文章编号:1671-4598(2017)10-0202-04 DOI:10.16526/j.cnki.11—4762/tp.2017.10.051 中图分类号:TP309 文献标识码:A

基于扩频技术联合小波算法的安全通信方案设计

张 弛[1],杜 洋[2]
(1. 西宁联勤保障中心,甘肃 白银 730900;2. 国防科技大学 信息通信学院,武汉 430010)

摘要:在信息化技术高度发达的今天,为了适应变化莫测的战场环境对于安全信息通信的高要求,文章在研究探讨水印嵌入检测技术的基础上,利用秘钥产生的扩频码调制水印信息,紧接着通过小波变换对调制后的水印进行信息嵌入操作,而在接收端采用相反的操作对加密信息进行计算机检测后解调恢复,实现信息的隐秘传输;通过实验仿真证明了所提方案可以有效实现对信息的隐蔽传输,其具有很好的安全性,同时对于剪裁攻击具有一定的鲁棒性。

关键词:扩频技术;数字水印;安全通信;小波变换

Design of Secure Communication Scheme Based on Spread Spectrum Technology and Joint Wavelet Algorithm

Zhang Chi[1], Du Yang[2]
(1. Xining Logistic Support Center, Baiyin 730900, China;
2. Information Commuaication Academy, NUDT, Wuhan 430010, China)

Abstract: In today's world is a modern information world, in order to adapt to the change constantly battlefield environment high requirement for secure information communication, based on watermark detection technology in the research on spread spectrum watermark information generated by the secret key, followed by the wavelet transform of the modulated watermark information is embedded in the operation. The receiver uses the reverse operation of the encrypted information is demodulated to restore the computer after detection, realize the secret information transmission. The simulation results show that the proposed scheme can effectively realize the covert transmission of information. It has good security and robustness to clipping attacks.

Keywords: spread spectrum technology; digital watermarking; secure communication; wavelet transform

0 引言

信息保密技术作为信息安全技术的一个分支,其吸引了众多的学者,发展至今已经成为了一门备受关注的热点学科。其在军事方面的应用更是具有着巨大的价值,在当前信息化的战场环境下,是否能够安全并且秘密地对重要的军事信息进行传输,同时要保证信息的不可窃听、数据完整,这决定着整个战场上的信息控制权,甚至影响着整个战争的胜负。因此应用于军事的隐蔽通信技术更加显得至关重要。当前阶段,主要的保密军事通信手段为:建立安全可靠的通信信道、对传送信息进行加密、以及将发送的信息进行隐藏使其不可见。几年来,随着信息隐藏技术的不断发展,扩频技术、语义编码和流星余迹散射通信技术等先进的信息隐藏技术都在军事通信中获得了应用[1-4]。

诞生于20世纪90年代的水印技术作为信息隐藏通信技术中一个最重要的分支,其可以将信息嵌入到特定的多媒体信息中,同时嵌入后其是不可见的,因此,其在知识产权保护中的应用也越来越广泛。伴随着军事通信对于保密通信的要求不断提高,将数字水印技术应用到军保密通信中所具有的巨大潜力也获得了更多研究学者的关注。本文讨论了数字水印技术,并采用扩频码作为调制,通过小波变换将水印嵌入到载体中实现信息的隐藏,进而达到信息隐藏安全通信的目的[5-7]。

本文的结构安排如下:首先介绍了数字水印算法实现水印嵌入与提取从而对信息进行隐藏的过程,随后介绍了扩频技术的原理及其应用场景,紧接着提出了基于扩频数字水印技术的军事安全通信方案其具体流程,最后通过仿真实验证明了该方案的可行性以及对于噪声污染的抗攻击性。

1 数字水印通信技术

采用数字水印对信息进行隐藏进行信息通信是一种非常合适的保密通信技术。当前有多种方法可以实现数字水印,一般分为空域水印和变换域水印,其分别通过改变对应载体图像的某些特定像素的灰度值或者是其在变换域中的特性进行水印信息的嵌入,同传统的空间域方法相比,变换域的方法更有利于确保信息的不可见特性。

在传统的通信系统模型中,一般分为3个部分组成,信息的发送方,信息的传输以及信息的接收部分,即输入信息的调制编码、含噪声信道、信息的接收解调部分。相对应的作为一种信息的通信过程,数字水印系统也有着类似于通信系统的结构,基本思想是从水印的嵌入方向水印的提取方即信号接收方发送信息,数字水印系统如图1所示[8-11]。

