浙江理工大学学报，第 29 卷，第 1 期，2012 年 1 月
Journal of Zhejiang Sci-Tech University
Vol. 29, No. 1, Jan. 2012

文章编号：1673-3851 (2012) 01-0084-05

基于图像归一化和 DCT 的感知图像哈希算法

曾　勇，孙树森，夏爱军
（浙江理工大学信息学院，杭州 310018）

摘　要：提出一种基于离散余弦变换的感知哈希算法，先对原始图像进行归一化处理，使图像具有几何不变性，然后利用离散余弦变换进行图像特征系数的提取并用混沌序列发生器加密图像，最后通过量化和编码生成感知哈希序列。该算法可以抵抗任意角度的旋转攻击和仿射变换。

关键词：感知图像哈希；预处理；图像归一化；离散余弦变换；混沌加密；仿射变换
中图分类号：TP391　　**文献标识码**：A

0　引　言

数字技术和网络的快速发展使得图像、视频、音乐的复制和传播变得极为容易，因此数字产品的版权认证问题进入了人们的议题[1]。图像被认为是现实中信息传递的主要手段[2]，而感知图像哈希是感知哈希的一个重要分支[3]，因此感知图像哈希的研究具有重要意义。感知图像哈希技术可以将任意分辨率的图像数据转化为几百或几千比特的二值序列，而且满足鲁棒性、安全性、唯一性等要求[4]，可以用于图像版权认证。抗几何攻击的感知图像哈希是目前研究的重点[5-6]。特征提取是感知图像哈希生成的关键[7]。Monga 等[8]基于非负矩阵分解生成图像哈希的方法，虽然能有效抵抗几何攻击，但伪随机序列容易产生冗余。张维克等[9]利用图像 DCT 低频系数的感知不变性得到的安全哈希序列索引，具有较好的唯一性、鲁棒性和安全性，但是只能抵抗 3°以下的旋转。王阿川等[10]融合 DCT 模型、Watson模型和混沌模型产生感知图像哈希的方法，虽可以抵抗内容保持的修改操作，但是对几何变换敏感。可见，相对于特征提取部分的研究，预处理过程的研究还不够深入。

本文对图像归一化预处理后的图像进行特征提取，然后对特征值进行加密、量化、编码生成感知图像哈希序列。本方法可以抵抗任意角度的旋转攻击，并对其它几何攻击也有很好的效果。

1　感知图像哈希的基本框架

现有的感知哈希生成框架基本包含 3 个部分：特征提取、量化和编码。然而在实际应用中，还要考虑到感知图像哈希的鲁棒性、安全性等基本要求，本文感知图像哈希生成的基本框架如图 1 所示。对经过归一化预处理后的图像进行特征提取可以满足鲁棒性；利用混沌数据的迭代不重复性和初值敏感性的特点[10]，对特征向量进行 Logistic 混沌加密，保证了特征向量的安全性。

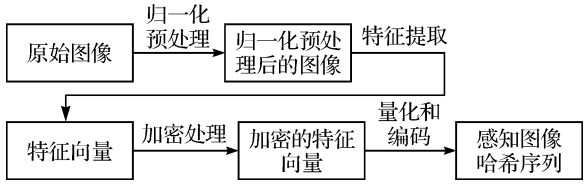

图 1　感知图像哈希生成基本框架

2　感知图像哈希的实现原理

2.1　图像预处理

2.1.1　图像归一化处理

图像的归一化处理的理论基础是矩函数。设 $f(x,y)$ 是图像在笛卡尔坐标系中的实值函数，且

收稿日期：2011－03－09
作者简介：曾　勇(1983－)，男，湖南益阳人，硕士研究生，主要从事图像处理、数字视频方面的研究。

$0 \leqslant x < N_1, 0 \leqslant y < N_2$,则笛卡尔矩 m_{pq} 和中心矩 μ_{pq} 可定义如下:

$$m_{pq} = \sum_{x=0}^{N_1-1} \sum_{y=0}^{N_2-1} x^p y^q f(x,y) \tag{1}$$

$$\mu_{pq} = \sum_{x=0}^{N_1-1} \sum_{y=0}^{N_2-1} (x-\overline{x})^p (y-\overline{y})^q f(x,y) \tag{2}$$

其中,质心坐标 $\overline{x}, \overline{y}$ 可定义如下

$$\overline{x} = \frac{m_{10}}{m_{00}}, \overline{y} = \frac{m_{01}}{m_{00}} \tag{3}$$

