

基于约束随机分块的 NMF 图像哈希算法

项世军^{*①} 杨建权^②

^①(暨南大学信息科学技术学院 广州 510632)

^②(中国科学院深圳先进技术研究院 深圳 518055)

摘要: 基于非负矩阵分解(Non-negative Matrix Factorization, NMF)的图像哈希(image hashing)算法对图像有损压缩, 低通滤波、尺度拉伸等处理具有很好的稳健性, 但对图像旋转比较敏感。为此, 该文在对 NMF 哈希算法的分块模式进行深入研究的基础上, 提出一种可抗旋转攻击的 NMF 图像哈希算法。该方法通过对随机分块的区域进行限制, 并选择合适的分块尺寸来减轻旋转攻击对图像造成的不良影响, 从而提高了特征的旋转稳健性。实验表明, 所提出的图像哈希算法在保持原 NMF 哈希算法对其它攻击稳健性的同时, 能有效地抵抗旋转攻击。

关键词: 图像处理; 图像哈希; 非负矩阵分解; 稳健性; 旋转

中图分类号: TN911.73

文献标识码: A

文章编号: 1009-5896(2011)02-0337-05

DOI: 10.3724/SP.J.1146.2010.00212

NMF-Based Image Hashing Algorithm Using Restricted Random Blocking

Xiang Shi-jun^① Yang Jian-quan^②

^①(School of Information Science and Technology, Jinan University, Guangzhou 510632, China)

^②(Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518055, China)

Abstract: The NMF (Non-negative Matrix Factorization)-based image hashing is robust to common image operations (such as lossy compression, low-pass filtering, resolution scaling and etc.), but is sensitive to rotation operations. After carefully investigating the blocking strategy of the original NMF-based scheme, a rotation-resilient image hashing algorithm is proposed. The proposed algorithm reduces the undesirable effect induced by image rotation through constraining blocking range and adopting appropriate block size, and thus provides better robustness to image rotation. Experimental results demonstrate that the proposed hashing algorithm provides a satisfactory robustness to image rotation while keeping its performance to common image processing operations.

Key words: Image processing; Image hashing; Non-negative Matrix Factorization (NMF); Robustness; Rotation

1 引言

图像哈希(image hashing)是图像数据的一种紧凑表达, 可用于图像内容真实性认证和基于内容的图像检索。用于认证的图像哈希需对常见的图像处理操作和几何失真稳健, 同时要能检测恶意的篡改^[1,2]。

目前已有的图像哈希算法中, 文献[1]利用DCT系数的相对关系来生成哈希值; 文献[3]则利用DCT系数本身来构造哈希函数; 文献[4]引入DCT频率敏感度矩阵来计算哈希值; 文献[2]提出一种基于图像小波分解的哈希构造方法; 文献[5]提取V变换域上

的系数来产生哈希值; 文献[6]结合DCT变换、Watson视觉模型和混沌模型来设计哈希算法。上述哈希方案对有损压缩、低通滤波等操作稳健, 但一个共同缺点是不能有效抵抗旋转、拉伸等几何攻击。在目前已提出的针对几何攻击的图像哈希算法中, 文献[7]的基于直方图形状的图像哈希算法能有效地抵抗几何失真; 文献[8]用傅里叶幅度谱极坐标变换的平移、旋转不变性来设计哈希算法; 文献[9]用SVD(Singular Value Decomposition)来构造哈希函数。上述3种哈希方案对图像的几何失真稳健, 但在图像特征的选取上存在不足^[10]。非负矩阵分解(NMF)能有效获取图像的特征^[11], 近年来在图像哈希研究中受到了高度重视^[12,13]。文献[12]利用图像的NMF特征向量来设计哈希, 对常见的图像处理操作及裁剪、拉伸等几何失真稳健。孙悦等人^[13]改进了NMF算法的稳定性, 用于图像检索。本文大量的实验及

2010-03-09 收到, 2010-09-23 改回

国家自然科学基金(60903177), 中央高校基本科研业务费专项资金(21609412), 博士点新教师基金(200805581048)和中国青年科学基金(61003297)资助课题

*通信作者: 项世军 xiangshijun@gmail.com

分析表明, 基于NMF的哈希算法(以标志性成果^[12]来进行说明)对图像旋转的稳健性并不十分理想。因此, 利用NMF来设计可抗图像常规处理和几何失真的哈希、要取得更好的图像认证性能, 仍需要进一步的深入研究。