如图1所示,数字水印系统是在传统通信传输系统模型上进行了功能扩展而发展来的。其对应于通信系统可以理解为:原始的载体信号可以当做是通信系统中信道和载波信号的合

收稿日期:2017-07-21; **修回日期**:2017-08-30。

作者简介:张 弛(1991-),男,陕西咸阳人,研究生,主要从事军事通信组织与运用方向的研究。

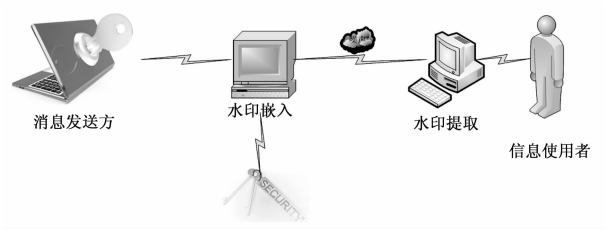

图 1　数字水印安全通信系统示意图

体，而要嵌入的水印则是待传输的信号，对于接收方对水印的提取与恢复则可以看做是对信号的解调过程。

2　扩频技术

根据信息理论的基础理论可知，在高斯白噪声信道条件下信道容量满足香浓公式[12-15]：

$$C = B\log_2\left(1+\frac{S}{N}\right) \tag{1}$$

其中：C 是信道的容量，B 是频带带宽，S 和 N 分别是信号的平均功率以及噪声功率。这表明，如果在信号以及噪声功率确定的情况下，通过采取合理的编码方式以使得信号充分利用信号的带宽就可以以接近于信道最大容量 C 的传输率进行信息传输。而如果在保持 信道容量 C 不变的情况下，信号的平均功率与噪声功率可以相互交换以满足不同通信的要求。也就是说通过增加信号的频带宽度，能够实现在低信噪比情况下以任意的差错概率进行信息传输，即便信号质量相当差淹没于噪声之中，只要带宽相应增加依然能够实现可靠通信。这种通过扩展频带进行通信的思想可以获得信噪比上的极大优势。如图 2 所示为一个一段信号的扩频后效果图。

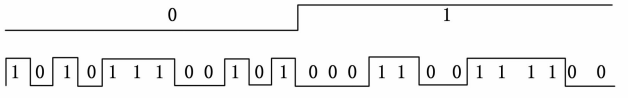

图 2　信号扩频示意图

M 序列扩频技术是一种非常常见的扩频技术，其采用一个数字编码序列直接对所传输的信号进行调制，因为编码的序列带宽远远大于原始信号的带宽，相当于其对信号的频谱进行了扩展。M 序列是最大长度线性以为寄存器序列的简称，通过将 n 个移位寄存器串接起来，适当的设置其反馈连接可以使序列周期最长达到 $T=2^n-1$，这个序列就是 M 序列。

M 序列的本原多项式可以如下表示：

$$f(x) = \sum_{j=0}^{N} c_j x^j \tag{2}$$

这里系数 c 是反馈的状态，如果为 0 则表示反馈不同，如果为则表示反馈是通的。在 M 序列的 n 很大的时候，其自相关值会出现尖峰，因此可以用来可靠地检测和恢复水印信息。

3　基于扩频技术联合小波算法的安全通信方案设计

结合扩频技术的优势，将制作好的水印信息转变到扩频后的编码上获取到扩频水印信息，随后采用小波变换对扩频信息进行变换，因为水印的位置是未知的，所以非法用户是不能够对水印信息进行解扩的，更得不到任何有效信息。如果非法用户对水印信息进行攻击，则需要在所有的小波域系数中加入一个非常大的噪声，而这样同时也会对原载体信号的质量造成非常大的破坏，很容易就暴露。只要保证水印信号的能量足够的小，加入原始数据中的水印信息就可以得到很好地隐藏同时不被感知。另一个方面，通过采用秘钥产生 m 序列，在合法用户一侧也必须获得控制秘钥以及相关的算法，不然的话其不能够正确地提取出水印信息。综上，基于扩频水印的安全通信方案的安全性和健壮性都较高。

