一种二进制数字指纹编码算法*

王 彦[1,2+], 吕述望[1,2], 徐汉良[1]

[1](中国科学院 研究生院 信息安全国家重点实验室,北京 100039)

[2](中国科学院 电子学研究所,北京 100080)

A Digital Fingerprinting Algorithm Based on Binary Codes

WANG Yan[1,2+], LÜ Shu-Wang[1,2], XU Han-Liang[1]

[1](State Key Laboratory of Information Security, Graduate School, The Chinese Academy of Sciences, Beijing 100039, China)

[2](Institute of Electronics, The Chinese Academy of Sciences, Beijing 100080, China)

+ Corresponding author: Phn: 86-10-68154759 ext 26, E-mail: ywang_cas@yahoo.com

http://home.is.ac.cn

Received 2002-04-17; Accepted 2002-09-06

Wang Y, Lü SW, Xu HL. A digital fingerprinting algorithm based on binary codes. *Journal of Software*, 2003, 14(6):1172~1177.

http://www.jos.org.cn/1000-9825/14/1172.htm

Abstract: Digital fingerprinting has appeared as a new technique for copyright protection of digital contents. How to defense collusive attack is one of the key problems when designing fingerprinting algorithms. In this paper, based on the binary random coding methods, a fingerprinting algorithm and the corresponding tracing algorithm are proposed by using a pseudo-random sequence to control the embedding of the fingerprint bits. Both theoretical analysis and experimental results show that under reasonable collusion size, by the fingerprinting algorithm, the owner can trace the traitors quite efficiently and the probability to accuse an innocent buyer can be made as close as to 0. Furthermore, because the owner need not know the buyers' fingerprints, the method can serve as a good coding algorithm in the design of asymmetric fingerprinting schemes.

Key words: digital fingerprinting; digital watermarking; collusive attack; copyright protection; pseudo-random number generator

摘 要: 抗合谋攻击是数字指纹技术中需要解决的关键问题之一.基于二进制随机编码,通过使用伪随机序列对指纹比特的重复嵌入进行控制,提出了一种有效的抗合谋攻击的数字指纹编码算法及其相应的跟踪算法.理论分析和实验结果表明,在适当的合谋尺寸下,该算法能够对非法分发者进行有效跟踪,同时无辜用户被诬陷的概率可以根据要求接近于0.由于在该算法中发行商无须知道用户原来的码字,因此可以说该算法是设计非对称

* Supported by the National Grand Fundamental Research 973 Program of China under Grant No.G1999035805 (国家重点基础研究发展规划(973)); the Youth Foundation of the National High-Tech Research and Development Plan under Grant No.2001AA140447 (国家高技术研究发展计划青年基金); the Innovation Foundation of the State Key Laboratory of Information Security of Graduate School of the Chinese Academy of Sciences of China (中国科学院研究生院信息安全国家重点实验室创新基金)

第一作者简介: 王彦(1976－),女,河南新乡人,博士生,助理研究员,主要研究领域为数字产品版权保护,密码学.

指纹的一个很好的备选算法.

关键词: 数字指纹;数字水印;合谋攻击;版权保护;伪随机数发生器

中图法分类号: TP309 **文献标识码**: A

近年来,信息技术的迅猛发展以及以信息技术为基础的电子商务的广泛应用使各类文字、图片、音乐、影视等作品通过网络的传播范围空前扩大,为创作者和发行商带来了新的机遇.但同时,以数字形式存在的产品很容易被非法拷贝和分发,如何对数字化产品进行版权保护已经成为信息时代产权保护的核心问题之一.

