# 电子海图数据安全解决方案研究*

杨益兴
(海军驻武汉701所军事代表室 武汉 430064)

**摘 要** 论文针对电子海图在应用中面临的数据安全问题,提出一套以非对称加密和可逆数字水印技术为核心、综合采用信息隐藏和USB密钥管理等软硬件手段的电子海图数据安全解决方案。该方案可有效克服现有海图安全技术的缺陷,全面实现数字海图的防伪、防篡改和流失途径追踪等功能,为电子海图的发放、管理提供可靠的安全保障。

**关键词** 电子海图; 数字签名; 数字水印
**中图分类号** U675.81 **DOI**:10.3969/j.issn.1672-9730.2016.03.027

# A Scheme of Digital Chart Data Security

YANG Yixing
(Navy Representative Office in 701 Research Institute, Wuhan 430064)

**Abstract** Towards the security issue of digital chart data, a solution is presented based on asymmetric encryption and digital watermarking. Both information hiding techniques and USB encryption equipments are utilized in our scheme. The proposed scheme can avoid the weaknesses of most current security methods and, furthermore, achieve more comprehensive security functions such as anti-fake, anti-tamper, and illegal-copy chasing. Consequently, it can provide a more reliable protection for digital chart data.

**Key Words** digital chart, digital signature, digital watermarking
**Class Number** U675.81

## 1 引言

我国大量船舶上都配备了电子海图系统。多年实践表明,电子海图系统在作业精度、自动化程度等方面具有传统纸质海图不可比拟的优势,现已成为航海人员不可缺少的信息化航海作业工具。但是,海图电子化为航海工作带来巨大便利的同时,也引发了许多不容忽视的问题,特别是电子海图数据的安全问题,成为制约其应用水平的关键因素。众所周知,电子海图数据制作复杂,具有很高的经济价值,而海图电子化后通常以矢量数据格式存储在计算机或移动存储介质中,这些数据很容易遭到非法复制、修改和传播[1]。根据目前主流电子海图设备的发展状况,只要具备初级的计算机知识,就能够很轻易地将海图数据从设备中拷贝出来。由于海图数据中并不包含使用者的任何身份信息,因此即使发生非法拷贝事件,也无从追查流失数据的具体来源。不仅如此,电子海图的安全问题还贯穿于数据发放和使用的全过程。例如:海图出版单位将新版海图发往各使用单位,在各个中间环节都存在数据被替换、篡改的风险,而目前各使用单位还没有有效的手段来检测数据是否真正来自于海图出版社、数据在传输过程中是否经历过有意或无意的改动[2]。基于以上分析,把电子海图的数据安全问题归结为以下三个方面:1)真实性验证(防伪)问题,即海图数据中需包含出版方的身份信息,供使用方确认数据的真实来源;2)完整性验证(防篡改)问题,即海图数据中需包含海图自身的验证信息,供使用方检测数据是否经历过任何改动;3)流失途径追踪问题,即海图数据中需包含使用方的身份信息,以供非法拷贝事件发生后对数据流失渠道的追查。

* 收稿日期:2015年9月7日,修回日期:2015年10月23日
作者简介:杨益兴,男,高级工程师,研究方向:舰船电子武备设计与监造。

事实上，我国海图出版单位早已关注上述问题，并采取了一定的技术手段来提升海图发放和使用管理的安全性。但就目前而言，这些措施仍无法全面解决上述三方面的安全问题。根据调查，目前采取的措施主要有两种：一是利用传统加密技术，将海图数据转换成密文后发送，接收方将数据解密后再安装到电子海图设备中。这种方法可以保护数据在传输环节的安全，但数据一经解密即完全丧失了保护功能。另一种方法是在海图文件中附加一段电子标签，其中记录了数据出版方和使用方的身份信息，用于实现双方的身份验证。但这种方法同样存在明显的缺陷：首先，电子标签是海图文件的附加内容，很容易被人为移除；另外，电子标签改变了海图文件的格式，在安装使用前必须手工移除后电子海图设备才能正确识别和使用。因此海图一旦安装到设备上，海图数据的保护功能即丧失[3]。

由上述分析可见，现有两种技术手段都无法可靠解决海图出版方和使用方的身份确认问题，同时由于数据安全机制与海图内容本身完全脱离，导致无法实现对海图数据的全周期保护，特别是海图安装到设备后的保护。为此，本文借鉴信息安全领域公钥基础设施(PKI)的工作机制，采用基于非对称加密算法的数字签名技术来实现海图数据的真实性和完整性验证，并通过可逆数字水印技术将数字签名嵌入到电子海图数据当中，从而实现安全信息与海图内容的紧密结合，达到对海图进行全周期保护的目的。本文旨在为电子海图的安全发放和管理提供一种可靠的“复合型”数据保护方案，通过融合非对称加密技术、数字签名技术和数字水印技术等多种信息安全技术的优势来有效克服现有单一技术途径的缺陷，为电子海图的发放、传播、接收及使用提供全面的数据安全保障。

