第35卷 第21期 计 算 机 工 程 2009年11月
Vol.35 No.21 Computer Engineering November 2009
·安全技术· 文章编号：1000—3428(2009)21—0169—02 文献标识码：A 中图分类号：TP311.02

基于SIFT特征的公钥水印算法

吕林涛，王 伟
(西安理工大学计算机科学与工程学院，西安 710048)

摘 要：针对现有公钥水印算法抗几何攻击能力弱的问题，提出一种利用SIFT特征实现抗RST攻击的公钥水印算法，采用SIFT算法对原始图像的特征点进行提取，构造局部特征区域，并在其DCT域中嵌入水印信息，使嵌入水印后的图像能够更好抵御RST攻击，从而满足公钥水印可公开检测的要求。实验结果表明，该算法能够有效抵抗RST攻击和一般信号处理的攻击。

关键词：公钥数字水印；SIFT特征；RST攻击

Public-key Watermark Algorithm Based on SIFT Feature

LV Lin-tao, WANG Wei
(Institute of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048)

【Abstract】 Aiming at the weak robust to the geometric attacks of the public-key watermark algorithm, a public-key watermark algorithm based on Scale Invariant Feature Transform(SIFT) is proposed for resisting Rotation Scale Translation(RST) attack in this paper. The feature keypoints of original image are extracted. The watermark in the DCT domain of the feature zone is embedded, so that it can resist the RST attack better, and the verification of the watermark is public. Experimental results demonstrate this algorithm can resist general RST attacks and signal processing attacks.

【Key words】 public-key digital watermark; Scale Invariant Feature Transform(SIFT) feature; Rotation Scale Translation(RST) attack

1 概述

目前广泛使用的数字水印技术大多采用对称密钥形式，即整个水印系统采用相同的密钥，这限制了水印技术的实用性，因此，数字水印的公开验证成为一个急需解决的问题。

RST(Rotate Scale Transform)攻击是最为常见的水印攻击方式的一种，这种攻击可以轻易实现，并且可以有效破坏现有大部分水印算法。目前，抵抗一般性几何攻击采用的主要方法是利用原始数据的重要不变特征。如文献[1]利用Harris算子提取图像特征点，将水印嵌入由特征点所构成的三角形表征区域中；文献[2]提出将水印信息嵌入到图像关键点构造的圆形表征区域中；文献[3]利用图像归一化具有仿射不变性进行水印嵌入。

本文针对公钥水印存在的2个关键性问题：公开验证和抗RST攻击，提出一种基于SIFT特征抗RST攻击的公钥水印方法，该算法在文献[4]的基础上对于水印的嵌入和密钥的生成进行改进，并采用SIFT(Scale Invariant Feature Transform)算法[5]，将水印信息嵌入在RST变换的不变域内，实现了水印图像在对旋转、缩放、噪声等变换都具有不变性，增强公钥水印算法的鲁棒性。

2 图像的SIFT特征

SIFT 算法是公认的在图像之间进行特征点匹配的有效方法之一。这种特征在对于图像的平移、旋转和仿射变换等方面都具有很强鲁棒性。SIFT特征的构造主要包括2个主要步骤：图像特征点提取和SIFT描述子的构造[5]。

原始图像通过不同尺度的高斯核进行滤波和下采样，形成高斯金字塔图像，对每层图像以不同标准差的高斯核生成图像组，在图像组中计算出高斯差分图像DoG(Difference of Gaussian)的局部极值点，即通过式(1)和式(2)求解得到。

$$G(x,y,\delta)=\frac{1}{2\pi\sigma^2}\exp(-\frac{(x^2+y^2)}{2\delta^2}) \quad (1)$$

$$D(x,y,\delta)=[G(x,y,k\delta)-G(x,y,\delta)]f(x,y) \quad (2)$$

其中，$G(x,y,\delta)$表示二维高斯函数；$f(x,y)$表示金字塔的每层图像；计算所得的局部极值位置即特征点的位置。对于每个点计算其在各个尺度下DoG算子的响应值，得到特征尺度轨迹曲线，取该曲线的局部极值点为该特征点的尺度。根据文献[2]，本文选取尺度在2~10之间的特征点，这是因为图像经过改变后，尺度过小的特征点可能检测不到，而尺度过大的特征点会发生偏移。