数字水印技术和数字指纹技术是近几年发展起来的新型数字版权保护技术.发行商通过在其所要发售的拷贝中嵌入与购买者有关的数字指纹可以对盗版行为进行跟踪.由于各个用户所得到的拷贝不同,通过合谋他们就可能发现码字的嵌入位置或内容.因此,抗合谋攻击是数字指纹研究中需要解决的一个根本问题之一.对要嵌入的指纹信息进行编码是解决此问题的一种有效手段.在指纹编码的经典文献[1]中,Boneh 和 Shaw 讨论了抗合谋攻击的数字指纹的编码和跟踪问题.他们首先提出了嵌入假设(marking assumption),并在此基础上提出了一种指纹码字的长度与用户个数的对数成比例的编码算法.由于该嵌入假设要求用户对码元相同的比特位无法作出修改,一个误发的随机错误就可能导致错误判断.文献[2]指出,若参与合谋的用户所对应的码字标号有较大间隔,则会以较高概率产生误判.文献[3,4]对文献[1]中的弱点进行了进一步的研究,并提出了更切合实际的嵌入假设.文献[5]提出了一种基于对偶二元汉明码的抗两个人合谋攻击的指纹编码算法.Löfvenberg 和 Wiberg 在文献[6]中提出了一种二进制随机指纹编码算法,并给出了一种对可疑用户组进行检测的算法,其码字的长度与抗合谋尺寸 C 的指数级成正比.不过该检测算法并非一个跟踪算法,它只是对用户组成的集合是否可能合谋进行检测.本文同样采用二进制随机码字作为用户的指纹信息,但我们对每个比特进行重复嵌入并采用二进制伪随机序列控制其中某些比特取反后嵌入,同时我们提出了相应的跟踪算法.而且在本算法中,即使发行商不知道用户原来的指纹码字,也可以通过相应的伪随机序列对合谋用户的码字信息进行还原,这有助于非对称数字指纹体制(参见文献[7])的构造.当合谋人数不太大时,我们的编码算法及跟踪算法是非常有效的.

本文第 1 节给出我们的编码及跟踪算法的基本思想及其具体描述.第 2 节给出理论分析及实验结果.第 3 节对该算法的特点进行了讨论.最后是结束语及进一步改进的建议.

1 编码及跟踪算法

1.1 基本思想

我们首先讨论数字指纹为二进制码字的情况.假设存在这样一个指纹嵌入算法:对于各个用户的指纹,其嵌入方法是相同的,而仅是嵌入的内容不同.设用户 u 的码字为 $a_u=(a_{u,1},...,a_{u,l})\in F_2^l$,$c$ 个用户 $u_1,u_2,...,u_c$ 合谋,如果在第 i 个比特处有 $a_{u_1,i}=a_{u_2,i}=...=a_{u_c,i}$,则称比特 i 处为不可侦察位.如果上述等式中有一个等号不成立,则称比特 i 处为可侦察位.另外,假设存在一个“安全”的嵌入方法(参见文献[1]中提出的“嵌入假设”).

合谋的用户通过对比他们的拷贝,只能在可侦察位发现指纹,且只能从两个版本中任选一个;对其他任何位置,合谋用户不能侦察到指纹;且在不破坏数据可用性的情况下,合谋用户无法改变这些位置处的指纹信息.

设合谋用户所伪造出的码字为 a_p,则根据嵌入假设,a_p 满足 $a_{p,i}\in\{a_{u_1,i},a_{u_2,i},...,a_{u_c,i}\}$,$i=1,...,l$.

每一个用户被分配一个长为 l 的随机二进制码字,每个比特重复 m 次.因此每个用户的码字的总长度为 $L=l\times m$.称每个码元重复嵌入的 m 个比特为一个块.假设发行商有一个安全的二进制伪随机数发生器,对于每个用户来说,发行商选择一个随机种子,用伪随机数发生器生成的伪随机序列去控制重复的比特中哪些比特取反后嵌入.跟踪时发行商将非法拷贝中的比特提取出来,并用相应的伪随机序列进行还原,如果该用户参与了合谋,则在还原后的块中将会出现‘0’占优势或者‘1’占优势的情况,因为非法拷贝中的比特含有合谋者在不可侦察位的信息.而对于无辜的用户,只要所使用的伪随机序列具有很好的随机性,则在还原后的块中,‘0’,‘1’将是均衡的.根据还原后块中‘0’,‘1’的均衡情况,我们可以对合谋用户与无辜用户进行区分.

1.2 具体算法

符号约定:n:用户数目;l:随机二进制码字长度;m:重复嵌入次数;$L=l\times m$ 是码字总长度;

r_B, seq_B:分别对应发行商 M 为用户 B 所选择的伪随机数发生器的种子及生成的伪随机序列;

$pirate\_seq$:从非法拷贝中提取出的长为 L 的序列;

m_{cri}:判断某个码元是否为可判定的门限值.

算法 1. 指纹编码(假设发行商拥有一个安全的伪随机数发生器).

每一位用户被分配一个长为 l 的随机二进制码字,如用户 B 得到 a_B,每个比特重复 m 次嵌入,重复序列记为 a_B^{rep},长度为 L.

发行商为用户 B 随机选择一个种子 r_B,并用该伪随机数发生器得到一个长度为 L 的伪随机序列 seq_B.然后将 $seq_B\oplus a_B^{rep}$ 作为嵌入内容嵌入到原拷贝,得到的新拷贝就是 B 要购买的拷贝.发行商存储 r_B(注意,如果随机种子的长度取为 r_l,则要求 $2^{r_l}>>n$,以使不同用户的随机种子不相关).

