}$$

式中,x_1 表示为初始水印,x_2 表示为提取的水印。

图 4　原始灰度图像与水印图像

Fig. 4　Original grayscale images and watermark images ((a) original image Lena; (b) original image Baboon; (c) original image Bridge; (d) watermark image (32×32 pixels); (e) watermark image (16×16 pixels))

3.1　鲁棒性实验

为验证本文水印算法具有较好的鲁棒性,做了多组实验。针对 16×16 像素和 32×32 像素的水印图像,利用天牛须优化算法在第 18 次实验中得到 Lena、Baboon 和 Bridge 这 3 幅灰色图像的最优参数 β 值为 0.298 3、0.642 4、0.533 2 和 0.737 0、0.991 4、0.873 5。分别对 3 幅灰色图像进行攻击实验,表 1 列出了待测图像在受到各种不同攻击后提取出 32×32 像素零水印图像的 NC 值,从表 1 中可以得出,随着攻击强度混合攻击的增加,水印的 NC 值受到一定的影响,但大多数 NC 值都在 0.99 以上。其中,通过对进行剪切、旋转等几何攻击提取出的水印 NC 值都接近于 1,这是由于原始灰度图像在旋转、剪切过程中图像失去了一些像素,所以生成的水印并不完整。随着压缩攻击参数的增大,得到的 NC 值也随之增大,说明本算法对 JEPG 压缩有较好的抵抗能力。对于各种噪声攻击,提取零水印的 NC 值都可以达到 0.99 以上。分析以上的结果可得,通过 Slant 与 BN-SVD 结合的算法斜变换得到的图像质量高,增强奇异值分解使对角方向上的灰度均衡化降低了图像矩阵受攻击时的敏感性,并结合天牛须优化算法,找到实验最佳的参数 β,天牛须优化算法智能搜索最优解,不需要对实验参数逐一对比,增强了该水印算法的鲁棒性。

表 1　待测图像攻击后提取出 32×32 像素水印图像的 NC 值

Table 1　Extracting the NC value of the 32×32 pixels watermark after attacking the image to be detected

攻击	强度	Lena	Baboon	Bridge
高斯噪声	0.01	**1.000 0**	0.999 9	**1.000 0**
	0.02	0.998 9	**0.999 9**	**0.999 9**
中值滤波	3×3	**1.000 0**	0.999 9	**1.000 0**
	5×5	0.999 9	0.999 9	**1.000 0**
高斯滤波	0.5	**1.000 0**	**1.000 0**	**1.000 0**
压缩攻击	20	0.999 9	**1.000 0**	**1.000 0**
	10	0.999 8	0.999 9	**1.000 0**
缩放	0.5	**1.000 0**	**1.000 0**	**1.000 0**
混合	高斯滤波加中心剪切 1/4	**0.998 4**	**0.998 4**	**0.998 4**
剪切攻击	左上角 1/16	**1.000 0**	0.999 9	**1.000 0**
	左上角 1/4	0.998 2	**0.998 3**	0.998 1
椒盐噪声	0.01	**1.000 0**	**1.000 0**	**1.000 0**
	0.02	0.999 9	**1.000 0**	**1.000 0**
旋转攻击	向左 1°	0.989 9	**0.999 8**	**0.999 8**
	向右 1°	0.988 6	**0.999 8**	**0.999 8**

注:加粗字体为本文算法的最优结果。

图5为部分攻击下提取的水印图像。实验结果可以得出,提取的水印图像与原始水印图像几乎没有差别,表明该算法具有较强的鲁棒性。

图5 受攻击后的实验图像

Fig. 5 Attacked experimental images((a) salt and pepper noise (0.02); (b) Gaussian noise(0.02); (c) shear upper left corner; (d) Gaussian noise and central shear(1/4); (e) JEPG compression(20); (f) median filtering(5×5))