针对哈希算法的旋转稳健性问题, 本文对基于NMF的哈希算法^[12]进行了深入研究, 取得了一些新的有意义的成果: (1)通过理论分析结合实验的方式考察了图像旋转操作对图像像素造成的影响; (2)通过分析这些影响, 提出了一种带约束的随机分块方法; (3)利用新的随机分块方法, 结合文献^[12]中哈希的计算方法, 设计了一种抗旋转攻击的图像哈希算法。实验结果表明, 所设计的哈希算法不仅对叠加噪声、低通滤波等稳健, 而且能有效地抵抗图像的旋转, 很好地解决了分块 NMF 哈希算法的旋转稳健性问题。

本文第2节简述文献^[12]所提出的NMF哈希方法; 第3节详细介绍所提出的带约束机制的随机分块策略; 第4节是NMF算法在新的分块机制使用前后的实验数据对比; 第5节是结论。

2 NMF 图像哈希算法

NMF 是在矩阵中所有元素均为非负数的约束条件下的矩阵分解方法^[11]。文献^[12]以NMF为特征提取手段, 所提出的哈希算法稳健性原理可简述如下: (1)对图像进行分块并分别计算哈希, 故哈希具有一定的篡改定位能力; (2)由于哈希值是通过NMF低秩分解图像块¹⁾后计算所得, 故算法对有损压缩、过滤和加噪等操作具有稳健性; (3)由于哈希在计算前对图像大小进行了归一化处理, 故哈希能抵抗一定的裁剪和拉伸。

然而, 我们的研究发现: 由于旋转前后图像内容发生了改变并且每一个图像块内容有很大的失真, 故该算法对图像旋转非常敏感。下面的章节中, 我们对旋转造成的图像和图像块的失真进行了分析, 在此基础上提出了带约束机制的随机分块策略、用于替换算法^[12]的自由分块策略, 以改善算法对旋转的稳健性。

3 带约束的随机分块策略

3.1 旋转对图像的影响分析

图像旋转有两种典型的模式: “Loose”模式和“Crop”模式, 我们分别讨论。

(1) “Loose”模式的全局旋转 “Loose”模式旋转效果见图1。注意到图1(b)比1(c)在圆周内的

内容更为丰富, 原因是“Loose”旋转模式会使旋转后图像较原图大, 因算法^[12]预处理时要归一化尺寸, 故更多的内容进入到圆周内。同时, 图像旋转后引入了不属于原图像的区域(即一些外来像素, 如图1(a)中的黑色区域)。



图1 “Loose”模式旋转效果

为使旋转图像在进行分块时不受外来像素的影响, 可以限制随机分块的范围。本文定义图1(b)的白色圆周半径为分块范围半径 R 。根据几何学原理(图2), 可以导出 R 的表达式:

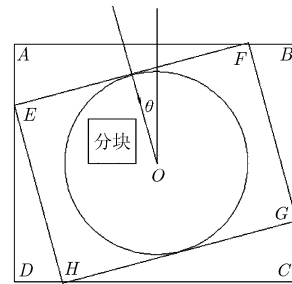


图2 “Loose”模式分块范围

$$\left. \begin{aligned} \overline{EF} &= \frac{\overline{AB} \cdot \cos\theta - \overline{BC} \cdot \sin\theta}{\cos 2\theta} \\ \overline{FG} &= \frac{\overline{BC} \cdot \cos\theta - \overline{AB} \cdot \sin\theta}{\cos 2\theta} \end{aligned} \right\} \quad (1)$$

那么 $R = (1/2)\overline{FG}$ (\overline{FG} 为短边)。

由图2及 R 的表达式可以看出: 为了克服因旋转引入的外来像素的影响, 旋转角度($\theta \leq 90^\circ$)越大, 分块范围半径 R 应越小。

(2) “Crop”模式的全局旋转 “Crop”模式旋转效果如图3所示。旋转图像与原图的尺寸相同, 部分区域由于移出图像边框而被裁剪, 部分区域则被外来像素填充。

注意到图3(b)与3(c)圆周内的像素只是发生了相对位移。可以在图3(b)所示的白色圆周内进行随机分块, 从而消除裁剪像素和填充像素对哈希计算的影响。可见, “Crop”模式的分块范围半径为图像短边的一半, 而与旋转角度的大小无关。