Ping Dong 等[11] 利用上述矩函数将图像归一化的过程总结为 4 步,构造了 4 个相乘矩阵,图像归一化的矩阵表达式如下:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_c \\ y_c \end{pmatrix} = \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_c \\ y_c \end{pmatrix} \tag{4}$$

从右至左可依次称为中心化、X-shearing 归一化、缩放归一化和旋转归一化。其中,(x_n, y_n) 是图像归一化后的坐标,(x_c, y_c) 是中心化后的坐标,β 表示 X-shearing 归一化参数,$\beta \in R$;α, δ 表示缩放归一化参数,$\alpha, \delta \in R$;ϕ 表示旋转归一化参数,$\phi \in (0, 2\pi)$。

2.1.2　改进后的归一化方法及实验结果

杨文学等[12] 对 Ping Dong 等的归一化方法进行了改进,从而达到了较好的效果,并设计了翻转归一化,但要通过判断 μ_{01} 和 μ_{10} 的正负来确定翻转方向。笔者直接做一个类似于 X-shearing 归一化的 Y-shearing 归一化操作,从而确定归一化图像的位置。因为本文归一化的过程中将会增加 Y-shearing 归一化操作,用它来满足归一化图像的方向不变性,因此图像归一化过程分为 5 步,构造了 5 个变换矩阵,矩阵表达式如下:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \rho & 1 \end{pmatrix} \begin{pmatrix} x_c \\ y_c \end{pmatrix} \tag{5}$$

从右至左可依次称为中心化、Y-shearing 归一化、X-shearing 归一化、缩放归一化和旋转归一化。根据矩阵变换性质,相乘矩阵的位置不可变换。采用 X-shearing 归一化和 Y-shearing 归一化就可以保证标准归一化图像的方向是一定的,而无需判断与方向有关的参数 μ_{01} 和 μ_{10},减小了计算复杂度。实验采用灰度图像 lena,然后按照改进的图像归一化方法进行实验。图 2((a) ~ (f)) 是将原始图像缩放和旋转处理后进行归一化处理后的图像,为保证攻击顺序的随机性,其中图 2(a) ~ 图 2(c) 是先旋转后缩放(选取参数分别为:15°,0.2 倍;30°,0.5 倍;45°,1.5 倍),图 2(d) ~ 图 2(f) 是先缩放后旋转(选取参数分别为:2 倍,90°;2.5 倍,135°;3.5 倍,180°)。

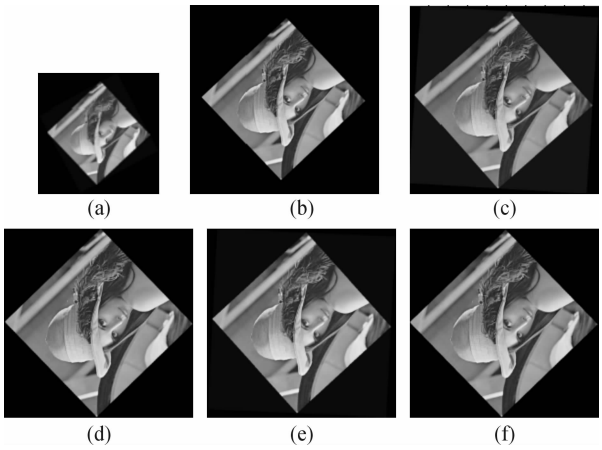

图 2　缩放和旋转归一化图像

2.13　改进的图像归一化结果分析

由图 2 可知,归一化后图像会随着原始图像尺寸和角度的变化而改变,对原始图像进行不同角度的旋转和不同比例的缩放后,经过归一化变换后会产生不同尺寸的归一化图像。但是图像内容和位置却是相同的,因此只需将这部分提取出来处理。笔者利用牛盼盼等[13] 提出的重要区域思想,提取图像的重要区域。图 3(a) 和图 3(b) 是提取的重要区域,图 3(c) 是将图 3(a) 和图 3(b) 统一为同一分辨率后的图像。经过预处理阶段,实际上已经解决了几何攻击的问题。

