第 36 卷 第 4 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.4 Computer Engineering February 2010
·安全技术· 文章编号：1000—3428(2010)04—0134—04 文献标识码：A 中图分类号：TP309

一种结合用户许可的多级安全策略模型

卢小亮，郁 滨
（解放军信息工程大学电子技术学院，郑州 450004）

摘 要：针对 BLP 模型存在“向上写”规则破坏数据完整性、主体分配权限过大及客体安全等级不变的问题，提出一种结合用户许可的多级安全策略模型。该模型利用可信度标识对主体写操作进行完整性保护，通过用户许可标识解决 BLP 模型和可信度标识存在的主体分配权限过大问题，结合系统管理员仲裁机制对修改的客体安全等级进行动态调整。理论分析表明，该模型能够保证系统的安全。

关键词：安全模型；可信度标识；用户许可

Multilevel Security Policy Model Combined with User Permission

LU Xiao-liang, YU Bin
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 Aiming at the problem that BLP model's access rule of "no write down" destroy data integrity, subject has most privilege and object holds constant security level, this paper presents a multilevel security policy model combined with user permission. In the model, trusted label is used in subject writing to protect object integrity. User permission solves the problem that subject privilege in BLP model and trusted label has more rights to steal data. By importing arbitration for system administrator, confidential label and trusted label for the modified objects is adjusted dynamically. Theory analysis indicates that the model can assure system security.

【Key words】 security model; trusted label; user permission

1 概述

保密性与完整性是安全模型的 2 个重要方面。BLP[1]模型是经典的多级安全策略模型，该模型主要解决了客体的保密性问题，能够防止敏感信息的泄漏，但存在一些不足。文献[2]指出 BLP 模型缺少对客体的完整性限制。

目前用于完整性保护的模型主要有 Biba 模型、Clark-Wilson 模型等。Biba 模型侧重保护客体的完整性，缺少对客体保密性的控制，是系统完整性保护的最常见模型。Clark-Wilson 模型是以良构事务为基础的模型，理论上较好地解决了完整性问题，但不易在实际系统中实现。因此，在实际系统的应用中，理想的选择是 Biba 模型。

为了保证信息的保密性同时确保信息的完整性，通常采用将 BLP 模型和 Biba 模型相结合的多策略模型。文献[3]通过形式化方法证明了该模型能保证系统的安全性；文献[4]指出该模型虽保护了客体的保密性和完整性，但信息的流动受到严格限制，降低了策略模型的可用性；文献[5]在此模型中引入主体的安全标记动态调整机制，提高了系统的可用性，但未考虑修改后客体的安全等级调整，存在修改后客体信息泄露的隐患。由于 BLP 模型和 Biba 模型都是基于格的安全策略模型，因此存在授权主体访问资源权力过大的问题，文献[6]指出主体的资源访问权力过大，破坏了最小权限原则。

针对上述问题，本文以保密性为前提，提出了一种结合用户许可的多级安全策略模型，并进行了形式化描述，给出了该模型的安全性质，分析了该模型的安全性。

2 结合用户许可的多级安全策略模型

2.1 基本思想

该安全模型以保密性为重点，针对 BLP 模型缺少完整性控制、不能控制“向上写”操作的缺陷，利用用户可信度标识对 BLP 模型中的写操作进行完整性保护。由于 BLP 模型是基于格的模型，因此与可信度标识都存在主体访问权限过大的问题，通过引入用户许可标识，对系统内信息进行严格控制，细化主体的访问权限，同时结合系统管理员仲裁机制，对系统内已修改客体的安全等级重新调整，从而保证客体的安全。

2.2 模型元素

模型为系统中的主体分配访问级别，为客体分配安全级别。主体访问级别主要包括保密性级别、可信度级别。客体安全级别主要包括保密性级别、可信度级别以及意愿值。模型中的保密性级别由保密级别和访问所属的范畴决定。其中，保密级别集合是全序的，即绝密>机密>秘密>无密级，可信度级别也是全序的，即最重要>很重要>重要>公开。通过可信度级别能够反映主体和客体的完整性等级。