¹⁾ NMF 低秩分解所得的特征向量反映了低频信息。



图 3 “Crop” 模式旋转效果

3.2 旋转对图像块的影响分析

由对“Crop”模式旋转的分析知, 分块范围半径内的像素在旋转前后只是发生偏移, 因此, 旋转前后同一分块中存在公有的像素。研究发现, 公有像素占块内像素的比例与 NMF 哈希算法的旋转稳健性有着重要关系。本文对旋转前后图像块公有像素的比例进行了理论上的估算, 以便在图像哈希的实施过程中对分块范围半径和分块尺寸の設定进行指导。

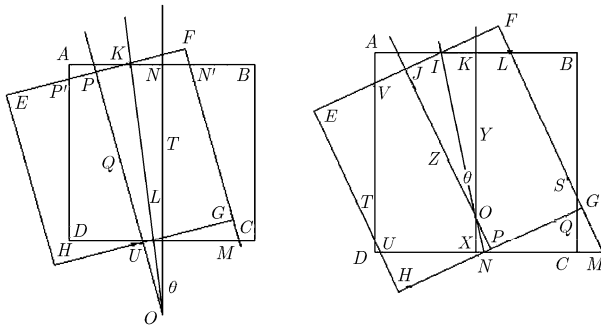
对分块是否包含图像中心分别讨论。

(1) 分块不包含图像中心 图 4(a)中, 点 O 为图像中心, $\square ABCD$ 为分块所在位置, 图像旋转 θ 度后, 偏移至 $\square EFGH$ 处。因此, 旋转前后分块公有像素的比例等于多边形 $P'KN'GLD$ 的面积占分块面积的比例。设分块中心到图像中心 O 的距离为 R , 分块为 $a \times a$ 的正方形, 则重合面积为

$$S_{P'KN'GLD} = \frac{1}{2}(\overline{AK} + \overline{LG}) \cdot (1 + \cos^{-1}\theta) \cdot a - \frac{1}{2} \cdot (\overline{AK}^2 + \overline{LG}^2) \cdot \tan\theta \quad (2)$$

式中 $R > \frac{a}{2}$ 。 $\overline{AK} = \frac{a}{2} - \left(R + \frac{a}{2}\right) \cdot \tan\frac{\theta}{2}$, $\overline{LG} = \frac{a}{2} - \left(R - \frac{a}{2}\right) \cdot \tan\frac{\theta}{2}$ 。

(2) 分块包含图像中心 由图 4(b)可以看出, 重合面积为八边形 $VILSQNUT$ 的面积。即



(a) 分块不包含图像中心 (b) 分块包含图像中心

图 4 分块公有像素计算的两种情形

$$\begin{aligned} S_{VILSQNUT} &= S_{ALMD} - S_{AIV} - S_{NGM} - 2S_{SQG} \\ &= \frac{1}{2}(\overline{AL} + \overline{MD}) \cdot \overline{AD} \\ &\quad - \frac{1}{2} \tan\theta \cdot (\overline{AI}^2 + \overline{NG}^2 + 2\overline{SG}^2) \quad (3) \end{aligned}$$

其中

$$\begin{aligned} \overline{AL} &= \left(1 + \frac{1}{\cos\theta}\right) \cdot \overline{AI} \\ \overline{MD} &= \overline{DC} + \frac{\overline{NG}}{\cos\theta} - \overline{XC} + \overline{NP} \\ \overline{AI} &= \overline{AK} - \overline{OK} \cdot \tan\frac{\theta}{2} \\ \overline{NG} &= \overline{NP} + \overline{PG} \\ \overline{SG} &= \overline{FG} - \overline{FL} - \overline{LS}, \quad \overline{FL} = \overline{AI} \cdot \tan\theta \\ \overline{LS} &= \frac{\overline{LB}}{\sin\theta} = \frac{1}{\sin\theta} \left[\overline{AB} - \overline{AI} \cdot \left(1 + \frac{1}{\cos\theta}\right) \right] \end{aligned}$$

由图 4 及推导过程可知, 旋转前后分块公有像素的比例与分块中心到图像中心的距离(称之为两心距离)、分块尺寸及旋转角度有关。两心距离越短、旋转角度越小、分块越大, 则公有像素比例越大。

上述对旋转前后分块公有像素比例公式的推导是在两心连线为垂直线的情况下进行的。当两心连线不为垂直线或水平线时, 上述公式不严格成立, 但可以用作估算, 估计精度是令人满意的。

推导上述公有像素比例估算公式的目的在于进行随机分块的图像哈希算法在选择分块范围及分块大小时提供一种参考²⁾, 也为我们从公有像素比例的角度研究分块 NMF 哈希算法对旋转攻击的稳健性提供了理论上的指导。