3.1　小波水印检测算法

假定一幅大小为 $M*N$ 的灰度图像 X（M，N）采用小波算法进行水印嵌入。第一步需要对图像 X（M，N）进行 I 层的小波分解，分解后得到 $3\times l$ 个细节图像和一个低频近似图像，

$$\begin{aligned} &X_k, I(m_i, n_j) \mid k = h, v, d; I = 1, 2, \ldots I; \\ &m_i = 1, 2, \ldots, M/2^I; n_j = 1, 2, \ldots, N/2^I \end{aligned} \tag{3}$$

表示选择的小波系数，其中 l 表示分解的层次，$k=h$，v，d 分别表示第 l 层水平、垂直和对角方向的子图像。考虑到量化低频子图可能产生较大失真，因此不在其中嵌入水印，而选择除低频外的中频系数。

第二部根据嵌入的信息量和对算法鲁棒性的要求，块越大，水印的鲁棒性越好，但嵌入的水印比特少。把 X_K，l（m_i，n_j）分成一定大小的块，用 $Block$（s，t）表示 X_K，l（m_i，n_j）中大小为 $s\times t$ 的系数块，其中 $s=1$，2，…，m_i，$t=1$，2，…，n_j，b 为正整数，代表该块的编号。其平均值为：

$$Ave = \sum Block(s,t)/(s*t) \tag{4}$$

其中：$\sum Block$ 为块内系数幅值的累计和。

水印序列 w 的嵌入是通过对 Ave 的量化完成的，例如：量化成奇数代表嵌入“1”，量化成偶数相当于嵌入“0”。根据对鲁棒性和隐藏性的折中考虑，设量化间隔 $\triangle_l$，$l=1$，2，…，l 表示分解层数，对于低频的第 l 层，由于系数幅值极大，可以作较大间隔的量化，对第 $l-1$，…，1 层次作间隔逐渐减小的量化。

根据 $w_i=\{0,1\}$ 将 Ave 量化到与之最近的奇、偶点。用 Dat（i，j）表示 $Block$ 中的一个小波系数，量化后的该系数用 Dat'（i，j）表示，其中 $i=1$，2，…，s；$j=1$，2，…，t。

设 $T=Ave/\triangle_l$，$Turdat=rem$（$[T]$，2）其中 [] 表示四舍五入取整，rem 表示求 $[T]$ 除以 2 的余数。

若 Turdat 与 w_i 相同，则量化的小波系数为：

$$Dat'(i,j) = Dat(i,j) + [T]\times\Delta_l - Ave$$

若 Turdat 与 w_i 不同，小波系数按下列量化：

$$\begin{aligned} Dat'(i,j) &= Dat(i,j) + ([T]+1)\times\Delta_l - Ave, T \geqslant [T] \\ Dat'(i,j) &= Dat(i,j) + ([T]-1)\times\Delta_l - Ave, T \geqslant [T] \end{aligned} \tag{5}$$

3.2　水印的嵌入

对于数字水印的嵌入过程就是将水印信息首先进行调制扩频操作后加入到目标载体信号中，从而得到一个加载了水印信息的载体。第一步将水印信息转换为一个一维的二进制信息 $w[i], i=1,2\ldots n; w[i]\in\{-1,+1\}$，随后对该信号进行采样，得到一个调制后的信号 $c[k]$，随后采用 m 序列扩频编码技术对该产生的调制信号 $c[k]$ 进行扩频，扩频后就得到扩频水印信号：$q[k]=c[k]m[k]$。得到扩频信号后使用小波变换对其进行

变换加载到经过小波变换的多媒体载体信息当中，随后再通过变换抑或是反变换得到包含水印信息的载体：

$$I'(i,j) = I(i,j) + aq[k] \tag{3}$$

各个频带的小波系数［ca ch cv cd］的水印嵌入公式如下所示：

$$\begin{aligned} c &= (1-a) * ca + a * cwa; \\ h &= (1-a) * ch + a * cwh; \\ v &= (1-a) * cv + a * cwv; \\ d &= (1-a) * cd + a * cwd. \end{aligned} \tag{4}$$

公式中的 a 系数是由主观决定的，a 大则是鲁棒性高，a 小则是更加透明，方案设计过程中应是首先使得透明度较高，是水印不易被感知。具体的水印嵌入过程如图 3 所示。