2.3 模型定义

定义 1 S 表示主体集合，$S_T \subseteq S$ 表示可信主体集合，$S' = S - S_T$ 表示非可信主体；O 表示客体集合；C 表示密级集合；K 表示部门范畴的集合；L 表示安全级集合。

定义 2 $A = \{r, w, a, e\}$ 表示访问属性；r 表示只读；w 表示读写；a 表示追加写；e 表示执行(不可读不可写)；R 表示请求集合；$D = \{\text{yes,no,error,?}\}$ 表示判定结果，?表示不能处理此请求；ρ 表示进行判定规则；v 表示状态；$W = \{\rho_1, \rho_2, \cdots, \rho_s\}$ 表示一组规则集。

定义 3 客体许可值表示客体的访问是否需要获得用户

作者简介：卢小亮(1984－)，男，硕士研究生，主研方向：信息安全，蓝牙技术；郁 滨，教授、博士生导师
收稿日期：2009-08-24 **E-mail：**lxlzl151@163.com

的操作许可，用于表示在同一类具有相同保密级别和可信度的客体中相对某一方面的重要性，用 $f_{cmp}(o)$ 表示，值域 $P=\{0,1\}$。其中，0 表示在主体访问客体时不需要征得用户许可；1 表示需要征得用户许可。

定义 4 当客体的许可值为 1 时，主体对客体的访问需要征得用户的操作许可用 $permit(s_i,o_j,x)$ 函数表示，值域也为 $\{0,1\}$。其中，0 表示用户未授权主体 s_i 以模式 x 访问客体 o_j；1 表示用户授权 s_i 以模式 x 访问客体 o_j。

定义 5 $V=B\times\boldsymbol{M}\times F\times H$ 表示系统状态集合，某一时刻的状态 $v\in V$ 由 $(b,\boldsymbol{M},f,H)$ 表示。其中，$b\subseteq(S\times O\times A\times P)$ 表示在某个特定的状态下哪些主体得到用户许可以何种模式访问哪些客体；$\boldsymbol{M}$ 表示访问矩阵；$F\subseteq L_S\times L_O\times L_C\times L_{CI}\times L_{OI}\times L_{cmp}$ 表示访问类函数；对于任意一个元素 $f\in(f_s,f_o,f_c,f_{ci},f_{oi},f_{cmp})$，$f_s$ 表示主体的最大保密等级，f_c 表示主体的当前保密等级，f_o 表示客体的保密等级，f_{ci} 表示主体的可信度等级，f_{oi} 表示客体的可信度等级，f_{cmp} 表示客体的意愿值，H 表示当前客体的层次关系。

系统任一时刻的状态 $v=(b,\boldsymbol{M},f,H)\in V$，其中，$b$ 表示当前访问的集合：

$$b(s:x_i\vee x_j)=\{o\mid o\in O\&\&((s,o,x_i)\in b\,\|\,(s,o,x_j)\in b)\}$$

公理1 用户许可特性：状态 $v=(b,\boldsymbol{M},f,H)$ 满足用户许可特性：

$$\text{iff }\forall(s,o,x,p)\Rightarrow$$
$$((f_{cmp}(o)=1\&\&permit(s,o,x)=1)\,\|\,f_{cmp}(o)=0)$$

公理 2 简单安全特性(ss-特性)：状态 $v=(b,\boldsymbol{M},f,H)$ 满足简单安全特性：

$$\text{iff } o\in b(s:x)\&\&x\in\{r,w\}\Rightarrow(f_s(s)>f_o(o))\&\&$$
$$((f_{cmp}(o)=1\&\&permit(s,o,x)=1)\,\|\,f_{cmp}(o)=0)$$

