数字水印技术综述

吴海涛，詹永照

（江苏大学 计算机科学与通信工程学院，江苏 镇江 212013）

摘 要：介绍了数字水印技术的基本框架、主要攻击方法以及评价标准，分析比较了数字水印算法中常用的经典算法，包括空域算法、时域算法等，给出了国内文献提及较少的优化类数字水印算法和近些年提出的 NSCT 分解，并介绍了数字水印技术常见的应用领域。

关键词：数字水印；多媒体数字产品；版权保护

DOI：10.11907/rjdk.151500

中图分类号：TP301 **文献标识码**：A **文章编号**：1672-7800(2015)008-0045-04

1 数字水印技术概述

1.1 数字水印技术定义

数字水印(Digital Watermarking)技术[1]，可以理解为在用户提供的原始数据中，如视频、音频、图像、文本、三维数字产品等载体上，通过数字水印技术手段，嵌入具有某些具有确定性和保密性的相关信息，称之为水印(通常由用户提供，如表示版权信息的特殊标志、logo、用户提供的具有某些意义的序列号、文字或者是产品的其它相关信息等)。除某些特殊要求外，水印信息一般要求是不可见的，并有相应的标准来评判其不可见性或透明性。数字水印技术发展至今，已经逐渐由传统的理论研究阶段发展到实际应用阶段，且为了增加其安全性，常与密码学相结合。

1.2 数字水印系统基本框架

一个完整的数字水印系统一般包含两个模块，即水印嵌入和水印提取与检测[2]。在实际应用过程中，为了进一步保护用户隐私，在嵌入水印之前，需要对原始水印进行加密或置乱处理，这种处理方式通常都是有效的、不可逆的。因此，需要用户提供一个有效的密钥来完成这一过程，称之为水印编码或者加密，在水印提取过程中，同样需要所有者提供该密钥以便完成水印的提取过程，称为解码[3-4]。一个完整的数字水印系统可以用图 1 表示。其中，水印提取过程中，并不一定需要借助原始数据。

原始水印可以有多种形式：随机序列、字符、二维图像等。在做最终的水印嵌入之前都需要进行某种转换以进一步加强水印安全，在实际应用过程中一般采用加密方式。可用式(1)来表达水印嵌入过程：

$$Iw = A(I, E(W, K)) \tag{1}$$

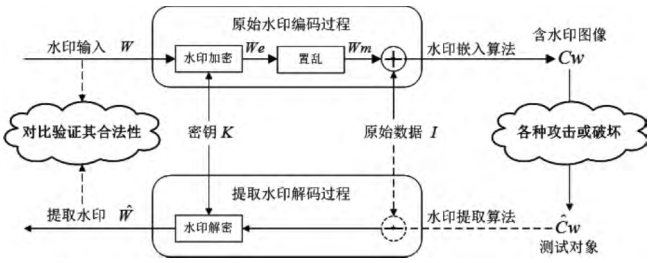

图 1 数字水印系统基本框架

其中，Iw 表示嵌入水印后的图像信息；I、W、K 分别表示原始图像、原始水印以及密钥；E 表示水印加密算法，A 表示水印嵌入算法。可用式(2)表示水印提取过程：

$$\hat{W} = D(K, \hat{A}(Iw, I \mid Iw, W \mid I)) \tag{2}$$

其中，$\hat{W}$ 表示提取后的水印信息；$\hat{A}$ 表示水印提取算法，在提取算法中可能会使用到原始数据或者原始水印信息；D 表示解密算法。

1.3 数字水印攻击方法

按照攻击方法原理及目的不同，可将攻击方法分为以下几类：

1.3.1 消除性攻击

消除性攻击一般是以去除原始水印为目的。在经过这类攻击方法之后，很难从二维数据中重新获得水印信息。

(1)有损压缩及降噪攻击。这类攻击的使用较为广泛，常见的图像处理如图像压缩、降噪等均属于此类。所谓的降噪可以将其理解为图像的二次滤波，由一些人为设

基金项目：高等学校博士学科点专项科研基金项目(201132271100211)；江苏省研究生科研创新计划项目(CX10B_273Z)