算法 2. 跟踪算法.

当发行商获得一个被非法分发的拷贝时,他首先运用相应的指纹提取算法提取出该拷贝中的信息 $pirate\_seq$.对所有的用户,执行以下操作(以用户 B 为代表):

对用户 B,发行商用 r_B 生成 seq_B,计算 $pirate\_B=pirate\_seq\oplus seq_B$,并将结果按顺序等分为 l 组,每组 m 个比特,记第 i 个分组为 $pirate\_B_i$,即 $pirate\_B_i=block\_pirate_i\oplus seq_{B,i}$,其中 $block\_pirate_i$, $seq_{B,i}$ 是分别将 $pirate\_seq$, seq_B 顺序等分为 l 组时的第 i 个分组.

对 $pirate\_B_i$,记其中占优势的比特个数为 Y_i,如果 $Y_i>m_{cri}$,则认为该块是可判定的,并认为 a_B 的第 i 个码元是该占优势的比特,此时也称该比特是可判定的;否则认为是不可判定的.

如果对用户 B,可判定的比特数目大于 N_T,则认为 B 是合谋分发者;否则,认为 B 是无罪用户.

在上述算法中,参数 m_{cri} 与 N_T 的选择与合谋人数 c 及跟踪成功率以及用户不被诬陷的概率要求等因素有关,在下一节中我们将对此进行讨论.

2 算法分析

2.1 参数选择

设合谋人数为 c.我们先对判断一个块是否为可判定的成功率进行分析.如果 c 个用户合谋,$block\_pirate_i$ 可以看成是与 $seq_{u_k,i}\oplus a_{u_k,i}^{rep}$ 有关的一个函数(其中,u_k 指代合谋用户,k 从 1 到 c).由嵌入假设,在 $block\_pirate_i$ 中,将有 $m/2^{c-1}$ 个不可侦察比特.对于合谋用户 B,用 $seq_{B,i}$ 进行还原后,该不可侦察比特将被还原为全‘0’或全‘1’(依于 a_B 的第 i 个码元的原符号).而其余 $m(1-1/2^{c-1})$ 个位置可能被合谋用户任意选取,但由于 $seq_{B,i}$ 的随机性,这些位置经过还原后,‘0’,‘1’将是均衡的.所以,还原后的比特中占优势的符号的比例为 $\frac{1}{2}+\frac{1}{2^c}$.

而对于无辜用户 B',如果该随机数发生器是安全的,则 $seq_{B'}$ 与合谋者所对应的随机序列 seq_{u_k} 是不相关的.又由于 $seq_{B'}$ 的随机性,因此在 $pirate\_B_i'$ 中,‘0’,‘1’的个数应是均衡的(以上讨论假设 m 足够大).

引理 1(Chernoff 界). 参考文献[8]中的定理 A.4 及其前面的注释.令 $X_1,X_2,...,X_n$ 是独立的 0-1 随机变量,且对任意 i,有 $\Pr[X_i=1]=p$.令 $X=\sum_{i=1}^{n}X_i$, $\mu=E(X)$, 则对于任意的 $t>0$, 有 $\Pr[X-\mu>t]<\exp\left(\frac{-2t^2}{n}\right)$ 及 $\Pr[X-\mu<-t]<\exp\left(\frac{-2t^2}{n}\right)$

下面的定理指出,当码元的重复次数取得足够大时,可以使对一个块进行判定时的两类错误概率足够小.

定理 1. 设 p_a, p_f 分别为无辜用户的某个码元被认为是可判定的概率及将合谋用户的码元认为是不可判

定的概率.只要 $m > 2^{2c-1}(\sqrt{-\ln\varepsilon_1}+\sqrt{-\ln\varepsilon_2})^2$,就可以取合适的 m_{cri} $(m/2 < m_{cri} < mp)$ 使得 $p_a < \varepsilon_1, p_f < \varepsilon_2$,其中 $p=\frac{1}{2}+\frac{1}{2^c}$.