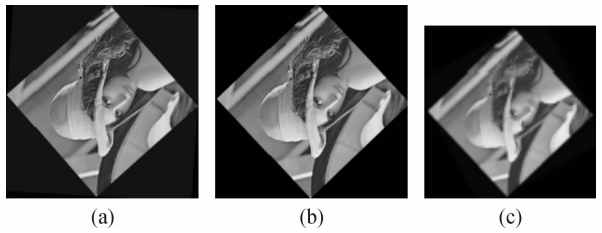

图 3　分辨率的统一

2.2　特征提取

特征提取是哈希序列生成的关键,本文将采用传统的图像哈希生成方法进行处理,具体步骤如下[9-10]:

a) 将归一化处理后的图像进行双线性插值,分辨率统一变为 32×32。

b) 将第一步中的图像分成 16 个 8×8 的小块,对每个小块分别进行 DCT 变换,将每个小块相同位置的 4 个低频系数分别组成长度为 16 的一维向量 A_i,并计算这四组向量的期望 m_i 和方差 δ_i,并对 A_i

进行标准化得到 $F_i=(A_i-m_i)/\delta_i$，再将 F_i 串成长度为 64 的一维向量 F。

2.3 加 密

利用 Logistic 方程作为混沌序列发生器进行加密，每个不同的密钥对应不同的加密矩阵，并用此矩阵对 DCT 系数矩阵进行加密，保证其安全性。Logistic 方程如下：

$$x_{n+1}=\mu x_n(1-x_n)\ 3.5699<\mu<4 \quad (6)$$

2.4 量化编码

对图像进行加密处理后，生成的向量矩阵是浮点类型的。浮点型数据的小数部分对实验结果的影响很小，因此将浮点数据转换为整型数据。这样可以减少冗余，节省存储空间。最后将整型数据转换为二进制形式，形成哈希序列。可以用 4 位、6 位或者 8 位二进制数表示这个整型数据大小，这完全取决于实际需要和存储空间。选定位数后，哈希序列的长度是一定的。

2.5 图像认证

图像认证阶段可以有多种衡量标准[4]，如文献[10]采用两哈希序列的汉明码距离进行匹配认证，文献[9]使用范数来计算两哈希间的距离进行匹配认证等。本文采用两哈希序列间误码个数作为衡量标准[14]。设两哈希的不同位的个数为 D，阈值为 T，若 $D\leqslant T$，则匹配成功，若 $D>T$，则匹配失败。

3 实验结果及分析

3.1 唯一性实验

感知图像哈希的唯一性，取决于人类感知阈值[7]。两张相似的图像，会产生不同的二值感知哈希序列，但是如果这种差别小于等于人类感知阈值，那么将两张图片视为相同内容的图像。如果这种差别大于人类感知阈值，那么将两张图像视为不同内容的图像。本实验取 100 张分辨率为 512×512 的灰度图像进行测试，先将经过旋转或缩放的图片进行归一化处理，然后提取特征点并加密量化，得到 100 组哈希序列，并对 100 组序列两两匹配。利用组合公式 $C_m^n=\dfrac{m!}{n!(m-n)!}$，(其中 $m=100,n=2$)，可得到 4 950 个匹配结果，图 4 为匹配值的统计直方图。

由图 4 可以看出，结果近似于高斯分布，经过拟合，可得 $\mu=121.22,\sigma=17.37$。门限的选取根据匹配值统计直方图和实际需求确定，以图 4 为例，误码个数小于 50 的哈希序列匹配对是不存在的，也就是说误码个数小于 50 的两个哈希序列不存在，即图像产生了唯一的哈希序列。门限 T 的值按如下方法确定：令 $0<T\leqslant 50,T\in Z$，取 $\mu=121.22,\sigma=17.37$，如图 5 所示。门限 T 的选取主要考虑冲突的数量级，取临界点 $T=30$。因此图像的冲突率为：

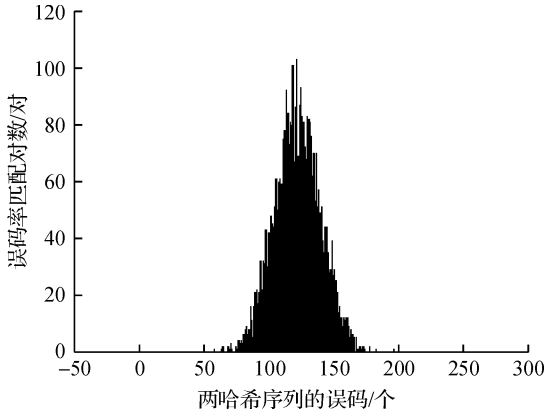

图 4 匹配值统计直方图

$$P=\int_{-\infty}^{T}\frac{1}{\sqrt{2\pi}\sigma}e^{\frac{-(x-\mu)^2}{2\sigma^2}}\mathrm{d}x=7.623\ 5\times10^{-8} \quad (7)$$