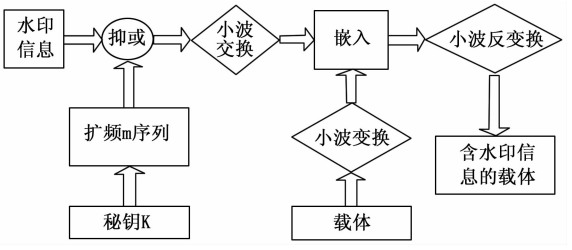

图 3 水印嵌入过程示意图

3.3 水印测量提取

在对水印信息进行提取时，为了能够提高整个系统的健壮性，通常利用载体信息进行水印的检测与恢复。分别对嵌入水印的载体信息以及原始未加水印的载体信息进行小波变换得到其各自的小波系数［$cwa\ cwh\ cwv\ cwd$］和［$ca\ ch\ cv\ cd$］，提取出小波系数后按照如下所示的公式提取出扩频水印信息的系数。

$$\begin{aligned} c &= (cwa - (1-a) * ca)/a; \\ h &= (cwh - (1-a) * ch)/a; \\ v &= (cwv - (1-a) * cv)/a; \\ d &= (cwd - (1-a) * cd)/a. \end{aligned} \tag{5}$$

通过以上公式进行计算后就可以得到水印信息的小波系数，随后利用相同的秘钥 K 控制的 m 序列进行反向解扩，将其恢复到原始的水印信息，具体的水印检测过程如图 4 所示。

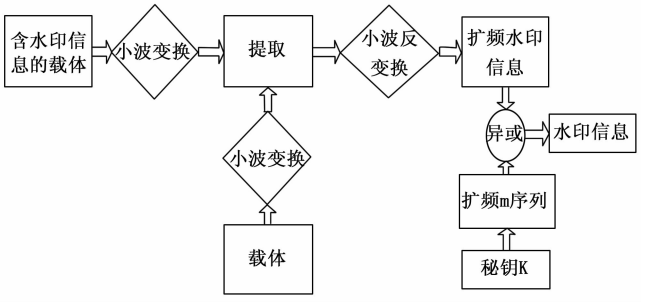

图 4 水印检测恢复示意图

4 实验结果与分析

这一章我们对所设计的安全通信方案进行仿真验证，验证一共分为两个部分，分别验证该方案的可行性以及其可靠性。为了能够客观的评价恢复前后图像的质量，引入峰值信噪比（PSNR）和相似度（NC）的概念作为对于图像质量的客观评价指标。其定义如下：

$$PSNR = 10\lg \frac{MN \max_{m,n} x^2(m,n)}{\sum_{m,n} (x(m,n) - x_s(m,n))^2} (\text{dB}) \tag{6}$$

$$NC = \frac{\sum_{m,n} Ws(m,n)W(m,n)}{\sum_{m,n} W^2(m,n)} \tag{7}$$

在试验中分别计算恢复图与原图的 PSNR 和 NC，以及水印恢复图与原图的 PSNR 和 NC，以此判断该通信方案过程中的信息隐藏与恢复效果。

4.1 结果验证与讨论

实验在操作系统为 Windows7，CPU 为 Intel i3 主频 2.27 GHZ 的 PC 上进行，采用 MATLAB 作为模拟仿真软件，通过将目标信息加载到数字图像上进行通信传输，载体图像大小 256 * 256 像素，而水印图像大小则为 64 * 64 像素。

如图 5 所示为一个大小为 256 * 256 像素的 airplane 图嵌入水印后进行水印恢复的恢复示意图，可以从图中看出采用本通信方案后载体信息以及水印信息都得到了很好的恢复，在通信系统的传输过程中可以看出载体信息嵌入水印后肉眼是识别不出水印的，同时原图像的视觉效果没有收到影响，可见成功实现了对水印信息的隐藏同时成功将信息通过通信系统进行了有效传输。最后也成功恢复出了传输的水印信息，表明该通信方案方案是有效可行的。采用该方案进行恢复的载体图像和水印图像的质量为：