3.3 带约束的随机分块策略

基于上述分析, 带约束的随机分块策略可表述如下:

(1) 设算法要抵抗的“Loose”模式旋转角度为 θ , 根据式(1)计算分块范围半径 R 。将该值视作分块范围半径的取值上限。

(2) 调整分块范围半径(或两心距离)和分块大小 a , 使分块公有像素比例达到期望值。

(3) 以图像中心为圆心, 在分块范围半径限定的区域内进行大小为 a 的矩形划分。

本文使用上述的约束随机分块方法代替了 NMF 哈希算法^[12]的自由随机分块方法, 从而得到改进后的 NMF 哈希算法。改进算法的主体部分与原算法是一致的, 因此不会增加算法的计算复杂度。

²⁾ 尤其对基于图像局部统计特性的哈希方案有明显的指导意义, 因为旋转前后同一分块的公有像素比例越高, 统计特性保持得越好。

4 实验测试

设置 NMF 哈希算法^[12]的参数为 $p=10$, $m=100$, $r_1=1$, $r_2=1$, $M=64$ 。对 400 幅 256×256 的灰度图像进行 16° 两种模式的旋转, 原算法与改进算法的抗旋转性能的实验结果比较如下。

(1)对“Loose”旋转稳健性的改善 分块范围半径设置为 100(pixel)。由图 5(a)的 ROC 曲线(Receiver Operating Characteristic, 又称误警率-漏警率曲线)可以看出, 采用带约束的随机分块方法的算法 ROC 曲线总在原算法^[12] ROC 曲线的下方。这表明基于旋转考虑的随机分块策略用于 NMF 图像哈希时取得了更好的抗“Loose”模式旋转的稳健性能。

(2)对“Crop”旋转稳健性的改善 分块范围半径设置为 128(pixel), 即图像短边的一半。由图 5(b)的 ROC 曲线可以看出, 采用带约束机制的分块方法的算法 ROC 曲线在原算法 ROC 曲线的下方, 表明改进算法比原算法对“Crop”模式的旋转更稳健。

(3)对类噪声攻击的稳健性 以对图像的高斯噪声干扰和高斯低通滤波为例, 通过实验评估改进算法对类噪声攻击的稳健性能。

实验参数设置与上述(2)实验的参数相同。向测试图像叠加的高斯噪声的均值为 0, 标准差为 40; 对测试图像进行高斯低通滤波时, 高斯核的标准差为 11, 滤波模板大小为 21×21 。由图 5(c), 5(d)的 ROC 曲线可以看出, 改进算法和原算法对高斯噪声干扰和高斯低通滤波的 ROC 曲线基本重合, 表明约束随机分块策略在增强原 NMF 哈希算法旋转稳健性的同时, 也很好地保持了其对类噪声攻击的稳健性。

(4)两心距离对旋转稳健性的影响 基于 3.2 节的分析, 公有像素的比例与两心距离和分块尺寸有关。本文首先改变两心距离以考察其对改进算法旋转稳健性的影响。需要指出的是, 图 5(e), 5(f)中圆括号内的百分比表示边缘分块旋转前后公有像素的比例。因此, 该数值表示的是在最不利的情况下(所有分块离图像中心最远时)的公有像素比例。

对 400 幅 256×256 的图像作 8° “Crop”模式旋转。分块尺寸保持为 50×50 。两心距离发生变化时, ROC 曲线的变化情况如图 5(e)所示。可以看出, 随两心距离的缩小, 分块在旋转前后公有像素比例增加, ROC 曲线往原点位置移动, 表明旋转稳健性