3 公钥水印算法

本文提出的公钥水印算法是由密钥生成、水印嵌入和水印检测3个部分构成的。

3.1 密钥生成算法

本文采用logistic映射产生水印系统的密钥序列，由该映射产生的序列具有初值敏感、表现形式复杂等特点。映射公式定义为

$$x_{n+1}=1-2x_n^2,\ x_n\in[-1,1] \quad (3)$$

其中，序列x_n是通过给定的初值x_0迭代所产生。密钥的生成过程如图1所示，其中，Key_{sup}表示用户的超级密钥，作为初值通过式(3)生成混沌序列x_k；密钥Key_p，Key_{in}和Key_{DCT}都从序列x_k中随机选取；Key_p表示公开密钥，用于对水印进行置乱；Key_{in}表示行索引密钥，用以确定水印的嵌入位置；

基金项目：西安市2008年科学技术计划基金资助项目(CXY08017)
作者简介：吕林涛(1955－)，男，教授，主研方向：计算机网络，网络信息安全，数据挖掘；王 伟，硕士研究生
收稿日期：2009-06-10 **E-mail：**lvlintao@xaut.edu.cn

Key_{DCT} 表示加密系数密钥，选取需嵌入水印的 DCT 系数。

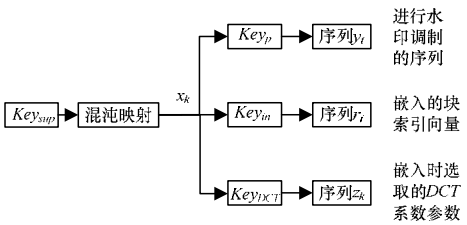

图 1　密钥的生成过程

3.2　水印嵌入算法

本文利用由 SIFT 算法提取图像特征点构成的区域实现水印嵌入，其实现过程如图 2 所示。

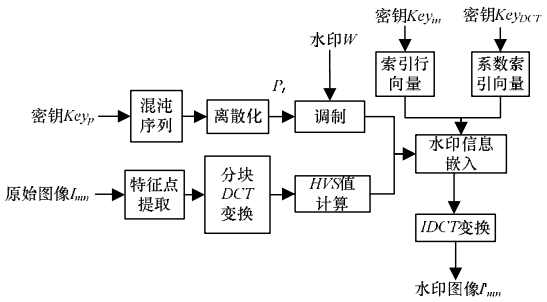

图 2　水印的嵌入过程

水印嵌入算法描述如下：(1)将原始图像进行 8×8 分块，对于图像中提取出的特征点集 P_k，$k=1,2,\cdots,k$ 所在的分块进行标记，所有标记的块总数为 T。(2)密钥 Key_{in} 生成随机排列的区域块向量索引 $\boldsymbol{I}_{index}$，$\forall i,j,\boldsymbol{I}_{index}(i)\in\{1,2,\cdots,T\}$，且如果 $\boldsymbol{I}_{index}(i)=\boldsymbol{I}_{index}(j)$，当且仅当 $i=j$。设水印信息为 w_t，$t=1,2,\cdots,k$，则水印信息将依次嵌入到原始图像的第 $\boldsymbol{I}_{index}(t)$ 块中。(3)对于所标记的区域进行 *DCT* 变换，所得的 *DCT* 系数块记为 F_t，求取各块的 *JND* 值。(4)利用密钥 Key_{DCT}，从 F_t 中选取 2 个中低频系数，记为 $F_t(i,j)$ 和 $F_t(k,l)$，嵌入规则如表 1 所示。

表 1　水印嵌入规则

嵌入条件	嵌入方法
当 $w_t=1$ 并且	$F_t(i,j)=F_t(i,j)\cdot(1+(JND)/2)$
$F_t(i,j)-F_t(k,l)<JND$	$F_t(k,l)=F_t(k,l)\cdot(1-(JND)/2)$
当 $w_t=-1$ 并且	$F_t(i,j)=F_t(i,j)\cdot(1-(JND)/2)$
$F_t(k,l)-F_t(i,j)<JND$	$F_t(k,l)=F_t(k,l)\cdot(1+(JND)/2)$