该特性表明：仅当主体的保密级别支配客体的保密级别同时符合用户许可时，主体才具有对该客体的“读”或“写”访问权限。

公理 3 星号安全特性(*-特性)：状态 $v=(b,\boldsymbol{M},f,H)$ 满足*-特性：iff$\forall s\in S'$，则有：

(1) $\forall o\in b(s:r,e)\Rightarrow(f_o(o)<f_c(s))\&\&$
$$((f_{cmp}(o)=1\&\&permit(s,o,x)=1)\,\|\,f_{cmp}(o)=0)$$

(2) $\forall o\in b(s:w)\Rightarrow(f_o(o)=f_c(s))\&\&$
$$((f_{cmp}(o)=1\&\&permit(s,o,x)=1)\,\|\,f_{cmp}(o)=0)$$

(3) $\forall o\in b(s:a)\Rightarrow(f_o(o)>f_c(s))\&\&(f_{ci}(s)>f_{oi}(o))\&\&$
$$((f_{cmp}(o)=1\&\&permit(s,o,x)=1)\,\|\,f_{cmp}(o)=0)$$

该特性表明：

(1)当主体对客体进行“读”或“执行”操作时，仅当该主体的保密级别支配客体的保密级别同时需要获取用户许可。

(2)当主体对客体进行“读写”操作时，仅当该主体的保密级别等于客体的保密级别同时需要获取用户许可。

(3)当主体对客体进行“追加写”操作时，仅当该主体的保密级别小于客体的保密级别同时主体的可信度级别大于客体的可信度级别且需获取用户许可。

公理 4 自主安全特性(ds-特性)：状态 $v=(b,M,f,H)$ 满足 ds-特性：

$$\text{iff }(s_i,o_j,x)\in b\Rightarrow(x\in m_{ij})\&\&$$
$$((f_{cmp}(o)=1\&\&permit(s,o,x)=1)\,\|\,f_{cmp}(o)=0)$$

该特性表明：主体以某种访问权限访问客体时，不但要符合自主访问矩阵的要求，也要满足用户许可。

定义 6 当主体完成对客体的“写”(包括“追加写”和“读写”)操作，系统管理员判断所写入内容的安全等级，其中，f_o' 表示系统管理员为写入内容设置的保密等级；f_{oi}' 表示系统管理员为写入内容设置的可信度等级。该安全等级可以人为决定，也可由专门的系统仲裁机制设定。

定义 7 当主体完成对客体的“写”(包括“追加写”和“读写”)操作后，用 f_o'' 表示客体新的保密等级，用 f_{oi}'' 表示客体新的可信度等级，访问后客体新的安全等级分别为

$$f_o''=\begin{cases}f_o' & f_o'\geq f_o\\ f_o & f_o'<f_o\end{cases}\qquad f_{oi}''=\begin{cases}f_{oi}' & f_{oi}'\geq f_{oi}\\ f_{oi} & f_{oi}'<f_{oi}\end{cases}$$

定义 8 状态 $v=(b,M,f,H)$ 是安全状态，则 v 同时满足用户许可特性、ss-特性、*-特性和 ds-特性；状态序列 Z 是安全状态序列，iff 对于$\forall t\in T\Rightarrow v\in Z$ 都是安全状态。

定义 9 系统 $\sum(R,D,W,Z_0)$ 是一个安全系统，则系统中的 $\forall z_i(i\in[0,n])$ 都是安全状态。

2.4 状态转换

系统状态间的转换由一组操作规则定义，一个规则是一个函数，它为每个状态和请求说明下一个状态和判断。结合定义 2，其规则函数可表示为

$$\rho:R\times V\to D\times V$$

定义 v 和 v^* 表示 2 个相邻的状态对；v 为前状态；v^* 为后续状态；f 为前状态的访问类函数；f^* 为后续状态的访问类函数。其中，$R\times V$ 表示系统的所有请求与当前状态 $v(v\in V)$ 的集合；$D\times V$ 表示系统对所有请求的判断与状态 $v^*(v^*\in V)$ 的集合。