作者简介：吴海涛(1988－)，男，河南固始人，江苏大学计算机科学与通信工程学院硕士研究生，研究方向为多媒体数字水印技术；詹永照(1962－)，男，博士，江苏镇江人，江苏大学计算机科学与通信工程学院教授、博士生导师，研究方向为多媒体语义分析。

定的准则来去除掉某些无用信息；压缩则更为常见，如JPEG、MPEG 标准等。

(2)解调攻击。解调攻击常见于各类滤波式攻击方法中，如低通滤波、高斯滤波、中值滤波等。1998 年，Langelaar G. C. 等[5]第一次系统证明了解调攻击的方法与危害，现在的数字水印算法已经具备低通特性。

(3)平均联合攻击。联合攻击针对大量含有水印的数字产品，每次使用不同的密钥或水印进行检测，最后以平均化的方法评估攻击对象。如在不同的含有水印的数字产品中分别提取部分信息，或多次进行平均化统计，则最终会得到一个几乎完全不含任何水印的载体数据[6]。

1.3.2 几何攻击

相比于消除性攻击，几何攻击并不直接消除载体数据中的水印信息，而是试图通过破坏水印和原始数据之间的同步性，使得水印的相关性检测或恢复变得不可能。载体数据中的水印信息虽然依然存在，但是相对位置早已错位。常见的攻击方法，如旋转、缩放、平移、剪切、图像重构、仿射变换等都属于此类。从数字水印技术的提出发展至今，人们对抗几何攻击依然缺少简单有效的手段。造成几何攻击处理难度大的另一个原因则是不清楚攻击者究竟使用了几种攻击手段。现有的成熟水印嵌入算法可能对一种或者数种几何攻击具有较好表现，但面临多种攻击方式的组合时，则有可能表现得不尽如人意。

1.3.3 混淆攻击或 IBM 攻击

混淆攻击最初由 IBM 提出，所以又被称为 IBM 攻击。混淆攻击的目的是试图通过伪造的水印信息或伪造的原始数据来达到侵害原始版权的目的。其基本原理为：设原始图像为 I，加入水印 W 之后的图像记为 $I_A = I + W$；攻击者会首先生成自己的水印 W'，随后创造一个伪造的原图 $I' = I_A - W'$；此后，攻击者即可声称其拥有 I_A 的所有权。这种攻击方式引起了研究者极大兴趣，由于在混淆攻击中同时存在着真实数据、真实水印、真实含水印数据、伪造数据、伪造水印、伪造含水印数据，因此要正确判断数字产品的所有权，则需要在一个数据载体的几个水印中决策出正确的水印信息。

除上述几大类常见的攻击方法外，还有专门针对水印加密过程的攻击方法，以及针对水印实际应用过程中的各种协议作出的攻击等攻击手段。

1.4 数字水印技术评判标准

可从如下方面评判数字水印技术[7-8]：

(1)不可见性/透明性。透明性是现代数字水印技术的一个最基本要求，在没有特殊要求的情况下，数字水印算法不可以影响载体数据的有效性，至少是人眼不可见的。对于透明性更高的要求，则是嵌入水印信息之后的载体和原始数据的某些特性一致，其数据分布是不可感知的，以至于非法拦截者也无法判断其中是否有水印信息存在。现代水印技术中常用峰值信噪比(Peak Signal to Noise Ratio，PSNR)来评估数字水印的透明性。PSNR 的计算公式如下：

$$PSNR = 10 \cdot \lg(\frac{MAX_I^2}{MSE}) = 20 \cdot \lg(\frac{MAX_I}{\sqrt{MSE}}) \quad (3)$$

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} || I(i,j) - I'(i,j) ||^2 \quad (4)$$