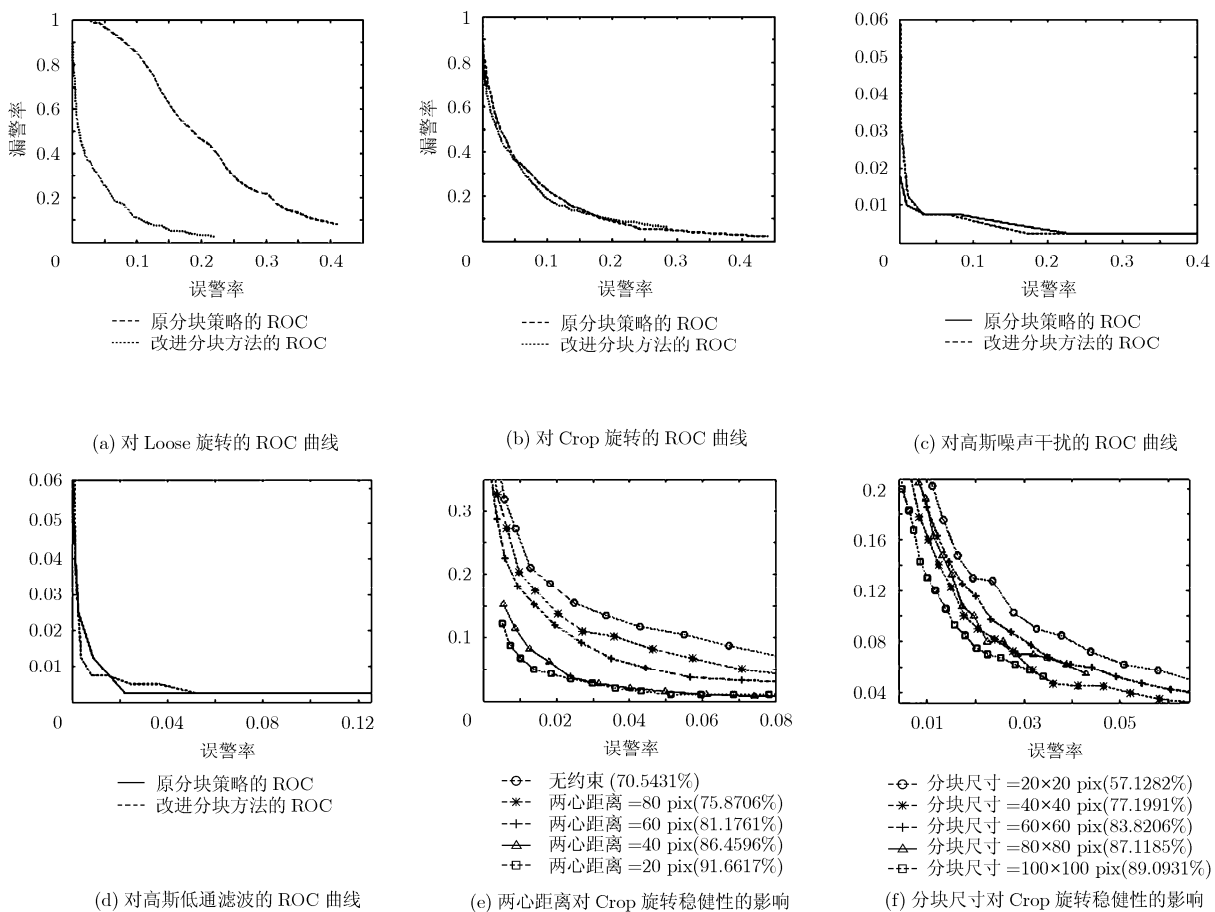


图5 实验测试结果

越好。

(5)分块尺寸对旋转稳健性的影响 分块尺寸对旋转前后公有像素的比例也有影响。这里, 我们评估分块尺寸对旋转稳健性的影响。对 400 幅 256×256 的图像作 8° “Crop”模式的旋转。两心距离保持为 60(pixel), 分块尺寸发生变化时, ROC 曲线的变化情况如图 5(f)所示。

随分块尺寸变大, 旋转前后公有像素比例提高, 但改进算法对旋转的稳健性并不总是增强的。注意到改进算法在分块尺寸为 40×40 时比在 60×60 和 80×80 时的 ROC 曲线要好。原因是: 虽然分块尺寸的增大能使公有像素比例提高, 有利于旋转稳健性的增强; 但在同秩 NMF 下, 对越大的分块, NMF 提取到的特征越模糊, 从而导致算法唯一性下降。图 5(f)的数据是稳健性增强因素与唯一性下降因素综合影响的结果。

上述实验数据表明, 带约束的随机分块方法能有效改善 NMF 哈希算法对“Loose”模式旋转的稳健性; 对“Crop”模式旋转的稳健性也有一定程度的提高。在实际应用中, 还可以根据具体应用场合的需要, 通过调整两心距离和分块尺寸来获得更好的抗“Crop”模式旋转的性能。