证明:设对应于无辜用户 B'的 $pirate\_B'_i$ 中'1'的个数为 X,由于 $seq_{B'}$ 的随机性,X 服从二项分布 $B(m,1/2)$.对于合谋用户 B,占优势的符号(不妨设为'1')的个数为 Y,则 Y 服从二项分布 $B(m,p)$,其中 $p=\frac{1}{2}+\frac{1}{2^c}$,则 $p_a = p(X > m_{cri}),\ P_f = P(Y < m_{cri})$.由引理 1 中 Chernoff 界可得:

$$p_a = p(X > m_{cri}) = P(X-\frac{m}{2} > m_{cri}-\frac{m}{2}) < \exp\left\{-\frac{-2(m_{cri}-m/2)^2}{m}\right\}.$$

设 $m_{cri} < mp$,则 $P_f = P(Y < m_{cri}) = p(Y-mp < m_{cri}-mp) < \exp\left\{-\frac{2(mp-m_{cri})^2}{m}\right\}$.我们希望 $p_a < \varepsilon_1, p_f < \varepsilon_2$,则只要

$$\exp\left\{-\frac{2(m_{cri}-m/2)^2}{m}\right\} < \varepsilon_1 \Leftrightarrow m_{cri} > \sqrt{\frac{-m\ln\varepsilon_1}{2}}+\frac{m}{2} = f_1(m,\varepsilon_1),$$

$$\exp\left\{-\frac{2(mp-m_{cri})^2}{m}\right\} < \varepsilon_2 \Leftrightarrow m_{cri} < mp-\sqrt{\frac{-m\ln\varepsilon_2}{2}} = f_2(m,\varepsilon_2),$$

因此要求 $f_1(m,\varepsilon_1) < f_2(m,\varepsilon_2)$.又 $p=\frac{1}{2}+\frac{1}{2^c}$,因此要求 $m > 2^{2c-1}(\sqrt{-\ln\varepsilon_1}+\sqrt{-\ln\varepsilon_2})^2$. □

我们还可以通过在一定范围内调节 m_{cri} 来调节误判和漏判的概率(即 p_a 和 p_f).举例:$c=3, \varepsilon_1=\varepsilon_2=1/e^2$,取 m=512,我们从图 1 可以看到从数量上两类错误概率随 m_{cri} 而发生变化的情况,图 2 中给出了两类错误概率的对应关系(图 1 和图 2 中,$c=3, \varepsilon_1=\varepsilon_2=1/e^2$,$m$=512).

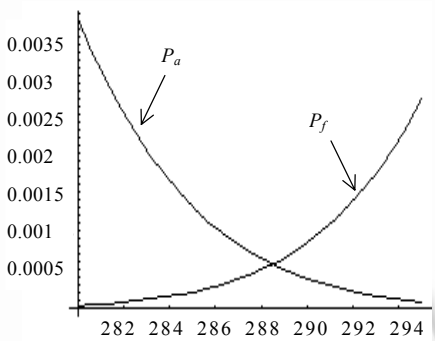

Fig.1 An example of P_a and P_f changing with m_{cri} in one block inversely

图 1 一个块中 P_a 和 P_f 随 m_{cri} 变化的例子

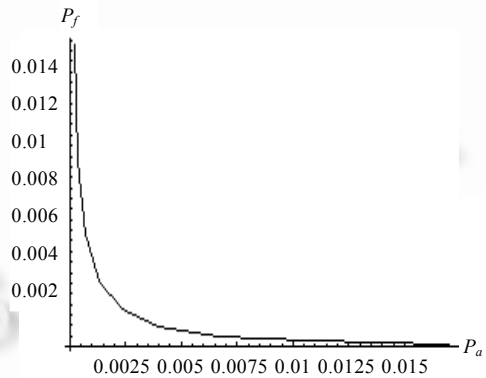

Fig.2 An example of P_a and P_f being related

图 2 P_a 和 P_f 间相互制约的例子

下面讨论 N_T 的选择.

因为用户的码字是随机二进制码字,所以我们可以认为各个块之间是独立的.同时假设合谋用户对整个拷贝的攻击方式是一致的(由于用户对嵌入的信息并不了解,这个假设是合理的).因此对于参与合谋的用户 B 而言,他的可判定块的个数服从二项分布 $B(l,(1-p_f))$,其均值是 $l(1-p_f)$.而对于无辜用户 B'来说,其可判定块的个数服从二项分布 $B(l,p_a)$,均值为 $l\times p_a$.当 p_a 和 p_f 都远远小于 $\frac{1}{2}$ 时,两者的区别非常明显,因此,也就比较容易取得 N_T 值.在表 1 中,我们给出在不同合谋尺寸及重复次数下,合谋用户与无辜用户可判定个数的对比.