其中，MAX_I 指图像的灰度级，通常为 255；MSE 为原始图像与检测图像之间的均方差(Mean Square Error，MSE)；I 表示原始图像；I' 为嵌入水印之后的图像。可以看出，PSNR 值基本上由 MSE 的值确定，且 PSNR 值越大，表示图像的透明性越高。

(2)鲁棒性。鲁棒性是现代水印技术对数字水印算法提出的另一个基本要求，即水印不能因为对载体数据进行简单的改动或者标准化的图像处理而轻易受到损坏。数据在传输过程中不可避免地会受到各种信号的干扰，如噪声、滤波操作、重采样、有损编码压缩、裁剪、缩放、旋转等，数字水印被设计成不会由于这些常见的干扰而造成水印失真。对鲁棒性更高的要求则是在面对各种恶意攻击时，依然能够尽量满足提取检测的条件。在现代水印技术中，鲁棒性一般由归一化互相关系数(Normalized Correlation，NC)来确定。NC 值的计算公式如下：

$$NC(X,\hat{X}) = \frac{\sum_i\sum_j X(i,j)\hat{X}(i,j)}{\sqrt{\sum_i\sum_j X(i,j)^2}\sqrt{\sum_i\sum_j \hat{X}(i,j)^2}} \quad (5)$$

其中，X 和 $\hat{X}$ 分别表示原始水印和提取水印信息；NC 值是一个小于 1 的小数，通常其值越大则表示提取出的水印效果越好。

(3)容量。容量被定义为能够嵌入到原始数据中的有效水印的数量。水印容量通常是平衡透明性和鲁棒性之间的关键因素。一个可以嵌入更大容量水印的算法其透明性和鲁棒性可能会较差，因而需要在保证鲁棒性和透明性的同时，尽可能加大水印的嵌入量。

(4)安全性。现有数字水印技术中，一个不安全的数字水印算法不可以被用于版权保护、数据认证、非法数据跟踪等任务中。与鲁棒性相比，安全性更关注于数字水印的密钥。如果一个恶意攻击者使用了相同的数字水印嵌入算法，在水印信息没有任何保护的情况下，则极有可能提取出水印，随后由于伪造而造成的损失将是巨大的。此外，使用某些更为复杂、高效的数字水印嵌入算法，在一定程度上也可以增加数字水印的安全性。

(5)误检率。误检率在被提出之前，可能大部分数字水印工作者并未意识到有这种问题的存在。水印误检是指使用正确的水印提取算法执行水印的提取过程时，有可能从并没有数字水印的伪载体中提取出一个水印信息；或者从正确的载体数据中提取不到正确的水印信息。虽然这些情况发生的概率较小，但确实存在这种可能。

2 常见数字水印算法分析比较

近年来，数字水印技术的发展取得了很大进步，各种

新的理论或算法随着研究人员的不同，其设计框架与思路也在不停转换。一些较为典型的数字水印算法主要有如下几种。

2.1　空间域算法

空域算法一般是通过直接修改原始图像的像素值来达到嵌入水印的目的。这种算法一般操作简单，具有一定的鲁棒性，但透明性较差。空域算法中最为典型的是 L. F. Turner[9] 与 R. G. van Schyndel[10] 等于 1994 年设计的最低有效位算法（LSB）。Schyndel 等首次科学地阐明了数字水印的重要概念和鲁棒水印检测的通用方法，其原理是通过修改原始数据中的最低有效位来实现水印的嵌入。一幅普通的灰度图像在计算机中存储，其像素值介于 0～255 之间，随意增减一个像素值而不会引起人眼视觉系统的感知。算法可以表示为：设待嵌入的水印为一个长度为 L 的 M－序列，$M=\{m(k),1\leqslant k\leqslant L\}$，则即可通过式(6)嵌入水印信息：

$$I'(i,j)=I(i,j)-\mathrm{mod}(I(i,j),2)+m(k) \qquad (6)$$

其中，$I'(i,j)$ 表示对原始图像每个像素点 $I(i,j)$ 修改之后的值。这种水印嵌入方式有一定的鲁棒性，且在不考虑图像失真的情况下，可以嵌入的水印容量即为原始图像的大小。但由于是直接替换了图像的像素最低位，因而很容易去除，且对各种图像处理攻击鲁棒性较差。