表2列出了待测图像在受到各种不同攻击后提取出16×16像素大小水印图像的NC值。在相同的攻击条件下,提取出两种不同大小水印的NC值大致相同。与大小为32×32像素的水印结果相比要稍差一些。由于零水印是从原始图像特征中构造,水印图像越大,从图像中提取出的特征信息就越多,并且在发生相同的攻击时,也会减小对像素的影响。两组鲁棒性实验中提取出零水印的NC值都接近于1,表明本文算法具有强鲁棒性。

图6为部分攻击下提取的水印图像。提取出的水印图像清晰可辨与原始水印图像用肉眼看几乎没有差别,说明本文算法对于各种不良攻击都可以有效地抵抗。

表2 待测图像受攻击后提取出16×16像素水印图像的NC值

Table 2 Extracting the NC value of the 16×16 pixels watermark after attacking the image to be detected

攻击	强度	Lena	Baboon	Bridge
高斯噪声	0.01	**1.000 0**	0.999 9	**1.000 0**
	0.02	0.998 8	**0.999 8**	0.999 7
中值滤波	3×3	**1.000 0**	0.999 9	**1.000 0**
	5×5	0.999 8	0.999 9	**1.000 0**
高斯滤波	0.5	**1.000 0**	**1.000 0**	**1.000 0**
压缩攻击	20	0.999 6	0.999 9	**1.000 0**
	10	0.999 5	0.999 9	**1.000 0**
缩放	0.5	**1.000 0**	**1.000 0**	**1.000 0**
混合	高斯滤波加中心剪切1/4	**0.998 3**	0.997 8	**0.998 3**
旋转攻击	向左1°	0.986 6	**0.999 8**	0.999 6
	向右1°	0.984 2	**0.999 7**	0.999 6
椒盐噪声	0.01	**1.000 0**	**1.000 0**	**1.000 0**
	0.02	0.999 7	0.999 9	**1.000 0**
剪切攻击	左上角1/16	0.999 9	0.999 7	**1.000 0**
	左上角1/4	**0.998 1**	0.998 0	0.997 7

注:加粗字体为本文算法的最优结果。

3.2 透明性和安全性评价

由于原始灰度图像没有任何更改,所以攻击者无法检测水印图像是否存在Arnold变换和Logistic映射,从而实现了水印信息图像特征的二次加密,保证了本文算法的安全性。本水印算法采用Arnold变换、混沌映射与Slant-BN-SVD算法,在不确定密钥K_1、K_2的情况下提取出零水印也是相当困难的。

3.3 对角线失真问题测试

参考文献[21]算法中提取的水印图像具有明显的对角线痕迹如图7所示。

本文算法提取的水印图像如图8,从中可以看出,水印图像无明显的对角线,痕迹实验表明克服了对角线失真问题。

3.4 虚警率问题实验测试

为了验证本文是否能够真实有效地解决SVD

图 6　6 种不同攻击下提取的水印图像

Fig. 6　Extract watermark images under six different attack ((a) salt and pepper noise (0.02); (b) Gaussian noise(0.02); (c) shear upper left corner; (d) Gaussian noise and central shear(1/4); (e) JEPG compression(20); (f) median filtering(5×5))

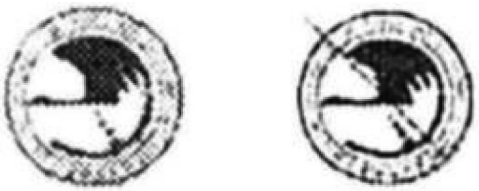


图 7　原水印图像与受攻击后提取的水印图像

Fig. 7　Original watermark image and extracted attacking watermark image((a) original watermark image; (b) extracted watermark image)

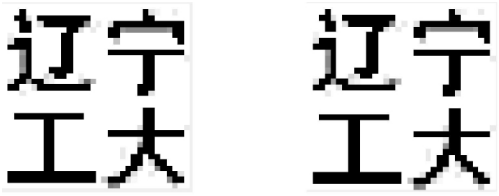


图 8　本文原水印图像与受攻击后提取的水印图像

Fig. 8　Original watermark image and extracted attacking watermark image in this paper((a) original watermark image; (b) extracted watermark image)