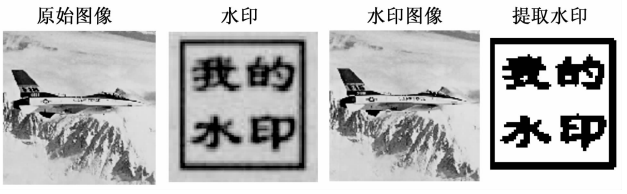

图 5 水印嵌入恢复示意图

$$\begin{aligned} &monkeyPSNR = 27.65, monkeyNC = 0.99; \\ &waterPSNR = \inf, waterNC = 1. \end{aligned} \tag{8}$$

随后我们对于该通信方案在不同剪裁攻击情况的健壮性进行性能分析，分别测试其在图像剪裁率 0 到 50%时的载体图像以及水印图像恢复质量。每次都是采用 monkey 图在相同的条件下进行试验，如图 6 所示是在不同剪裁率下恢复信息的质量变化趋势。

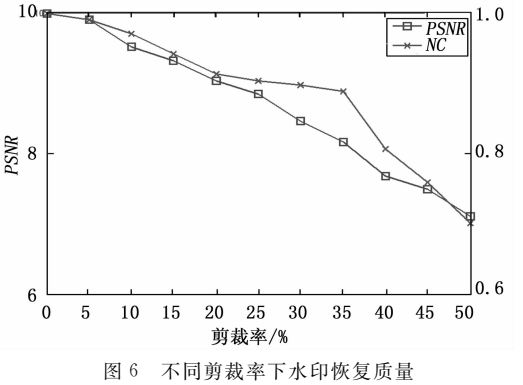

图 6 不同剪裁率下水印恢复质量

如图 6 所示，可以看出随着剪裁率的不断增加，目标水印的恢复质量也随之不断地下降，PSNR 与 NC 两者都随着剪裁

率的不断增加而随之不断下降，但是在另一方面可以看出虽然剪裁攻击对于水印的恢复质量产生了影响，但是其并没有造成致命性的破坏，水印的质量依然可以满足需求。这证明所提方案针对于剪裁攻击具有相当好的健壮性。

4.2　实验方案的不足

该通信方案结合扩频水印技术设计了安全通信方案，虽然可以实现对信息安全传输的目的需求，但是依然存在一些有待改进的地方。

1）该方案采用水印技术对信息进行隐藏，水印算法是多种多样的，这里只采用了小波算法做水印隐藏，没有对其他算法进行相应的分析，这导致了该方案的片面性。

2）为了能够满足信噪比的要求采用了扩频技术进行相应的处理，但是这样做对信号的处理性能提出了更高的要求，同时也给算法复杂度带来了挑战，降低了运行效率。

5　结论

本文基于扩频数字水印技术，结合小波变换算法针对战场对于信息安全的高要求设计了基于扩频数字水印技术的安全通信方案。提出了首先将待加载的水印信息转换为一维二进制信息，随后对其进行采样调制进行水印信息的预备工作，然后使用秘钥产生 m 序列的扩频编码技术对其进行扩频编码，这一方法使得水印信息的安全性获得了极大的提高。随后通过小波变换对水印进行嵌入与提取操作，控制合适的水印能量使得水印信息不可被感知然后经过通信系统的传输接收，这同时保护了水印信息难以收到破坏性攻击的侵入。最后通过仿真实验证明该方法是有效的，可以实现信息的隐藏，同时其对于破坏性攻击具有一定的防护。该通信方案针对于保密传输拥有很高的安全性，同时对于剪裁攻击也具有很好的鲁棒性，在实际应用中具有很广阔的前景。

参考文献：

[1] 孙　锐，孙　洪，赵晓岚. 基于量化的扩频水印技术 [J]. 通信技术，2002 (2)：63－66.

[2] 龚　阳，崔　琛，王　津，等. 基于扩频通信的无线抄表系统设计与实现 [J]. 计算机测量与控制，2016，24 (12)：237－240.

[3] 周利军. 数字图像水印的扩频实现 [J]. 红外与激光工程，2000，29 (5)：27－31.

[4] 张　东，倪江群，李大捷. 基于 GSM 模型的扩频水印安全性分析 [J]. 自动化学报，2009，35 (7)：841－850.

[5] 孙圣和，陆哲明. 数字水印处理技术 [J]. 电子学报，2000，28 (8)：85－90.

[6] 程兴国，高　升. 信息隐藏与数字水印 [J]. 湖北工业职业技术学院学报，2004，17 (2)：65－67.