2.2　变换域算法

和空域算法不同，变换域算法一般通过修改图像的其它附加属性（如颜色、纹理、频域）来嵌入水印，这种方法可以使图像具有较高鲁棒性的同时，保证含有水印的图像具有较好的透明性。

1995 年，Cox 等[11-12] 最先将数字水印嵌入在原始图像的 DCT（Discrete Cosine Transform）域中，并由此开创了变换域水印的先河，该算法在数字水印技术中占有十分重要的地位。其基本思想是：首先采用 DCT 变换将原始图像 I 转换为频域表示，随后从 I 的 DCT 系数中选择 n 个最重要的频率分量，使之组成序列：$S=s_1,s_2,\cdots,s_n$，以提高对 JPEG 压缩攻击的鲁棒性；然后以密钥 K 为种子产生伪随机序列，即原始水印序列：$W=w_1,w_2,\cdots,w_n$，其中 $w_i(i\in[1,n])$ 是一个满足高斯分布 $N(0,1)$ 的随机数；再将水印序列 W 叠加到序列 S 中，产生含水印的序列 $S'=s'_1,s'_2,\cdots,s'_n$，使用 S' 替换掉原始图像中的 DCT 系数序列 S，再通过逆 DCT 变换（IDCT）得到含有水印的图像。同时，水印的检测依赖于一个手动控制的阈值 σ，当相关性检测结果大于 σ 时，则认为含有水印，否则认为没有。该算法的思想较为简单具有一定的鲁棒性，后来，通过其他学者的研究改进，陆续出现了其它变换域算法，包括离散傅里叶变换（Discrete Fourier Transform，DFT）、离散小波变换（Discrete Wavelet Transform，DWT）等。

Ruanaida 等[13] 最先在 1999 年提出将数字水印嵌入在原始图像的 DFT 域中。该算法和其它开创性算法类似，通过简单修改原始水印的相位值来嵌入水印：$F(k_1,k_2)=F(N_1-k_1,N_2-k_2)$，其中 F 是离散傅里叶变换，N_1、N_2 用于控制水印的嵌入量。该算法从对图像的理解和通信理论角度指出相位调制更适合鲁棒性水印。

Kunder 等[14] 最早尝试将水印嵌入到图像的 DWT 域中。其依据是图像经过小波分解后，原始图像将会被分为若干子带，这非常类似于人眼视觉系统在浏览图片时将图片分解为若干个部分。因此，图片的空－频转换特性能够很好匹配视觉系统。随着 MPEG-4 及 JPEG-2000 图像压缩标准的公布，受其核心技术小波变换的影响，利用 DWT 分解嵌入数字水印的算法也越来越多。Kunder 等最初的做法是分别对原始图像及水印进行小波分解，并在不同分辨率水平之下将水印小波系数叠加到图像小波系数中，并在此之前，对水印的小波系数使用一种人类视觉模型约束进行调制。

2005 年以后，A. L. Cunha 等在图像处理方面提出了一个新算法，称之为非下采样 Contourlet 变换（nonsubsampled contourlet transform，NSCT）。NSCT 算法具有平移不变形及旋转不变性，其对于简单的几何攻击，如旋转、平移、缩放等攻击有较强的鲁棒性，因此很快被用于图像数字水印领域，并取得了相应进展。但 NSCT 分解的算法计算量远远大于其它变换域数字水印算法，很难做到数字水印嵌入时的同步性，目前也尚处于理论研究阶段。