重复步骤(4)，直到所有的水印信息都嵌入到所标记的区域内，最后将嵌入水印后的 F_t 进行 *IDCT* 反变换，得到含有水印信息的图像。

3.3　水印检测算法

在本方案中采用的是盲水印，所以，在水印的提取或检测时不需要原始图像，只需要水印信息在原始图像的位置序列和特征区域在变换域的系数，即可进行水印的提取或检测。

私钥的提取方法就是水印嵌入的逆过程，算法描述如下：

(1)利用私钥 Key_{sup} 生成解调混沌序列，通过密钥 Key_{in} 确定水印嵌入的位置，*DCT* 系数选择密钥序列以及水印解密密钥 Key_p。

(2)将水印图像 I' 进行 8×8 分块，并通过索引向量 $\boldsymbol{I}_{index}$ 和密钥 Key_{DCT} 提取出经过加密后的水印信号。设提取水印信息为 w'_t，$t=1,2,\cdots,k$，则

$$w'_t=\begin{cases}1 & F_t(i,j)-F_t(k,l)\geq 0\\ -1 & \text{other}\end{cases} \tag{4}$$

然后对 w'_t 进行解调，即 $w'_k=w'_t\cdot p_t$，其中，p_t 由密钥 Key_p 产生。按上述方法依次提取水印信息位，直到所有水印信息提取出来。

公钥用于水印的检测，方法与私钥水印提取的方法近似。需要 2 个主要步骤：首先，通过密钥 Key_{in} 来确定水印所嵌入的位置序列；再通过 Key_{DCT} 密钥确定水印的嵌入系数；水印检测采用假设检验方法，定义如下：

$$H_0:F=f,H_1:F=f+w \tag{5}$$

其中，假设 H_0 表示假定进行检测的图像不含水印信息；假设 H_1 假定接受检测的图像含有水印。根据 Neymann-pearson 准则来计算决策阈值 L_r，并计算出所要检测图像的似然比 L，若 $L>L_r$，则判定水印存在；若 $L<L_r$，则判定水印不存在。

4　实验结果分析与比较

实验采用原始载体图像是 512×512 的 Lena 作为实验图像，选择随机长度为 128 bit 的二值序列作为水印。实验结果如图 3 所示。

(a)原始图像　(b)特征点图像　(c)水印图像

图 3　实验结果

实验针对 10 张不同的原始图像进行水印嵌入，测试了整个水印算法对旋转、缩放、平移(RST)等不同的几何攻击和其他攻击方式的鲁棒性。表 2 给出了私钥所提取出的水印与原始水印信息进行比较得到的相关值。表 3 给出了水印图像经过攻击后，仍可以检测到水印信息的图像数量。

表 2　私钥提取水印的相关值

攻击类型	水印的相关值	
	本文方法	文献[4]方法
锐化	1.00	1.00
JPEG(压缩 80%)	0.90	0.89
行列去除(4 行 8 列)	0.68	0.34
剪切(1/4)	0.96	0.78
缩放(10%)	0.84	0.24
旋转(5°)	0.74	0.31
叠加噪声(高斯)	1.00	1.00
水平平移(30)	0.74	0.61
滤波(低通滤波)	0.90	0.92

表 3　各类攻击的检测结果

攻击类型	图像检测的相关值					
	Lena	Peppers	Lake	Baboon	Boats	Barbara
锐化	9	10	10	10	9	10
JPEG(压缩 80%)	10	10	10	10	9	10
行列去除(4 行 8 列)	10	10	9	10	10	10
剪切(1/4)	9	7	8	6	7	8
缩放(10%)	10	8	9	10	9	10
旋转(5°)	8	7	6	7	6	7
叠加噪声(高斯)	9	10	10	9	10	10
水平平移	9	10	9	10	8	9

（下转第 173 页）