关于码长 l: $l > \log_2^n$,其中 n 是用户个数.在我们的算法中,码长 l 对于跟踪算法的成功率影响并不是很大,当

然,在 p_a 和 p_f 一定的情况下,l 越大,无辜用户与合谋用户的差别越明显.

2.2 实验结果

我们取 $n=2^{20}$, $l=100$, $\varepsilon_1=\varepsilon_2=e^{-2}$ (实际上 p_a 和 p_f 比它们要小).我们考察不同合谋尺寸及不同重复次数情况下合谋用户与无辜用户可判定个数的差别.其中我们选择 m_{cri} 使得 p_a 与 p_f 尽量相等.在表 1 中,c 是合谋尺寸,第 1 行的 m 是重复嵌入次数.每一对数字中,左边的数字表示对合谋用户而言平均能够进行判定的比特个数,右边的数字表示对无辜用户而言平均能够判定的比特个数.由表 1 可见,随着所要求的合谋容忍尺寸的增加,要求码字的重复次数也要增加.在同样的合谋尺寸下,码字重复次数越多,合谋者与无辜用户的区分也就越明显.总的来说,在一定的合谋尺寸下,我们的跟踪算法能够对合谋用户与无辜用户进行有效区分.

Table 1 Comparison of determinable bits between collusive and innocent users under different collusive sizes and repetition times

表 1 不同合谋尺寸及不同重复次数下合谋用户与无辜用户可判定个数对比

c \ m	64	256	1 024	2 048	4 096
2	98 4	100 1	100 0	100 0	100 0
3	74 26	99 5	100 2	100 0	100 0
4	–	85 29	99 4	100 2	100 0
5	–	–	88 29	96 9	100 0
6	–	–	–	67 50	90 9

3 讨 论

(1) 本文从理论上给出了对某个具体块作判断时要求两类错误概率小于某特定值时的块长要求.此外,在特定块长下,通过调节判决门限的大小可以调节两类错误概率的大小.

(2) 第 2 节中的嵌入假设可以放宽.我们可以假设合谋用户不仅在可侦察位能够从他们的相应拷贝中任选,而且可以假设在任何位置允许用户以一定的概率将该位置置为不可读.在跟踪时,我们可以将不可读位置任意置为‘0’或‘1’.在这样的假设下,码长的增长也是可以接受的.例如,设合谋用户以 $\frac{1}{2}$ 的概率使码字比特不可读,码长只需增加因子 2.因此在合适的合谋尺寸下,本算法是切实可行的,并且具有很好的容错能力.

(3) 由于算法要求嵌入的重复次数足够大,因此本算法的嵌入数据量较大.考虑到鲁棒性,本文的算法适用于对数据量较大的数字产品进行保护的情况,如数字电影、游戏、音乐等,并且需要对该类拷贝的数据嵌入技术做深入研究.对于图像等数据量较小的拷贝,不推荐使用本文的方法.

(4) 在本算法中,发行商无须知道用户的码字.而在非对称数字指纹体制中,要求发行商不能知道用户的码字,因此本算法为非对称指纹体制的构造提供了一种备选算法.事实上,通过合理选择每个码字的重复次数及判决门限,发行商可以正确判定出大部分的码字.

(5) 随机数控制变反的思想也可以用于文献[1]中的算法.这种置乱方式优于文献[1]中算法的置换方式.如文献[1]中用户的码字的内码可能是‘11111111’,置换后对应的比特位仍全为‘1’,但若采用随机数控制变反方式,将有一半变为‘0’,因此有更好的置乱效果.

尽管本算法具有以上几个特点,但仍需指出本算法适用于合谋尺寸不是很大的情况.事实上,因为人们在无把握的情况下并不愿意与人合作,因此讨论一定合谋尺寸下的指纹编码算法是有意义的.此外,在 c 较小($c\leq 6$)的情况下,本算法优于同样参数下文献[1]中的算法,而且具有更好的容错特性.

4 结束语

本文提出了一种简洁、有效的二进制合谋容忍数字指纹编码算法.该算法中用户的码字可以不为发行商所知,因此有利于构造非对称数字指纹体制.此外,该算法提出的跟踪算法具有较低的错误概率.事实上,如果码长 l 选取得不是太小,而 ε_1 和 ε_2 又取得合适的话,合谋与非合谋用户的可判定个数是非常容易区别的.如何结合实际的攻击策略进一步将该编码算法进行优化并提高抗合谋尺寸,如何将其应用于非对称数字指纹体制的构造以及如何结合数字水印的嵌入技术,将该编码算法具体应用于多媒体数据的版权保护,都是值得我们进一步研究的方向.