2.3　优化类水印算法

20 世纪 90 年代开始，人工智能及生物模拟算法为新的研究热点，并诞生了许多优秀算法，如模拟蚂蚁群落采集食物过程的蚁群算法（ant colony optimization）、模拟鸟类运动的粒子群优化算法（particle swarm optimization）、模拟生物遗传的进化算法（EA）、神经网络等[15-18]。这类算法的提出也为数字水印算法带来了新的生命力。虽然不能直接由这些算法嵌入水印，但在嵌入水印之后可利用此类算法优化含水印的图像，以达到鲁棒性和透明性之间更好的平衡。

（1）粒子群优化算法。粒子群优化算法由 Ebehart 和 Kennedy 等于 1995 年提出，它以无质量无体积的粒子作为个体，并为每个个体定义简单的运动规则，从而使整个粒子群呈现出复杂的特性，求解过程类似于在三维空间中求最短路径，可用于求解复杂的优化问题，在图像分割、图像识别、图像压缩、图像融合领域均有其独特应用。K. Kuppusamy 和 K. Thamodaran 提出一个基于 PSO 算法的主要用于版权保护的优化水印方案。该方案使用常规的水印嵌入算法，如针对 DCT 域作水印嵌入时，使用 PSO 算法快速选择子带中的高能量子带来嵌入水印。同时使用图像质量指数指标（IQIM）来评估图像失真。

（2）差分进化算法。同 PSO 算法类似，差分算法也是进化算法簇中的一员。第一个简单、快速、具有鲁棒性的 DE 算法由 Storn 和 Price 于 1995 年提出，随后，针对 DE 算法中缩放因子和交叉因子的选择，不同的改进算法先后被提出并用于数字水印领域。在国内，使用 DE 算法优化数字水印的文献并不常见。Musrrat Ali 等提出了一种基

于 DE 算法的数字水印优化算法。在水印嵌入过程中，依然使用传统算法，将水印嵌入在原始图像的 DWT-SVD 域中，再对含有水印的图像使用多种不同的攻击方式进行攻击测试，最后使用差分进化算法对水印嵌入强度加以优化，以寻求一个面对不同攻击时都有不俗表现的算法。

2.4 其它水印算法

(1)奇异值分解(Singular Value Decomposition，SVD)。奇异值分解是线性代数中的一种重要矩阵分解，是矩阵分析中正规矩阵酉对角化的推广。在信号处理、统计学等领域有重要应用。由于图像在计算机存储时的特殊性，因而完全可以使用线性代数中矩阵分解的方法来应对图像处理中的问题。单纯使用 SVD 分解的方法来嵌入数字水印的文献较少，经典的做法是配合 DWT 分解和 DCT 分解，这类叠加算法通常对大部分攻击都有较好的鲁棒性。

(2)分形水印。分形(Fractal)是 Mandelbrot 在 1977 年提出的几何学概念，图像分形压缩的基本原理是利用分形几何中的自相似性来进行图像压缩。Puate 和 Jordan[19]在 1997 年首先提出基于图像分形压缩原理的水印算法。该算法将原始图像随机分为若干个大小为 $n\times n$ 的块，记为 RB，并利用分形压缩技术和块周围的搜索区域(LSR，Local Searching Region)建立一定的对应关系，称之为编码。原始水印为一串二值序列，记为 $V=v_1,v_2,\cdots,v_n$。水印的嵌入过程表示为：$v_i(i\in[1,n])$ 为 1 时，利用 RB 和其周围大小为 $3n\times 3n$ 的 LSR 的关系对 RB 进行编码；反之，则利用 RB 和周围大小为 $2n\times 2n$ 的 LSR 的关系对 RB 进行编码。实验表明，该算法对 JPEG 压缩攻击有较好的鲁棒性，当压缩质量为 50% 时，水印依然可以较好地被提取出来。但该算法计算量较大、速度慢。

(3)扩频水印。Tirkel 等首先注意到扩展频谱技术可以用于数字水印的嵌入，随后出现了一系列的基于扩频技术的数字水印算法。由于在图像的高频区域嵌入水印，则算法的透明性较高，但鲁棒性较差；相应地，在图像的低频区嵌入水印，则图像的鲁棒性良好，但不易控制透明性。扩展频谱技术可以将一个能量信号(原始水印信息)嵌入到每个频带，从而缓解这些矛盾。