的虚警错误问题,将本文算法与 SVD 算法进行对比实验,结果如图 9 所示。实验结果表明,当采用 BN-SVD 算法在不能确定参数 β 值的情况下提取水印图像时,不能提取出正确的水印图像(密文),大大降低了算法的虚警率。引入参数 β 后,便存在图像与奇异值向量一一对应的关系。即图像的不同奇异值向量也就不同,图像的奇异值体现着图像的特征,因此解决了虚警错误的问题。

为验证上述虚警率问题,表 3 给出了上述实验后提取的水印图像与原始水印图像的 NC 值对比。

由表 3 可知,采用本文算法提取出的水印图像和伪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。

3.5　本文算法与文献[12-13]的对比实验

本文利用斜变换算法的计算简单、计算速度快的特点,结合 BN-SVD 使奇异值分解后均衡化对角线方向上的灰度增强水印的鲁棒性,利用天牛须优化算法自适应参数 β,使水印的鲁棒性达到最理想的效果。为了更好地检测本文算法具有强鲁棒性,选取 512×512 像素的 Lena 图像作为原始图像,32×32 像素的"辽宁工大"图像为水印图像,将受攻击后提取出的水印 NC 值与文献[12-13]算法得到的实验结果进行了对比,结果如表 4 所示。在水印算法上,参考文献[12]使用DWT与DCT两种算法结合

(a) 原始图像 (b) 伪造水印图像 (c) SVD算法 (d) 本文算法

图9 虚警错误仿真实验结果

Fig. 9 Simulation results of false positive errors

((a) original images; (b) forgery watermark images; (c) SVD; (d) ours)

表3 两种算法NC值对比

Table 3 Two algorithms of NC value contrast

图像	SVD算法	本文算法
Lena	0.996 3	**0.356 9**
Baboon	0.994 7	**0.324 8**
Bridge	0.989 6	**0.315 1**
Plane	0.994 2	**0.334 2**

注:加粗字体为算法对比的最优结果。

得到低频系数矩阵,利用BN-SVD形成特征向量,不同之处在于,本文算法采用斜变换,然后进行BN-SVD构成特征向量,文献[13]与本文算法使用相同的BN-SVD,通过DWT得到低频系数矩阵,最后生成特征向量,本文算法采用天牛须优化算法对参数β实现自适应过程,使实验效果达到最优。

从表4中数据可以看出,在剪切攻击方式下,本文算法在剪切1/16的情况下优于文献[13],但

表4 本文与文献[12-13]算法的NC值对比

Table 4 Comparison of NC values between our algorithm and reference [12-13]

攻击	强度	文献[12]	文献[13]	本文
旋转攻击	向左1°	0.986 1	0.986 1	**0.989 9**
	向右1°	0.986 0	0.984 8	**0.988 6**
剪切攻击	左上角1/16	1.000 0	0.998 9	**1.000 0**
	左上角1/4	**0.998 7**	0.987 3	0.998 2
椒盐噪声	0.01	1.000 0	0.997 5	**1.000 0**
	0.02	0.997 5	0.995 6	**0.999 9**
高斯噪声	0.01	1.000 0	0.997 1	**1.000 0**
	0.02	0.998 7	0.996 7	**0.998 9**
中值滤波	3×3	1.000 0	1.000 0	**1.000 0**
	5×5	0.996 2	0.995 7	**0.999 9**
压缩攻击	20	0.998 7	0.998 2	**0.999 9**
	10	0.996 2	0.992 5	**0.999 8**

注:加粗字体为对比实验的最优结果。

随着剪切面积的增加,抗攻击能力随之下降。在旋转攻击方面,本文算法得到的 NC 值大于 0.98,比参考文献[12-13]中抵抗旋转攻击能力效果更明显。对于噪声、滤波和压缩等攻击,本文算法 NC 值都达到 0.99 以上并且普遍高于文献[12-13],通过对比实验可以得出本文算法的鲁棒性更强。