## 2　非对称加密与数字签名

非对称加密是指采用成对密钥的加密算法，其密钥由公钥和私钥组成，数据的加密和解密必须由公钥和私钥分别完成：即用公钥加密，则用私钥解密；而用私钥加密，则用公钥解密。采用非对称加密算法的体制称为公钥密码体制。公钥密码体制的思想最早由 Diffie 和 Hellman 在 1976 年提出，迄今为止应用最为成功的是 RSA 公钥密码体制，它是 1978 年美国麻省理工学院的 Rivest、Shemir 和 Adelman 三位科学家提出的，并以这三个科学家的名字命名。其优点是用户甲可以利用公钥加密规则发出一条加密的消息给用户乙，而不需要预先的共享密钥的通信。乙将是唯一能够利用自己的私钥来对密文解密的人。乙可以让任何人发布他的公钥，任何人用公钥将数据加密后在网络中传输，即使在传输过程中被别人截获并拥有乙的公钥，也无法利用这些信息来破译加密数据，而只有乙通过自己的私钥才能顺利解密密文。这样便实现了数据在 RSA 公钥密码体制下的安全传输。

数字签名的本质就是将被保护数据的数字摘要用发送者的私钥进行加密。国际标准化组织(ISO)关于数字签名的定义为“附加在数据单元上的一些数据，或是对数据单元所做的密码变换，这种数据或变换允许数据单元的接受者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人伪造”。采用数字签名可以保证签名者无法根据自己的利益抵赖签署过的信息，而验证者也无法根据自己的利益伪造他人的签名。2005 年 4 月 1 日起正式施行的《中华人民共和国电子签名法》第十四条中明确规定“可靠的电子签名与手写签名或者盖章具有同等的法律效力”，从而在法律上保证了数字签名的合法性和有效性。本文即采用数字签名来实现电子海图的防伪和防篡改功能。为进一步解决海图的泄密途径追踪问题，我们对传统的数字签名进行改进，在其中添加海图使用者的身份 ID，并借助数字水印实现泄密途径追踪功能[4]。

## 3　电子海图可逆数字水印技术

数字水印技术是通过一定的算法将一些标志性信息直接嵌到多媒体内容当中，但不影响原内容的价值和使用，并且不能被人的知觉系统觉察或注意到。与加密技术不同，数字水印技术并不能阻止盗版活动的发生，但它可以判别对象是否受到保护，监视被保护数据的传播、真伪鉴别和非法拷贝、解决版权纠纷并为法庭提供证据。而可逆数字水印是指当水印数据从含水印的载体中提取出来以后，能够完整地恢复原始载体数据。由于电子海图对数据精度有严格的要求，因此可逆水印技术更加适合于海图数据的安全保护。本文即采用可逆数字水印技术来实现数字签名与海图数据的无缝融合，并确保二者的不可分割，从而实现海图数据的全周期保护[5~6]。

## 4　电子海图数据安全解决方案设计

本文力图从两个方面达到预期目标，一是为电子海图提供较为全面的数据保护功能，包括防伪、

防篡改和泄密途径追踪;二是为电子海图应用的各个环节提供全周期数据保护,特别是海图安装到设备后的数据保护[7]。为此,以非对称加密、数字签名和数字水印技术为核心,构建了一套具备上述功能的总体技术方案(如图 1 所示)。

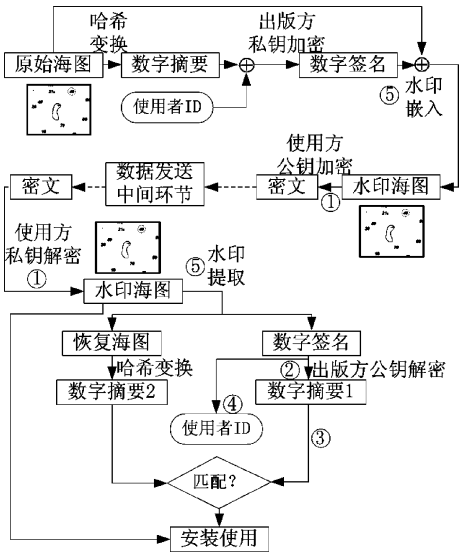


图 1 海图数据安全解决方案

上述技术方案的基本工作流程如下:

1) 在数据发送阶段(图 1 上半部分),海图出版方首先采用哈希变换算法计算出原始海图的数字摘要(该摘要是原始海图数据唯一的数字标识,可用于验证海图数据的完整性),然后将数字摘要与接收单位的身份标识(即使用者 ID)组合后用出版方的私有密钥加密,得到海图的数字签名,接着将数字签名作为水印数据嵌入到原始海图中,得到含水印的海图数据,最后将含水印海图用使用方的公开密钥加密后得到密文,该密文经由各个中间环节传送给海图使用方。采用密文传输可以有效避免数据在各个中间环节的安全隐患,同时由于采用使用者公钥加密,还可以确保只有拥有对应私钥的指定使用者才能够对该数据解密(图中①)[8]。

2) 在数据接收阶段(图 1 下半部分),海图使用者接收到密文海图数据并用自己的私有密钥对数据进行解密,得到含有水印信息的海图数据。为验证数据的真实性和完整性,使用者首先采用水印提取算法将海图中的水印提取出来。由于本方案采用了可逆数字水印算法,使用者可同时获得海图的数字签名和恢复后的原始海图。接下来,使用者采用海图出版方的公开密钥对数字签名解密。如果解密成功,则说明这份海图确实是来自于海图出版方(真实性验证,图中②),同时可得到自己的身份 ID 和海图的数字摘要(数字摘要 1)。另外,对恢复海图进行哈希变换可得到其数字摘要(数字摘要 2)。将两份数字摘要进行比对,如果完全一致,则说明海图数据完全正确,没有经历任何篡改(完整性验证,图中③)。在通过上述验证后,使用者即可将含有水印的海图数据安装到电子海图设备中使用。由于安装的电子海图数据始终含有水印信息,一旦发现非法拷贝数据,即可从隐藏的水印数据中读取使用者的 ID,从而判断数据流失的途径(流失途径追踪,图中④)[9]。

上述技术方案综合利用了非对称加密技术、数字签名技术和数字水印技术的优势,可以完全实现预期的目标。首先,该方案具备对海图数据的全功能保护(防伪、防篡改、泄密途径追踪,图中②、③、④);其次,该方案可以实现对海图数据的全周期保护:在数据传输环节采用非对称加密技术(图中①),在数据使用环节采用数字水印技术(图中⑤)。

## 5 主要算法和密钥管理

本文所述技术方案涉及的主要算法都比较成熟:海图数字摘要的计算可采用 MD5 或 SHA 算法,非对称加密可采用 RSA 体制,而数字水印可采用基于差值扩展的可逆数字水印算法[10]。另外,上述方案还涉及到密钥的管理问题。密钥管理是信息安全领域的关键技术,其核心问题是密钥分配。可考虑设置密钥管理中心来统一生成、分配和管理海图出版方、使用方的密钥。由于双方均需知道自己的私钥和对方的公钥,这些密钥可采用目前广泛应用的 USB 加密设备来存储。

## 6 结语

本文通过对电子海图应用安全需求和现有技术手段缺陷的分析,采用非对称加密、数字签名和数字水印技术,提出了一套完整的海图数据安全解决方案。该方案综合利用多种信息安全技术的优势,能够实现电子海图数据的全周期、全功能安全保护。以该方案为基础,可以进一步构建完整的电子海图数据安全管理体系,借助现代计算机软硬件技术来全面保障电子海图数据在发放、传输和使用管理各个阶段的数据安全。

### 参 考 文 献

[1] 尹浩,林闯,邱峰,等. 数字水印技术综述[J]. 计算机研究与发展,2005,42(7):1093-1099.

[2] IHO Data Protection Scheme. Special Publication S-63 [S]. Edition 1.1-March,2008.

[3] 陈永强,胡汉平,李新天,等. 一种基于 PKI 和数字水印

的电子印章应用方案[J]. 武汉工业学院学报,2005,2:28-32.

[4] XiaoTong Wang, ChengYong Shao, XiaoGang Xu, et al. Reversible Data-Hiding Scheme for 2-D Vector Maps Based on Difference Expansion[J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3):311-320.

[5] 邵承永,王孝通,徐晓刚,等. 矢量地图的无损数据隐藏算法研究[J]. 中国图象图形学报,2007,2:23-28.

[6] 王勋,林海,鲍虎军. 一种鲁棒的矢量地图数字水印算法[J]. 计算机辅助设计与图形学学报,2004,16(10):1377-1381.