[7] 兀旦晖，郑恩让. 基于混沌 Logistic 和 Arnold 二次加密的图像水印算法研究 [J]. 计算机测量与控制，2017，25 (4)：193－196.

[8] 钮心忻，杨义先，NIUXin－Xin，等. 基于小波变换的数字水印隐藏与检测算法 [J]. 计算机学报，2000，23 (1)：21－27.

[9] 傅德胜，孙文静，张小飞. 基于混沌特性的小波数字水印技术及实现 [J]. 计算机科学，2008，35 (6)：246－250.

[10] 徐祗军，吴晓娟，杜会斌，等. 扩频数字水印与军事通信 [J]. 军事通信技术，2005 (4)：58－60.

[11] 胡　鹏. 基于正交扩频码和 HVS 的 DCT 域图像数字水印技术 [J]. 信息安全与通信保密，2008 (7)：80－82.

[12] 刘忠英，许金勇，柳永祥. 频谱水印技术与军事应用分析 [J]. 现代军事通信，2013 (1)：45－48.

[13] 刘勇顺. 数字水印技术在军事信息安全中的应用 [J]. 现代电子技术，2006，29 (19)：64－66.

[14] 靳小晖. 音频信息隐藏技术在军事通信中的实际运用 [J]. 信息通信，2015 (5)：178－178.

[15] 康　芳，谭　薇，杨森斌. 信息隐藏技术及其在军事通信领域的应用研究 [J]. 现代电子技术，2008，31 (23)：97－99.

(上接第 201 页)

动化与智能化，由于学习到的模式与规律在各种类型的恶意代码中是基本稳定的，对新出现的恶意代码也有很好的检测能力。

目前实验的恶意代码库规模较小，特征提取的维数较小，图特征提取没有对冗余信息进行处理，这是下一步需要解决和完善的问题。

参考文献：

[1] 冯本慧. 基于数据挖掘于机器学习的恶意代码检测技术研究 [D]. 长沙：中南大学，2013.

[2] Nagaprasad S，Reddy T R，Reddy P V，et al. Empirical evaluations using character and word N－grams on authorship attribution for Telugu text [M]. Intelligent Computing and Applications，Springer India，2015：613－623.

[3] Shubair A，Ramadass S，Altyeb A A. kENFIS：kNN－based evolving neuro－fuzzy inference system for computer worms detection [J]. Journal of Intelligent & Fuzzy Systems Applications in Engineering &Technology，2014，26 (4)：1893－1908.

[4] Zhang M，Duan Y，Yin H，et al. Semantics－ AwareAndroid Malware Classification Using Weighted Contextual API Dependency Graphs [A]. ACM [C]. 2014：1105－1116.

[5] 刘　星. 恶意代码的函数调用图相似性分析 [J]. 计算机工程与科学，2014：1－3.

[6] 杨　帆. 基于图编辑距离的恶意代码检测 [J]. 武汉大学学报，2013：1－3.

[7] 赖兴瑞. 基于最大公共子图的中文 Web 文本分类研究 [D]. 厦门：厦门大学，2011.

[8] 颜克文. 基于图特征向量的安卓程序相似性检测算法研究 [D]. 湘潭：湘潭大学，2014.

[9] Seo S H，Gupta A，Mohamed S A，et al. Detecting mobile malware threats to homeland security through static analysis [J]. Journal of Network and Computer Applications，2014，38：43－53.

[10] Jang J，Woo M，et al. Towards automatic software lineage inference [A]. Proceedings of the 22nd USENIX conference on Security. USENIX Association [C]. Berkeley，CA，USA：USENIX Association，2013：81－96.

[11] Grace M，Zhou Y，Zhang Q，et al. RiskRanker：Scalable and Accurate Zero－day Android Malware Detection [A]. Proceedings of the 10th International Conference on Mobile Systems，Applications and Services (MobiSys'12) [C]. 2012：4－20.

[12] Arp D，Spreitzenbarth M，Hübner M，et al. Drebin：Efficient and Explainable Detection of Android Malware in Your Pocket [A]. Proceedings of the 21th Annual Network and Distributed System Security Symposium (NDSS'14) [C]. 2014.

[13] Peng H，Gates C，Sarma B，et al. Using Probabilistic Generative Models for Ranking Risks of Android Apps [A]. Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS' 12) [C]. 2012：2－5.