2.5 数字水印典型应用

目前，数字水印技术主要应用于如下几个领域：

(1)基于数字水印技术的版权保护。数字水印技术用于版权保护几乎已达成共识，许多数字水印算法在设计之初是以版权保护为目的。目前，许多图像处理公司通过和各种可信的第三方机构合作，开始将数字水印技术用于商业化目的，如 Digimarc 公司的 ImageBridge 解决方案。该方案提供一个被称之为 ImageBridge 的水印检测器，该检测器可以识别包括 Adobe Photoshop 和 Corel PhotoPaint 在内的多种图片格式。当用户使用该检测器时，它可以识别出水印信息，并从远程数据库中调取水印密钥以确定作者身份。

(2)基于数字水印技术的指纹识别。该领域也是近年来数字水印技术中的热门研究方向。在面临各种需要个人唯一身份凭证的商业行为时，不可避免地会发生各种信息泄露状况，对个人隐私造成极大威胁。指纹识别的兴起正好可以解决这一问题。目前，指纹识别所面临的主要问题是水印信息的来源，由于不能从公共数据库中获取大量的指纹信息，因此，目前大多数数字水印指纹识别还局限于在某个实验室或者科研机构中进行。

(3)拷贝控制。严格来说，拷贝控制也算是版权保护领域中的一个应用。其主要目的是使用脆弱水印防止他人误用、盗用未经授权的数字信息。拷贝控制应用颇为广泛，尤其是在电子音乐、视频等领域。

3 结语

随着互联网的发展，多媒体数字产品面临的攻击方式也逐渐呈现出多样性与不确定性，这为数字水印技术带来了新的挑战。几何攻击依然是现代数字水印领域的难点之一，它尚无简单有效的解决方案。人工智能算法的引进，给数字水印算法带来了新的活力。目前，数字水印技术已经应用到实际生活中，但总体看来，其受众依然较少，尚需进一步研究和推广。

参考文献：

[1] VAN SCHYNDEL R G，TIRKEL A Z，OSBRNE C F. A digital watermark[C]. IEEE International Conference on Image Processing，1994：86-90.

[2] 向辉. 基于信息重组思想的多媒体数据压缩与多媒体数据安全技术研究[D]. 杭州：浙江大学，1999.

[3] L F TRUNER. Digital data security system[S]. Patent IPN WO 89/08915，1989.

[4] BENDER W，GRUHL D，MORIMOTO N，et al. Techniques for data hiding[J]. IBM Syst J，1996，35(3)：313-336.

[5] GC LANGELAAR，RL LAGENDIJK，J BIEMOND. Real-time labeling of MPEG-2 compressed video[J]. Journal of Visual Communication & Image Representation，1998，9(4)：256-270.

[6] KUTTER M，WINKLER S. A vision-based masking model for spread spectrum image watermarking[J]. IEEE Trans. On Image Processing，2002，11(1)：16-25.

[7] FABIENA P PETITEOLAS，ROSS J，ERSON，et al. Information hiding——a survey[J]. Special Issue on Protection of Multimedia Content，1999，87(7)：1062-1078.

[8] M KUTTER，F A RPETITCOLAS. A fair bench mark for image watermarking systems[J]. Electronic imaging'99 Security and Watermarking of Multimedia Contents，1999，3657(5)：226-239.

[9] TURNER L F. Digital data security system[S]. Patent IPN WO89/08915，1989.

[10] VAN SCHYDEL R G，TIRKEL A Z，OSBORNE C F. A digital watermark[C]. IEEE International Conference on Image Processing，1994(2)：86-90.

[11] COX I，KILIAN J. Secure spread spectrum watermarking for images，audio and video[C]. in Proceedings of IEEE International Conference on Image Processing，1996.

[12] COX I，KILIAN J，LEIGHTON T. Secure spread spectrum watermarking for multimedia [J]. IEEE Transaction on Image Processing，1997.