规则 ρ 保持系统安全状态，iff 所有的 $\rho(R_k,v)=(D_m,v^*)$，均有 v 是安全状态$\Rightarrow v^*$ 也是安全状态。模型定义了一组必须满足的规则集合来保证系统的安全，一个系统的状态是安全的当且仅当满足这些安全规则，按照模型给出的 4 条公理，本文给出主体对客体的只读、执行、读写、追加写这 4 种访问请求的安全状态转换规则，具体描述如下：

定义 10 $dom(R_i)$ 表示规则 R_i 的定义域，用于判断访问请求是否在 R_i 规则的范围内。

规则 1(R_1)：主体 s_i 对客体 o_j 请求只读访问：

$$R_1(R_k,v)=\begin{cases}(?,v) & R_k\notin dom(R_1)\\ (\text{yes},(b\cup(s_i,o_j,r,1),\boldsymbol{M},f,H)) & R_k\in dom(R_1)\text{且满足条件(1)}\\ (\text{no},v) & \text{其他}\end{cases}$$

满足只读访问的条件(1)：

$$[r\in M_{ij}]\&\&[f_s(s_i)>f_o(o_j)]\&\&[f_c(s_i)>f_o(o_j)]\&\&$$
$$[((f_{cmp}(o_j)=1\&\&permit(s_i,o_j,r)=1)\,\|\,f_{cmp}(o_j)=0)]$$

该规则表明：当主体 s_i 的访问属性中存在对客体 o_j 的“读”权限、主体的当前保密等级高于客体的保密等级、且主体的最大保密级别高于客体的保密等级同时需要系统使用

者许可的客体已得到允许时，主体 s_i 才能对客体 o_j 进行读访问。

主体 s_i 完成对客体 o_j 的读访问后，主客体的安全等级保持不变。

规则 2(R_2)：主体 s_i 对客体 o_j 请求执行访问：

$$R_2(R_k,v)=\begin{cases}(?,v) & R_k\notin dom(R_2)\\ \left(\text{yes},\left(b\cup(s_i,o_j,r,1),\boldsymbol{M},f,H\right)\right) & R_k\in dom(R_2)\text{且满足条件(2)}\\ (\text{no},v) & \text{其他}\end{cases}$$

满足执行访问的条件(2)：

$$\left[e\in M_{ij}\right]\&\&\left[f_c(s_i)>f_o(o_j)\right]\&\&\left[\left(\left(f_{cmp}(o_j)=1\&\&permit(s_i,o_j,e)=1\right)\|\ f_{cmp}(o_j)=0\right)\right]$$

该规则表明：当主体 s_i 的访问属性中存在对客体 o_j 的“执行”权限、主体的当前保密等级高于客体的保密等级同时需要系统使用者许可的客体已得到允许时，主体 s_i 才可以对客体 o_j 进行执行访问。主体 s_i 完成对客体 o_j 的执行访问后，主客体的安全等级保持不变。

规则 3(R_3)：主体 s_i 对客体 o_j 请求读写访问：

$$R_3(R_k,v)=\begin{cases}(?,v) & R_k\notin dom(R_3)\\ \left(\text{yes},\left(b\cup(s_i,o_j,r,1),\boldsymbol{M},f,H\right)\right) & R_k\in dom(R_3)\text{且满足条件(3)}\\ (\text{no},v) & \text{其他}\end{cases}$$

满足读写访问的条件(3)：

$$\left[w\in M_{ij}\right]\&\&\left[f_s(s_i)>f_o(o_j)\right]\&\&\left[f_c(s_i)=f_o(o_j)\right]\&\&\left[\left(\left(f_{cmp}(o_j)=1\&\&permit(s_i,o_j,w)=1\right)\|\ f_{cmp}(o_j)=0\right)\right]$$

