

一种使用机器学习方法的数字水印算法

作者：孙晓霞，佟国香 发表时间：2021年

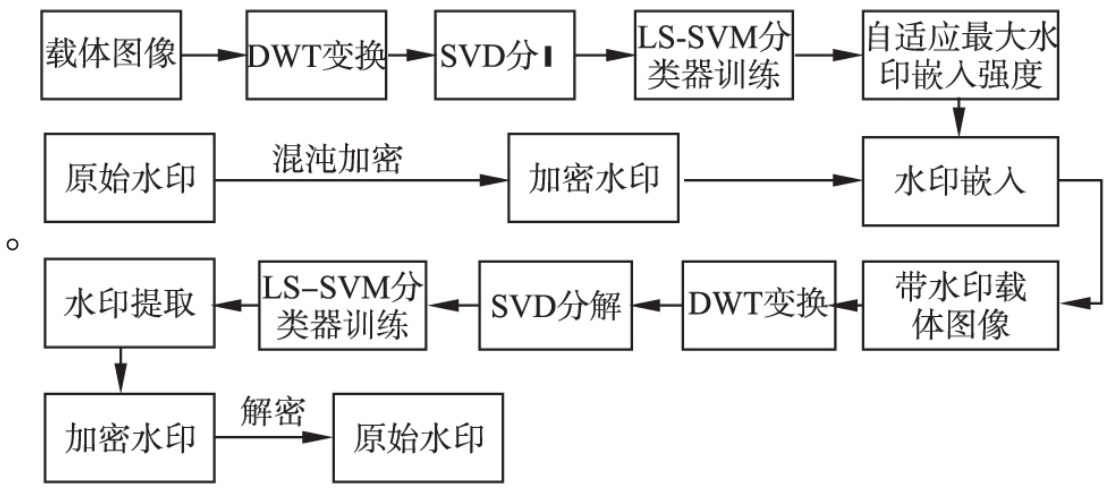
期刊：小型微型计算机系统 第2期第42卷

1. 主要内容

- 该文针对数字水印算法存在的不足，将离散小波变换和奇异值分解相结合，提出了一种基于机器学习的图像数字水印算法。其主要过程是：将载体图像进行一级小波变换，提取其低频子带图像对其进行4x4分块处理，然后对每一块进行奇异值分解后嵌入水印，并提取特征向量用于最小二乘支持向量机的训练，训练好的最小二乘支持向量机用于自适应最大水印嵌入强度的计算以及水印的盲提取。
- 该文先介绍了一些简单的图像数字水印算法，然后分析了他们的缺点，比如空域水印算法快捷，但是鲁棒性、透明性差；变换域和基于变换域算法较为复杂，透明性和鲁棒性有所提高，但是其抵抗旋转缩放等攻击的能力整体较低。而随着机器学习的发展，许多基于机器学习的算法被应用于图像数字算法领域，其可以解决参数优化和水印盲提取两个问题，但是使用机器学习的水印算法在不同程度上实现了更好的鲁棒性与透明性，但是在参数优化以及算法复杂度等方面仍然存在很大的提升空间。基于以上的问题，该文将DWT和SVD相结合，提出了基于机器学习的图像数字水印算法

2. 基本原理

- 该文将算法分为自适应最大水印嵌入强度、水印嵌入、LSM-SVM分类器的训练和水印提取四个部分，算法流程图见图



- 混沌加密算法：是混沌理论的一个重要应用领域，混沌加密算法具有伪随机性、便利性和对初值敏感等特性，在水印加密中被广泛使用。
- 自适应最大水印嵌入强度：自适应最大水印嵌入强度算法根据不同图像子块的相关特征来计算对应的最大水印嵌入强度，利用 LS-SVM 分类器进行预测分类。

3. 不足与缺点

- 该文在后半段对提出的方法进行了实验验证，结果表明该文提出的算法抵抗抵抗常规攻击的能力较高且保持均衡，适用性较广，在面对剪切、缩放等几何攻击时，算法的鲁棒性和复杂度较优，但是这个算法也有不足之处，如抵抗中值滤波攻击时鲁棒性较弱，有待于提高。

4. 总结

- 通过阅读这篇论文，知道水印的应用和研究不仅仅局限于几类算法中，还有很多领域和方法可以进行交叉。机器学习和深度学习也一直在学习，这个星期还了解了一点基于GAN的水印算法，只不过是通过视频进行学习，主要原理还是用GAN网络进行训练和监督水印的生成，最终生成一个鲁棒性透明性较好的水印。