References:

[1] Boneh D, Shaw J. Collusion-Secure fingerprinting for digital data. In: Coppersmith D, ed. Advances in Cryptology: Proceedings of the CRYPTO'95. Berlin: Springer-Verlag, 1995. 452~465.

[2] Liu ZH, Yin P. Techniques and Applications of Information Hiding. Beijing: Science Press, 2002. 178~180 (in Chinese).

[3] Guth J, Pfitzmann B. Error- and collusion-secure fingerprinting for digital data. In: Pfitzmann A, ed. Proceedings of the 3rd International Workshop on Information Hiding (IH'99). Berlin: Springer-Verlag, 2000. 134~145.

[4] Safavi-Naini R, Wang Y. Collusion secure q-ary fingerprinting for perceptual content. In: Sander T, ed. Security and Privacy in Digital Rights Management: Proceedings of the ACM Digital Rights Management Workshop. Berlin: Springer-Verlag, 2002. 57~75.

[5] Domingo-Ferrer J, Herrera-Joancomartí J. Simple collusion-secure fingerprinting schemes for images. In: Latifi S, ed. Proceedings of the International Symposium on Information Technology: Coding and Computing (ITCC 2000). Los Alamitos: IEEE Computer Society Press, 2000. 128~132.

[6] Löfvenberg J, Wiberg N. Random codes for digital fingerprinting. Technique Report, LiTH-ISY-R-2059, Department of Electrical Engineering, Linköping University, 2000. http://www.it.isy.liu.se/~jacob/texter/RandCodes/.

[7] Pfitzmann B, Schunter M. Asymmetric fingerprinting. In: Maurer UM, ed. Advances in Cryptology: Proceedings of the EUROCRYPT'96. Berlin: Springer-Verlag, 1996. 84~95.

[8] Alon N, Spencer J. The Probabilistic Method. New York: John Wiley & Sons, Inc., 1992. 234~240.

附中文参考文献:

[2] 刘振华,尹萍.信息隐藏技术及应用.北京:科学出版社,2002.178~180.

敬 告 作 者

《软件学报》创刊以来,蒙国内外学术界厚爱,收到许多高质量的稿件,其中不少在发表后读者反映良好,认为本刊保持了较高的学术水平.但也有一些稿件因不符合本刊的要求而未能通过审稿.为了帮助广大作者尽快地把他们的优秀研究成果发表在我刊上,特此列举一些审稿过程中经常遇到的问题,请作者投稿时尽量予以避免,以利大作的发表.

1. 读书偶有所得,即匆忙成文,未曾注意该领域或该研究课题国内外近年来的发展情况,不引用和不比较最近文献中的同类结果,有的甚至完全不列参考文献.

2. 做了一个软件系统,详尽描述该系统的各个方面,如像工作报告,但采用的基本上是成熟技术,未与国内外同类系统比较,没有指出该系统在技术上哪几点比别人先进,为什么先进.一般来说,技术上没有创新的软件系统是没有发表价值的.

3. 提出一个新的算法,认为该算法优越,但既未从数学上证明比现有的其他算法好(例如降低复杂性),也没有用实验数据来进行对比,难以令人信服.

4. 提出一个大型软件系统的总体设想,但很粗糙,而且还没有(哪怕是部分的)实现,很难证明该设想是现实的、可行的、先进的.

5. 介绍一个现有的软件开发方法,或一个现有软件产品的结构(非作者本人开发,往往是引进的,或公司产品),甚至某一软件的使用方法.本刊不登载高级科普文章,不支持在论文中引进广告色彩.

6. 提出对软件开发或软件产业的某种观点,泛泛而论,技术含量少.本刊目前暂不开办软件论坛,只发表学术文章,但也欢迎材料丰富,反映现代软件理论或技术发展,并含有作者精辟见解的某一领域的综述文章.

7. 介绍作者做的把软件技术应用于某个领域的工作,但其中软件技术含量太少,甚至微不足道,大部分内容是其他专业领域的技术细节,这类文章宜改投其他专业刊物.

8. 其主要内容已经在其他正式学术刊物上或在正式出版物中发表过的文章,一稿多投的文章,经退稿后未作本质修改换名重投的文章.

本刊热情欢迎国内外科技界对《软件学报》踊跃投稿.为了和大家一起办好本刊,特提出以上各点敬告作者.并且欢迎广大作者和读者对本刊的各个方面,尤其是对论文的质量多多提出批评建议.