访问函数 f^* 表示为

$$f^*=\left(f_s,f_o^{''},f_c,f_{ci},f_{oi}^{''},f_{cmp}\right)$$

该规则表明：当主体 s_i 的访问属性中存在对客体 o_j 的“读写”权限、主体的当前保密等级等于客体的保密等级、且主体的最大保密级别高于客体的保密等级同时需要系统使用者许可的客体已得到允许时，主体 s_i 才能对客体 o_j 进行读写访问。

主体 s_i 完成对客体 o_j 的读写访问后，主体的安全等级不变，而客体的安全等级随着主体写入的内容而调整。写入的内容依据系统管理员仲裁机制来决定其安全等级，若该安全等级低于原有客体的安全等级，则已修改客体的安全等级保持不变，若该安全等级高于原有客体的安全等级，则已修改客体的安全等级调整为写入内容的安全等级。

规则 4(R_4)：主体 s_i 对客体 o_j 请求追加写访问：

$$R_4(R_k,v)=\begin{cases}(?,v) & R_k\notin dom(R_4)\\ \left(\text{yes},\left(b\cup(s_i,o_j,r,1),\boldsymbol{M},f,H\right)\right) & R_k\in dom(R_4)\text{且满足条件(4)}\\ (\text{no},v) & \text{其他}\end{cases}$$

满足追加写访问的条件(4)：

$$\left[r\in M_{ij}\right]\&\&\left[f_o(o_j)>f_c(s_i)\right]\&\&\left[f_{ci}(s_i)>f_{oi}(o_j)\right]\&\&\left[\left(\left(f_{cmp}(o_j)=1\&\&permit(s_i,o_j,a)=1\right)\|\ f_{cmp}(o_j)=0\right)\right]$$

访问函数 f^* 表示为

$$f^*=\left(f_s,f_o^{''},f_c,f_{ci},f_{oi}^{''},f_{cmp}\right)$$

该规则表明：当主体 s_i 的访问属性中存在对客体 o_j 的“追加写”权限、主体的当前保密等级低于客体的保密等级、且主体的可信度等级高于客体的可信度等级同时需要系统使用者许可的客体已得到允许时，主体 s_i 才可以对客体 o_j 进行追加写访问。

主体 s_i 完成对客体 o_j 的追加写访问后，主体的安全等级不变，而客体的安全等级随着主体写入的内容而调整。写入的内容依据系统管理员仲裁机制决定其安全等级，若该安全等级低于原有客体的安全等级，则已修改客体的安全等级保持不变，若该安全等级高于原有客体的安全等级，则已修改客体的安全等级调整为写入内容的安全等级。

3 模型的性质

定义11 $f_o(v,o)$ 表示状态 v 下客体 o 的保密等级，$f_{oi}(v,o)$ 表示状态 v 下客体 o 的可信度等级，$v_1\prec v_2$ 表示状态 v_1 可以转换到状态 v_2，$v_1\to v_2$ 表示 v_1 和 v_2 为相邻状态且 v_2 是 v_1 的后续状态。

定理 1 重要客体的访问是安全的。

证明：设重要客体集合为 O_{im}，$O_{im}=\{o\mid f_{cmp}(o)=1\}$，则 $\forall o\in O_{im},\forall s\in S',\forall a\in A$。