可以看到冲突率是 10^{-8} 数量级的，也就是说接收 10^8 幅不同的图像时，只有两幅图像会产生相同的哈希序列，所以可以保证感知图像哈希的唯一性。

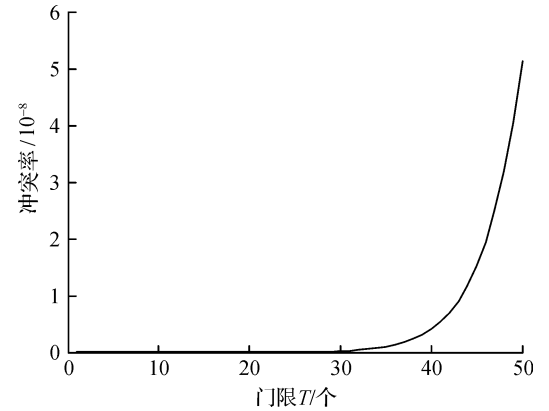

图 5 图像冲突率曲线

3.2 安全性实验

随机选择密钥验证感知图像哈希的安全性。安全性是指如果用不同的密码对归一化图像加密后，应该产生不同的哈希序列，即图像用不同的密钥加密后生成的哈希序列要满足唯一性，所以要求两哈希序列的误码个数要大于门限 T。本文取 key=0.323 2和 0.323 3 对选取的 100 张归一化图像进行加密，可以得到 4 950 个匹配的结果。key=0.323 2 和 key=0.323 3 时的哈希序列匹配结果统计直方图为图 6 和图 7。由图可知匹配结果均大于门限 $T=30$。取 lena 的归一化图像，在 key=0.323 2 和 0.323 3下匹配，可知两序列的误码个数为 141，远远大于门限 $T=30$。所以本算法满足图像的安全性

要求,而且在不知道密钥的情况下,得不出正确的感知图像哈希序列。

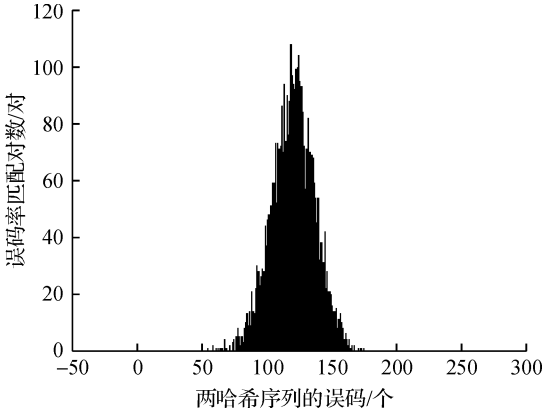

图 6　key=0.323 2 时的匹配值统计直方图

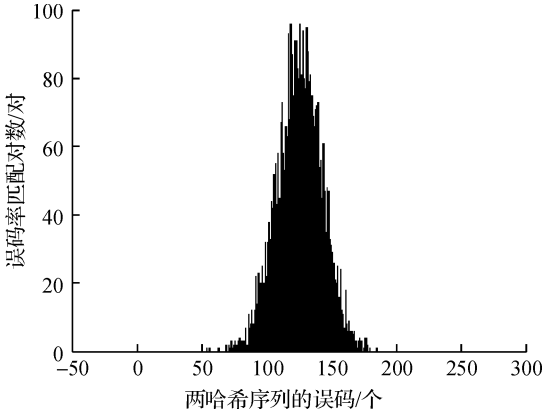

图 7　key=0.323 3 时的匹配值统计直方图

3.3　感知图像哈希的序列长度

感知图像哈希序列的长度可以根据实际的情况进行选取,本文选取了 64 个 Logistic 的随机值,每个数据用六位二进制编码,因此哈希序列长度为 384bit,存储量是非常小的。可以对过长的哈希序列进行压缩,如文献[9]中的 huffman 编码,可以将长度压缩为原来的 1/3 左右。

4　结　语

提出一种基于预处理的感知图像哈希生成方法,采用图像的归一化处理,使处理后的图像具有极强的鲁棒性,可以抵抗缩放、旋转、缩放旋转组合的几何攻击,大大减弱了旋转和几何攻击对图像的影响。实验结果说明,预处理过程提高了特征提取的效果,本文的算法具有唯一性、安全性、鲁棒性。图像归一化产生的冗余,对特征提取有一定的影响,虽然经过重要区域的提取后这种影响有所减弱,但是还存在。如何解决冗余对图像的影响将还需做进一步的研究。

参考文献:

[1] Han Shuihua, Chu Chao-hsien, Yang Shuangyuan. Content-based image authentication: current status issues, and challenges[C]. ICSC 2007 International Conference on Semantic Computing, 2007: 630-636.