5 结论

本文通过对图像旋转模式进行分析, 提出了一种基于新的随机分块模式的 NMF 哈希算法。主要工作如下: (1)分析了两种图像旋转模式(“Loose”和“Crop”)对图像内容的影响, 提出了对图像分块区域进行限制的策略。结果表明, 对分块区域进行限制可以有效地克服在图像旋转中由于外来像素的填充和图像内容的缺失给哈希带来的影响; (2)分析了分块大小对算法抗旋转性能的影响。实验结果表明, 选取合适的分块尺寸有利于提高哈希算法的抗旋转性能; (3)通过对分块区域及分块大小进行限制, 本文用 NMF 哈希算法进行了实施。结果表明, 所提出的基于新的分块模式的 NMF 哈希算法与原算法^[12]相比, 在抗旋转的稳健性上有了显著的提高。本文针对分块 NMF 哈希算法抗旋转性能进行了研究, 对基于分块的其它图像哈希算法^[1,3]的研究, 将会是下一阶段的工作。

参考文献

- [1] Lin C Y and Chang S F. A robust image authentication system distinguishing JPEG compression from malicious manipulation [J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2001, 11(2): 153-168.
- [2] Venkatesan R, Koon S M, Jakubowski M H, and Moulin P. Robust image hashing[C]. *IEEE Conference on Image Processing*, Vancouver, Canada, September 2000: 664-666.
- [3] 张维克, 孔祥维, 尤新刚. 安全鲁棒的图像感知哈希技术[J]. *东南大学学报(自然科学版)*, 2007, 37(增刊(I)): 188-192.
Zhang Wei-ke, Kong Xiang-wei, and You Xin-gang. Secure and robust image perceptual hashing [J]. *Journal of Southeast University (Natural Science Edition)*, 2007, 37(Sup.(I)): 188-192.
- [4] 秦川, 王朔中, 张新鹏. 一种基于视觉特性的图像摘要算法[J]. *中国图象图形学报*, 2006, 11(11): 1678-1681.
Qin Chuan, Wang Shuo-zhong, and Zhang Xin-peng. Image hashing based on Human visual system [J]. *Journal of Image and Graphics*, 2006, 11(11): 1678-1681.
- [5] 邹建成, 周红丽, 邓欢军. 一种安全鲁棒的图像哈希方法 [J]. *计算机应用研究*, 2009, 26(6): 2122-2124.
Zou Jian-cheng, Zhou Hong-li, and Deng Huan-jun. Secure and robust image hashing scheme [J]. *Application Research of Computers*, 26(6): 2122-2124.
- [6] 王阿川, 陈海涛. 基于离散余弦变换的鲁棒感知图像哈希技术 [J]. *中国安全科学学报*, 2009, 19(4): 91-96.
Wang A-chuan and Chen Hai-tao. Robust image perceptual hashing technology based on discrete cosine transform [J]. *China Safety Science Journal*, 2009, 19(4): 91-96.
- [7] Xiang Shi-jun, Kim Hyoung-joong, and Huang Ji-wu. Histogram-based image hashing scheme robust against geometric deformations [C]. *The 9th ACM Multimedia and Security Workshop*, New York, USA, September 2007: 121-128.
- [8] Swaminathan A, Mao Y, and Wu M. Robust and secure image hashing [J]. *IEEE Transactions on Information Forensics Security*, 2006, 1(2): 215-230.
- [9] Kozat S S, Venkatesan R, and Mihcak M K. Robust perceptual image hashing via matrix invariants [C]. *IEEE Conference on Image Processing*, Singapore, 2004: 3443-3446.
- [10] 何妙谊. 稳健及安全的数字图像签名的研究[D]. [硕士论文], 中山大学, 2007.
He Miao-yi. Robust and secure image hashing [D]. [MA. dissertation], Sun Yat-sen University, 2007.
- [11] Lee D D and Seung H S. Algorithms for non-negative matrix factorization [C]. *Neural Information Processing Systems 13*, Cambridge, MA: MIT Press, 2000: 556-562.
- [12] Kivanc M M. Robust and secure image Hashing via non-negative matrix factorizations [J]. *IEEE Transactions on Information Forensics and Security*, 2007, 2(3): 376-390.
- [13] 孙锐, 高隽. 组合 NMF 和 PCA 的图像哈希方法 [J]. *电子测量与仪器学报*, 2009, 23(5): 52-57.
Sun Rui and Gao Jun. Image Hashing method via combination of NMF and PCA [J]. *Journal of Electronic Measurement and Instrument*, 2009, 23(5): 52-57.

项世军: 男, 1974 年生, 副教授, 博士, 韩国高丽大学博士后, 研究方向为信息隐藏和多媒体信息安全。
杨建权: 男, 1985 年生, 硕士, 研究助理, 研究方向为信息隐藏和多媒体信息安全。