由公理 1 可知：$f_{cmp}(o)=1$ 既保护了保密性要求高的客体，也保护了可信度要求高的客体，实现了从保密性和可信度 2 个维度上对客体安全性的保护。

如果 $permit(s,o,a)=1$，则表示系统管理主体允许访问主体 s 以 a 方式访问客体 o，同时还需结合保密等级和可信度标识决定主体是否访问该客体。

如果 $permit(s,o,a)=0$，则表示系统管理主体不授权于访问主体 s 以 a 方式访问客体 o，保护了重要客体的安全。

定理 2 客体的当前状态保密等级随状态可达性是不减的。

设 $o\in O$，$v,v'\in V$，$v\prec v'$，需要证明 $v\to v'$ 时，$f_o(v',o)\geq f_o(v,o)$。

证明：先证明当 $v\to v'$ 成立时，$f_o(v',o)\geq f_o(v,o)$ 成立。

若从状态 v 转换到状态 v' 主体进行“读”或“执行”操作时，则由规则 1 或规则 2 可知：$f_o(v',o)\geq f_o(v,o)$。

若从状态 v 转换到状态 v' 主体进行“读写”或“追加写”操作时，则由规则 3 或规则 4 可知：$f_o(v',o)\geq f_o(v,o)$。

由此可见，任何状态 v 到状态 v' 的转换，都有 $f_o(v',o)\geq f_o(v,o)$。

如果 $v\to v'$ 不成立，则存在 $v_1,v_2,\cdots,v_k$ 使得 $v\to v_1$，$v_i\to v_{i+1}(1\leq i\leq k-1)$，$v_k\to v'$ 根据 $v\to v'$ 时证明的结论可知：$f_o(v_1,o)\geq f_o(v,o)$，$f_o(v',o)\geq f_o(v_k,o)$，$f_o(v_{i+1},o)\geq f_o(v_i,o)(1\leq i\leq k-1)$，同样可以得到 $f_o(v',o)\geq f_o(v,o)$。因此，对于任何 $v,v'\in V$，当 $v\prec v'$ 时，都有 $f_o(v',o)\geq f_o(v,o)$。

定理 3 客体的可信度等级随状态可达性是不减的。

设 $s\in S'$，$o\in O$，$v,v'\in V$，$v\prec v'$，需要证明 $v\to v'$ 时，$f_{oi}(v',o)\geq f_{oi}(v,o)$。

证明方法与定理 2 类似，此处不再详细说明。

4 模型安全性

定义 12 $b_v(s:x_1\vee x_2)$，其中，$x_1,x_2\in A$ 表示在状态 v 下主体 s 以 x_1 或 x_2 方式访问客体 o。

如果系统能够保证其保密性，则要求在系统中信息不能从高保密等级的客体流向低保密等级的客体，防止敏感信息的泄露。

设 $s\in S^{'},o_1,o_2\in O,v,v^{'}\in V,v\prec v^{'}$，需证明：在状态 v 和 $v^{'}$ 下，分别有 $o_1\in b_v(s:r\vee w),o_2\in b_{v^{'}}(s:a\vee w)$，则 $f_o(v,o_1)\le f_o(v^{'},o_2)$。

证明：由 $o_1\in b_v(s:r\vee w)$ 可知，必有主体 s 在状态 v 下依据规则 1 或规则 3 获取对客体 o_1 的“读”或“读写”授权。

由规则 1 和规则 3 可知，在状态 v 下式(1)恒成立。

$$f_c(s)\ge f_o(v,o_1) \tag{1}$$

由 $o_2\in b_{v^{'}}(s:a\vee w)$ 可知，必有 $v^{'}$ 之前的某一状态 v_3，主体 s 在状态 v_3 下依据规则 3 或规则 4 获取对客体 o_2 的“读写”或“追加写”授权。