[7] 孙建国,门朝光. 基于二维矢量地图属性特征的数字水印算法[J]. 高技术通讯,2009,19(7):713-717.

[8] 赖明珠,孙建国,张国印. 双特征下的二维电子海图水印技术研究[J]. 哈尔滨工程大学学报,2015,36(5):678-681.

[9] 曹刘娟,门朝光,孙建国. 基于空间特征的二维矢量地图可逆水印算法原理[J]. 测绘学报,2010,39(4):422-427.

[10] 郑海,邵承永,钟云海. 数字海图信息安全应用研究[J]. 中国航海,2013,36(1):44-46.

(上接第 27 页)

利用式(10)可得 $U_{11}$ 对各灰色的灰色评价权向量为 $r_{11}=(r_{111},r_{112},r_{113},r_{114})=(0.31,0.31,0.375,0)$,同理可得 $r_{12}$。

于是,$R_1=\begin{bmatrix}0.31 & 0.31 & 0.375 & 0\\ 0.458 & 0.458 & 0.083 & 0\end{bmatrix}$

利用同样的方法计算

$$R_2=\begin{bmatrix}0.375 & 0.375 & 0.25 & 0\\ 0.229 & 0.229 & 0.458 & 0.083\\ 0.167 & 0.167 & 0.333 & 0.333\\ 0.25 & 0.25 & 0.417 & 0.083\\ 0.524 & 0.524 & 0.042 & 0\end{bmatrix}$$

$$R_3=\begin{bmatrix}0.354 & 0.354 & 0.292 & 0\\ 0.489 & 0.468 & 0.043 & 0\\ 0.393 & 0.393 & 0.208 & 0\end{bmatrix}$$

### 4.4　舰载机部队训练水平的灰色综合评价

先对 $U_i$ 作一级综合评判:

$B_1=w_1\times R_1=(0.4568,0.4568,0.1237,0)$

$B_2=w_2\times R_2=(0.4551,0.4551,0.1395,0)$

$B_3=w_3\times R_3=(0.4769,0.3978,0.1937,0)$

则 $U_i$ 对于各类评价灰类的灰色评价矩阵:$R=(B_1,B_2,B_3)$,$U$ 的二级综合评判结果为:$B=w\times R=(0.4687,0.4331,0.1562,0)$

取优、良、中、差对应评分标准中的值作为各评价灰类等级的值化向量,则值化向量:$D=[9\quad 7\quad 5\quad 3]$。根据式(14),计算出航母编队舰载机部队训练水平的评估值:$Z=B\times D^T=7.8863$。

综合评价值和评分标准(表 1)来看,该航母编队舰载机部队训练水平为“良”类,与实际情况相符。

## 5　结语

本文采用灰色层次分析法,建立了舰载机部队训练水平评估指标体系,对舰载机部队训练水平进行了评价,通过实例分析验证,该方法切实可行,大大降低了主观因素的影响,可以切实提高对舰载机部队训练水平评估的精确度,从而为舰载机部队训练决策提供依据。

## 参 考 文 献

[1] 魏岳江. 复杂电磁环境下的联合训练[J]. 国防科技,2008,28(4):62-67.

[2] 郭齐胜,等. 装备效能评估概论[M]. 北京:国防工业出版社,2005:100-106.

[3] 覃菊莹. 灰色层次分析法-GAHP[D]. 南宁:广西大学,2002:5-25.

[4] 张笑,徐廷学,范树海. 基于灰色层次分析法的武器系统综合保障能力评估[J]. 海军航空工程学院学报,2009(3):351-355.

[5] 魏培智,复杂电磁环境下航空兵训练评估系统研究[J]. 计算机工程与应用,2012,48(31):236-243.

[6] 黄勇,孙德翔,邢国平. 基于灰色层次分析法的装备备件重要度评价[J]. 航空维修与工程,2010(4):66-68.

[7] 王保乳,等. 基于 G-AHP 的舰载机一体化训练系统支持能力评估[J]. 四川兵工学报,2014(8):59-64.

[8] 刘义,王国玉,冯德军,等. 基于装备作战效能的复杂电磁环境下训练效果评估[J]. 系统仿真学报,2009,21(17):5375-5378.

[9] 彭鹏菲,任雄伟,张建强. 复杂电磁环境下舰艇编队装备体系作战效能评估研究[J]. 舰船科学技术,2009,31(5):105-107.

[10] 高辅刚,赵晔,胡晓峰,等. 复杂电磁环境下作战仿真系统指挥控制体系建模[J]. 火力与指挥控制,2008,33(7):112-116.