[2] Wu Di, Zhou Xue-bing, Niu Xia-mu. A novel image hash algorithm resistant to print-scan[J]. Signal Processing, 2009, 12: 2415-2424.

[3] Menezes A, Oorschot P, Vanstone S. Handbook of Applied Cryptography [M]. Boca Raton: CRC Press, 1997.

[4] Martin Schmucker, Hui Zhang. Benchmarking Metrics and Concepts for Perceptual Hashing[R]. Leuven, Belgium: European Network of Excellence in Cryptology, 2006.

[5] Wang Shuozhong, Zhang Xinpeng. Recent development of perceptual image hashing[J]. Journal of Shanghai University: English-Edition, 2007, 11(4): 323-331.

[6] Lu Chunshien, Hsu Chaoyong. Geometric distortion-resilient image hashing scheme and its applications on copy detection and authentication[J]. Multimedia Systems, 2005, 11(2): 159-173.

[7]牛夏牧, 焦玉华. 感知哈希综述[J]. 电子学报, 2008, 36(7): 1405-1411.

[8] Monga V, Mihcak M K. Robust image hashing vianon-Negative matrix factorizations[C]//Acoustics, Speech and Signal Precessing. Toulouse: ICASSP, 2006: 225-228.

[9] 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, 9(37): 189-192.

[10] 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.

[11] Ping Dong, Galatsanos N P. Affine transformation resistant watermarking based on image normalization [C]//Image Processing, 2002 Proceeding. New York: ICIP, June 2002: 489-492.

[12] 杨文学, 赵　耀. 抵抗仿射变换攻击的多比特图像水印[J]. 信号处理, 2004, 20(3): 245-250.

[13] 牛盼盼, 杨红颖, 邬　俊, 等. 基于归一化图像重要区域的数字水印方法[J]. 中国图像图形学报, 2007, 12(10): 1774-1777.

[14] 邹建成, 周红丽, 邓欢军. 一种安全鲁棒的图像哈希算法[J]. 计算机应用研究, 2009, 26(6): 2122-2125.

Image Perceptual Hashing Based on Image Normalization and DCT

ZENG Yong, *SUN Shu-sen*, *XIA Ai-jun*
(School of Informatics, Zhejiang Sci-Tech University, Hangzhou 310018, China)

Abstract: This paper presents an improved image preprocessing algorithm, and on this basis, an image perception hash algorithm is proposed. The original image is first normalized and a geometric invariant image achieved, and then discrete cosine transform coefficients are extracted as image feature and encrypted using chaotic sequence generator, and finally generated by quantization and coding are applied to produce perceptual hash sequence. The algorithm can resist against attacks of any angle rotation and affine transformation.

Key words: image perceptual hash; preprocessing; image normalization; discrete cosine transform; chaotic encryption; affine transformation

(责任编辑: 陈和榜)

(上接第73页)

Research on Ammonium Chloride Deposition Rules Based on Flow Analysis in Hydrogenation Air Cooling System

OU Guo-fu, *XIE Hao-ping*, *ZHAN Jian-liang*, *JIN Hao-zhe*, *CAO Jing*
(The Lab of Multi-Phase Deposition and Erosion, Zhejiang Sci-Tech University, Hangzhou 310018, China)

Abstract: Aimed at the typical frequent failure cases of hydrogenation high-pressure air cooling system caused by the process of chlorine raw material oil through the process modeling and CFD software, the flow field numerical simulation for bundle of first row in reactor effluent air coolers is carried out. The vapor phase rate, multi-phase velocity and the distribution of shear stress on wall is obtained. so it is proposed that the under-deposit corrosion which caused by ammonium chloride is the main reason of the bundle top failure of reactor effluent air coolers first row. The correctness of the model and conclusions are verified by the comparison between the simulation results and the failure cases. The research conclusion provides the basis for failure analysis and optimization design in hydrogenation air coolers' bundle and complex piping system.

Key words: ammonium chloride deposition; numerical simulation; under-deposit corrosion; optimization design

(责任编辑: 杨元兆)