一种基于特征空间分解的非对称鲁棒水印方法

作者：谭秀湖，刘国枝，王雪松 发表时间：2006年

期刊：电子学报 第34卷第11期

主要内容：

- 针对数字图像的版权保护，提出了一种基于特征空间分解的非对称数字水印方法，即对数字图像的特征空间分解，将水印嵌入到最少受图像改变影响的子空间，使嵌入的水印具有鲁棒性。同时，因水印嵌入矩阵（密钥）与提取矩阵（公钥）不同，可公开除密钥外所有其他信息。通过对特征子空间选取限制，算法具有高的检测概率和安全性，低的虚警概率。
- 数字水印技术大多采用了对称方式，即水印检测密钥与嵌入密钥相同，这就导致严重安全问题。因为密钥还可用于移去水印，在水印检测时，需出示私人密钥，且密钥一旦暴露，攻击者就能伪造、修改和移去水印，从而背离了版权保护目的，且在所有权鉴别时会出现无法判别版权真正所有者的问题。而采用非对称水印可以解决水印的安全问题，并且同时满足Kirckhoffs准则，其采用两套钥匙，公钥和密钥。密钥用于嵌入，公钥用于检测。公钥不能移除水印，而密钥是不公开的，所以攻击者将无法伪造、修改和移除水印，从而达到版权保护的目的，且密钥可鉴别版权所有者。
    - Kirckhoffs准则：一个安全保护系统的安全性不是建立在它的算法对于对手来说是保密的，而是应该建立在它所选择的密钥对于对手来说是保密的。

主要步骤：

- 先在时域将水印W_0嵌入到图像中生成I,生成含水印图像I_W，对I和I_W分别进行离散余弦变换DCT2（或离散小波变换DWT），得到系数矩阵A和A_W
- 模仿攻击者对I_W进行各种操作（如旋转，模糊和锐化的等），得到一组图像
- 在DCT2域中计算这组图像的数学期望A_g
- 将A_g和A_W按照矩阵列顺序展开为列矢量cs(A_g)和cs(A_W)后，再对cs(A_g)和cs(A_W)作差，得到特征向量α（α为随机变量）
- 计算α的协方差矩阵，对协方差矩阵进行奇异值分解（SVD），得到酉矩阵（协方差矩阵为对称矩阵，SVD分解后两个酉矩阵相同）为特征空间Z，将Z分为两个子空间，X空间和正交补Y空间。
- 其中X（水印嵌入空间）为Z中较小的特征值对应的特征向量张成，因而X为最不受I变化影响空间，使得嵌入水印具有鲁棒性，而Y为Z较大特征值对应的空间，受I变换影响明显

安全分析：

- 对信息隐藏和嵌入算法，安全性是至关重要，是性能评价重要组成部分，该文算法从Projection攻击，盲攻击（在仿真中给出），拷贝攻击，Oracle攻击和掩蔽攻击进行分析。
- 通过理论分析和实验结果，该文证明了基于特征空间分解的非对称鲁棒水印是一种可行的水印方法，有较高的安全性和鲁棒性。但是该文提出，在作水印提取时，需要原始图像，未能做到盲提取。

总结

- 这篇论文一开始以较短的篇幅介绍了非对称水印的主要步骤，随后使用大量的篇幅对构造非对称算法所涉及的线性代数进行讲述，出现大量的公式和相关证明，文章还在安全分析通过理论证明水印对待攻击的能力强，并在仿真实验中给出实验结果。
- 这样的论文是第一次阅读，有些地方还是比较难以理解，使用公式进行证明的理论结果和通过实验验证是非常简洁有力的，后续自己也需要加强对理论知识的了解和相关的基础知识