由规则 3 和规则 4 可知，在状态 v_3 下式(2)恒成立。

$$f_c(s)\le f_o(v_3,o_2) \tag{2}$$

由于 $v_3\prec v^{'}$，因此由定理 2 可知：

$$f_o(v_3,o_2)\le f_o(v^{'},o_2) \tag{3}$$

若 $v_3\prec v$，说明主体先写客体 o_2 再读客体 o_1，不存在客体 o_1 与客体 o_2 之间的信息传递，不影响系统的安全。

若 $v\prec v_3$，依据式(1)~式(3)可知：

$$f_o(v,o_1)\le f_o(v^{'},o_2)$$

得证，该模型能够保证系统的保密性。

由于模型只在写操作中通过可信度标识实现对客体的完整性，能够确保高可信度的主体向低可信度的客体写入信息，因此在写操作中系统能够确保客体的完整性。

得证：该模型以保密性为前提能够同时保证客体的完整性。

5 结束语

本文分析了 BLP 模型存在的安全缺陷，提出了一种结合用户许可的多级安全策略模型，描述了模型中主体的访问不仅满足 BLP 模型的规则，还要得到可信度标识和用户许可标识的约束，并对已修改客体的安全等级进行调整。该模型以保密性为前提，既防止了系统内客体的泄露，又控制了系统内客体的非授权篡改，保证了系统的安全。下一步将主要针对该模型在文件等资源中的具体应用进行研究。

参考文献

[1] Bell D, Lapadula L J. Secure Computer System: Unified Exposition and Multics Interpretation[M]. Massachusetts, USA: MITRE Corporation, 1976.

[2] 谷千军, 王　越. BLP 模型的安全性分析与研究[J]. 计算机工程, 2006, 32(22): 157-159.

[3] 周　正, 刘　毅, 沈昌祥. 一种新的保密性与完整性统一安全策略[J]. 计算机工程与应用, 2007, 43(34): 1-4.

[4] 黄　强, 沈昌祥. 基于可信计算的保密和完整性统一安全策略[J]. 计算机工程与应用, 2006, 42(10): 15-18.

[5] 张　俊, 周　正, 李　建, 等. 基于 MLS 策略的机密性和完整性动态统一模型[J]. 计算机工程与应用, 2008, 44(12): 35-37.

[6] 曹四化, 何鸿君. 基于用户意愿的改进 BLP 模型 IB_BLP[J]. 计算机工程, 2006, 32(23): 171-173.

编辑　张正兴

(上接第 133 页)

另外，如果测试中判断某含密音频含有秘密信息，算法能同时给出含密音频嵌入的 PN 序列长度，实验结果表明，算法给出的 PN 序列长度与含密音频实际嵌入的 PN 序列长度完全符合。

由表 1 实验结果可知，对于含密音频的检测，含密音频中 PN 序列嵌入强度越大，检测的正确率越高。在嵌入强度只有 0.002 时，本文算法的检测正确率已超过 80%。

5 结束语

本文提出的基于小波去噪和小波突变点检测技术的扩频音频掩密分析算法具有以下优点：

(1)算法性能不受秘密信息嵌入容量影响，只要秘密信息被连续地嵌入到一段音频之中，并且具有一定的嵌入强度，本算法就能检测出来。

(2)该算法不但对 PN 序列低嵌入强度的扩频含密音频具有良好的检测正确率，而且能确定嵌入的 PN 序列长度。

另外，虽然该算法主要是针对音频信号的，但是从原理上同样适用于检测经过扩频掩密的图像数据。算法的不足之处在于只能检测扩频类掩密算法，下一步将重点研究通用型掩密分析算法。

参考文献

[1] Özer H, Sankur B, Memon N, et al. Detection of Audio Covert Channels Using Statistical Footprints of Hidden Messages[J]. IEEE Trans. on Signal Processing, 2006, 16(4): 389-401.

[2] Ru Xuemin, Zhang Hongjuan, Huang Xiao. Steganalysis of Audio: Attacking the Steghide[C]//Proceedings of the 4th International Conference on Machine Learning and Cybernetics. Guangzhou, China: [s. n.], 2005: 3937-3942.

[3] Tavakoli E, Vahdat B V, et al. Audio Watermarking for Covert Communication Through Telephone System[C]//Proc. of IEEE International Symposium on Signal Processing and Information Technology. Vancouver, Canada: IEEE Press, 2006: 955-959.

[4] Garcia J, Nakano M, Perez H. Real-time MCLT Audio Watermarking and Comparison of Several Whitening Methods in Receptor Side[C]//Proceedings of the 8th IEEE International Symposium on Multimedia. San Diego, USA: IEEE Press, 2006: 991-997.

编辑　张正兴