4 结 论

本文分析了增强奇异值分解中引入的最抗攻击缩放比例参数 β 具有随机性以及传统 SVD 分解水印算法中,对于提取出的水印存在对角线失真与虚警错误的问题,提出了一种增强奇异值的自适应零水印算法。水印通过原始灰度图像二值化与双置乱水印异或生成。利用天牛须优化算法自适应确定最优参数,以克服实验参数的随机性缺点,使水印的鲁棒性达到最佳。实验结果表明,本文在有效地解决水印图像的对角线失真与虚警错误问题的同时,在原始灰度图像受到剪切、滤波、噪声、压缩以及旋转等常见攻击下,所提取出的水印 NC 值均可达到 0.98 以上,有效提高了算法的鲁棒性。但该算法对于旋转上的抗攻击能力有待提高,需要进一步探究。

参考文献(References)

[1] Yi K X, Shi J Y, Sun X. Digital watermarking techniques: an introductory review [J]. Journal of Image and Graphics, 2001, 6A(2): 111-117. [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, 6A(2): 111-117.] [DOI: 10.11834/jig.20010229]

[2] Ye T Y. Perfectly blind self-embedding robust quantization-based watermarking scheme in DWT-SVD domain [J]. Journal of Image and Graphics, 2012, 17(6): 644-650. [叶天语. DWT-SVD 域全盲自嵌入鲁棒量化水印算法 [J]. 中国图象图形学报, 2012, 17(6): 644-650.] [DOI: 10.11834/jig.20120605]

[3] Zhu X, Ho A T S. A slant transform watermarking for copyright protection of satellite images [C]//Proceedings of the 4th International Conference on Information, Communications and Signal Processing, 2003 and the Fourth Pacific Rim Conference on Multimedia. Singapore: IEEE, 2003: 1178-1181. [DOI: 10.1109/ICICS.2003.1292646]

[4] Sikder I, Dhar P K, Shimamura T. A semi-fragile watermarking method using slant transform and LU decomposition for image authentication [C]//Proceedings of 2017 International Conference on Electrical, Computer and Communication Engineering. Cox's Bazar, Bangladesh: IEEE, 2017: 881-885. [DOI: 10.1109/ECACE.2017.7913027]

[5] Xiao Z J, Li N, Wang Y B, et al. Strong robust digital watermark algorithm based on contourlet singular value decomposition [J]. Computer Engineering, 2016, 42(9): 138-143. [肖振久,李南,王永滨,等. 基于 Contourlet 奇异值分解的强鲁棒数字水印算法 [J]. 计算机工程, 2016, 42(9): 138-143.] [DOI: 10.3969/j.issn.1000-3428.2016.09.025]

[6] Chen L, Ma X H. Blind watermarking algorithm based on DWT and SVD [J]. Software Guide, 2014, 13(1): 51-53. [陈璐,马小虎. 基于离散小波变换和奇异值分解的盲水印算法 [J]. 软件导刊, 2014, 13(1): 51-53.]

[7] Xiao Z J, Sun J, Wang Y B, et al. Wavelet domain digital watermarking method based on fruit fly optimization algorithm [J]. Journal of Computer Applications, 2015, 35(9): 2527-2530. [肖振久,孙健,王永滨,等. 基于果蝇优化算法的小波域数字水印算法 [J]. 计算机应用, 2015, 35(9): 2527-2530.] [DOI: 10.11772/j.issn.1001-9081.2015.09.2527]

[8] Yang J C, Li S X, Li L. Singular value decomposition and bee colony optimization based robust image watermark algorithm [J]. Control Engineering of China, 2017, 24(9): 1935-1941. [杨俊成,李淑霞,李亮. 基于奇异值分解与蜂群优化的鲁棒图像水印算法 [J]. 控制工程, 2017, 24(9): 1935-1941.] [DOI: 10.14107/j.cnki.kzgc.160376]

[9] Wen Q, Sun T F, Wang S X. 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]

[10] 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]