民用飞机系统功能危险性评估

贺 娜

(上海飞机设计研究院 飞控部,上海 201210)

摘 要:功能危险性评估作为安全性评估的第一步,起着至关重要的作用。介绍了系统功能危险性评估的目标和流程,以自动飞行控制系统为例详述评估过程,可为民用飞机系统功能危险性评估提供参考。

关键词:民用飞机;自动飞行控制系统;功能危险性评估;安全评估

DOI:10.11907/rjdk.151788

中图分类号:TP301 **文献标识码**:A **文章编号**:1672-7800(2015)008-0049-03

0 引言

对于民用飞机而言,安全性是其首要考虑的问题,贯穿于飞机从研制、生产、运营到退役的整个生命周期,同时也是民用飞机能否通过适航审查、进入市场并获得公众信任的前提条件。自动飞行控制系统作为民用飞机机载系统的一个重要部分,安全性是其至关重要的设计因素。

系统安全性分析包括功能危险性评估、系统安全性初步评估、系统安全性评估、共因分析、失效模式影响评估等。本文以 ASE ARP 4761 为指导,以某民用飞机自动飞行控制系统为例,主要对安全性分析的第一步——功能危险性评估过程进行介绍和分析。

1 功能危险性评估概述

功能危险性评估是系统综合检查产品的各种功能,识别功能的各种失效状态,并根据失效状态的严重程度对其进行分类的一种安全性分析方法。以系统为对象,功能危险性评估研究其在飞机设计的整个飞行包线和不同飞行阶段内,可能影响系统乃至飞机整机飞行安全的功能失效[1]。

功能危险性评估过程是一种自上而下识别功能失效状态并评估其影响的方法,它的目标是在系统功能丧失和功能失常等情况下,识别失效状态和其相关分类。

作为民用飞机安全性评估的第一步,功能危险性评估是下一步安全性评估流程的必要输入,也为后续系统、子系统设计架构提出安全性设计需求,帮助确认系统架构的可接受性,发现潜在问题和所需的设计更改,并确定进一步的需求范围。系统功能危险性评估给出各种功能的危险评估,推导或确认系统安全性设计准则,提出系统安全性要求,还提供对安全性至关重要的潜在功能失效状态信息,这些信息可用来确立所需系统的结构方案、软件完整性水平要求、系统分离和隔离要求以及最低设备清单要求[2]。

系统功能危险性评估的输入主要有系统功能清单、外部接口示意图、飞机级功能危险性评估功能清单、飞机级功能危险性评估识别失效状态、设计要求和目标、飞机级设计方案选择及其原理,以及系统使用的适航规章。

[13] RUANAIDH J,DOWLING W,BOLAND F. Phase watermarking of digital image[C]. in Proceedings of IEEE International Conference on Image Processing,1999.

[14] KUDUR D,HATZINAKOS D. A robust digital image watermarking method using wave let-based fusion[J]. in Proceedings of IEEE IC IP97,1997:544-547.

[15] S S RAO. Optimization theory and application[Z]. New Delhi:Wiley Eastern Limited,1984.

[16] A COLORNI,M DORIGO,V MANIEZZO. Distributed optimization by ant colonies[C]. Proceedings of ECAL91-European Conference on Artificial Life,1991:134-142.

[17] J KENNEDY,R C EBERHART. Particle swarm optimization[C]. Proceedings of the IEEE International Conference on Neural Networks,1995:1942-1948.

[18] H P SCHWEFEL. Numerical optimization of computer models [M]. John Wiley &Sons,1981.

[19] JS JORDAN. Individual and group action as the control of image-schema across fractal time-scales:a response to vandervert[J]. New Ideas in Psychology,1997(4):1-6.

(责任编辑:孙 娟)

作者简介:贺娜(1988—),女,陕西延安人,上海飞机设计研究院飞控部工程师,研究方向为自动飞行控制系统设计和安全性分析。