[11] Chen W Q, Li Q. A DWT-SVD based double-zero-watermarking algorithm [J]. Computer Engineering & Science, 2014, 36(10): 1991-1996. [陈伟琦,李倩. 基于 DWT-SVD 的图像双零水印算法 [J]. 计算机工程与科学, 2014, 36(10): 1991-1996.] [DOI: 10.3969/j.issn.1007-130X.2014.10.024]

[12] Xiao Z J, Zhang H, Chen H, et al. Zero-watermarking based on boost normed singular value decomposition and cellular neural network [J]. Journal of Image and Graphics, 2017, 22(3): 288-296. [肖振久,张晗,陈虹,等. 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): 288-296.] [DOI: 10.11834/jig.20170302]

[13] Rao Y R, Nagabhooshanam E. A novel image zero-watermarking scheme based on DWT-BN-SVD [C]//Proceeding of 2014 Inter-

national Conference on Information Communication and Embedded Systems. Chennai, India: IEEE, 2014: 1-6. [10.1109/ICICES.2014.7034073]

[14] Bao R, Zhang T Q, Tan F Q, et al. Semi-fragile watermark algorithm of color image based on slant transform [J]. Computer Engineering, 2012, 38(5): 122-125. [包锐, 张天骐, 谭方青, 等. 基于斜变换的半脆弱彩色图像水印算法 [J]. 计算机工程, 2012, 38(5): 122-125.] [DOI: 10.3969/j.issn.1000-3428.2012.05.037]

[15] Jiang X Y, Li S. BAS: beetle antennae search algorithm for optimization problems [EB/OL]. [2018-06-25]. https://arxiv.org/abs/1710.10724.

[16] Jiang X Y, Li S. Beetle antennae search without parameter tuning (BAS-WPT) for multi-objective optimization [EB/OL]. [2018-06-25]. https://arxiv.org/abs/1811.02395.

[17] Zhu Z Y, Zhang Z Y, Man W S, et al. A new beetle antennae search algorithm for multi-objective energy management in microgrid [C]//Proceedings of the 13th IEEE Conference on Industrial Electronics and Applications. Wuhan, China: IEEE, 2018: 1599-1603. [DOI: 10.1109/ICIEA.2018.8397965]

[18] Xu Y, Zhang S W. Encryption algorithm of image blocking and double adaptive diffusion with Arnold mapping [J]. Journal of Image and Graphics, 2015, 20(6): 740-748. [徐亚, 张绍武. 基于 Arnold 映射的分块双层自适应扩散图像加密算法 [J]. 中国图象图形学报, 2015, 20(6): 740-748.] [DOI: 10.11834/jig.20150602]

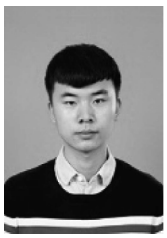
[19] Dhoka M S, Patki A. Robust and dynamic image zero watermarking using hessian laplace detector and logistic map [C]//Proceedings of 2015 IEEE International Advance Computing Conference. Banglore, India: IEEE, 2015: 930-935. [DOI: 10.1109/IADCC.2015.7154841]

[20] Fan Y J, Sun X H, Yan X D, et al. An image-scrambling a lgorithm Based on mixed chaotic sequences [J]. Journal of Image and Graphics, 2006, 11(3): 387-393. [范延军, 孙燮华, 阎晓东, 等. 一种基于混合混沌序列的图像置乱加密算法 [J]. 中国图象图形学报, 2006, 11(3): 387-393.] [DOI: 10.11834/jig.20060363]

[21] 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]

作者简介

肖振久, 1968 年生, 男, 副教授, 主要研究方向为图像与视觉信息计算、网络与信息安全、数字水印。
E-mail: 892380517@qq.com



姜东, 通信作者, 男, 硕士研究生, 主要研究方向为数字水印。
E-mail: 892390517@qq.com

张晗, 女, 硕士, 主要研究方向为数字水印。E-mail: 517185264@qq.com

唐晓亮, 男, 讲师, 主要研究方向为半监督学习、神经网络。E-mail: 1016841322@qq.com

陈虹, 女, 副教授, 主要研究方向为网络安全。E-mail: 2242892018@qq.com