

参数化系统二维抽象的理论基础

庞征斌 屈婉霞 郭 阳 杨晓东

(国防科学技术大学计算机学院 长沙 410073)

摘要 模型之间的等价关系和抽象模型的性质保持是保证验证正确的必要条件,参数化系统二维抽象从构成系统状态空间的二维方向分别进行抽象,证明了此抽象方法的正确性和合理性,即 TDA 模型与原始模型存在模拟关系,而且在 TDA 模型中成立的只对单个变量进行全称量化的单索引 ACTL* 公式,在任意规模的原始模型中也成立,为简化参数化系统验证提供了理论依据。

关键词 参数化系统验证,二维抽象,模拟,性质保持

中图法分类号 TP391.72 **文献标识码** A

Two-dimension Abstraction Theory for Parameterized System

PANG Zheng-bin QU Wan-xia GUO Yang YANG Xiao-dong

(College of Computer, National University of Defense Technology, Changsha 410073, China)

Abstract In order to preserve interesting properties of a system under consideration during verification, it is necessary to establish an equivalent relation between models. Two-dimension abstraction for parameterized system, where the size of the state transition graph for individual process is decreased independently at first, and the whole system composed of reduced processes is then abstracted based on the design principle of parameterized systems, thus avoiding the construction of the complete state space that might be too big to fit into memory. The paper gave the correctness and soundness proofs of two-dimension abstraction. It was shown that simulation relation exists between TDA model and concrete model, and TDA model is weak preserved with respect to ACTL* formula. Importantly, a single-indexed ACTL* formula satisfied by TDA model, is also satisfied by concrete models with arbitrary replicated (and a constant number of non-replicated) processes. This work lays the theoretical basis for simplifying parameterized system verification.

Keywords Parameterized system verification, Two-dimension abstraction, Simulation, Property preservation

1 引言

参数化系统由一组结构相同、协同运行的进程组成,这类具有重复结构的系统如通信协议、互斥协议和 Cache 一致性协议等在现实中普遍存在。并发进程本身的复杂性和进程数目的任意性导致系统状态空间规模激增,如何高效验证参数化系统成为当前验证领域面临的挑战性难题。

抽象^[1,2]是缓解状态空间爆炸最有效的手段之一,已有的参数化系统抽象研究^[3-6]对进程或进程间的交互方式增加若干约束以简化问题,无法处理现实中大量存在的进程行为非常复杂的系统。参数化系统二维抽象(TDA-Two-dimension Abstraction)框架和方法^[7]对进程状态空间是否有限、进程间的交互方式均无严格限制甚至允许包含常数个不同构的进程,这些问题通过分解-抽象-组合-再抽象,可最大限度地降低其复杂度。

本文简要介绍二维抽象的相关概念,然后给出抽象模型必须满足的条件,最后从理论上证明 TDA 模型与原始模型存在模拟关系,而且在 TDA 模型中成立的性质在包含任意

多个进程的原始模型中均成立,这也是参数化系统验证需要解决的最根本的问题。

2 二维抽象相关概念

二维抽象的研究对象是具有真并发语义的异步并发参数化系统,系统模型通过进程间的真并发异步合成运算 $\parallel$ 建立。若用 x 轴表示系统包含的进程数 n (为便于讨论,假定所有进程结构完全相同), y 轴表示单个进程的状态数 m (进程状态称为局部状态),连接 n 个局部状态的 n 维向量 $(s_1, s_2, \dots, s_n)$ 表示一个全局状态,其中, s_i ($1 \leq i \leq n$) 的值域为 m ,则全局状态数目最大可达 m^n 。

二维抽象对 m 和 n 构成的二维空间进行处理,一方面沿 Y 方向对单个进程的状态空间进行压缩,过滤与待验证的系统性质无关的信息。另一方面从参数化系统的设计思想中得到启发,在 X 方向设法用有限状态描述无限状态,进一步压缩系统状态空间。

定义 1 (Y-抽象与 Y-抽象模型) 在二维抽象框架中,对单个进程的状态空间独立进行压缩以减小 m 的过程,称为 Y-

到稿日期:2010-05-28 返修日期:2010-10-09 本文受国家自然科学基金项目(60773025,61070036)资助。

庞征斌(1972-),男,博士,副研究员,CCF 会员,主要研究方向为高性能计算机系统结构,E-mail:zbpang@163.com;屈婉霞(1972-),女,博士,副研究员,CCF 会员,主要研究方向为计算机系统结构、可靠性设计、集成电路功能验证;郭 阳(1971-),男,博士,研究员,CCF 高级会员,主要研究方向为微处理器设计与验证技术;杨晓东(1936-),男,博士生导师,主要研究方向为计算机系统结构、性能评价、可靠性理论。

抽象。原始模型经过 Y-抽象后得到的模型,称为 Y-抽象模型。

任何性质保持的方法都可用于 Y-抽象过程,我们采用标准的谓词抽象方法。谓词在原始模型的状态空间上定义一个等价关系,通过状态集合之间的映射,把一个大范围的或者包含无穷多个状态的原始模型转换成一个易于处理的、包含有限状态的抽象模型。

定义 2(X-抽象和 TDA 模型) 在二维抽象框架中,用有限状态描述无限状态、隐藏系统进程数 n 的过程,称为 X-抽象。Y-抽象模型经过 X-抽象后得到的模型,称为 TDA 模型。

设计人员在设计参数化系统时,通常以一个进程为主并保存其足够详细的信息,然后考虑与其它进程的交互,以此简化设计过程。我们称主进程为 *hub*,其它进程为 *rim*。

本文用 Kripke 结构 $M=(AP, S, I, R, L)$ 描述系统(包括进程), $PS^s(n)$ 表示进程 $M_k (1 \leq k \leq n)$ 组成的异步并发参数化系统的原始模型, $PS^y(n)$ 表示对 $PS^s(n)$ 进行 Y-抽象后得到的模型,是 n 个 Y-抽象模型 $M_k^y (1 \leq k \leq n)$ 的真并发异步合成, $PS^x(n)$ 表示对 $PS^y(n)$ 进行 X-抽象后得到的 TDA 模型。

3 性质保持与模型等价

为了保证验证的正确性,抽象模型必须是性质保持的。

定义 3(性质保持, Property Preservation) 如果抽象模型满足某一性质,则原始模型也满足该性质。性质保持可进一步分为强保持和弱保持。

定义 4(强保持, Strong Preservation) 抽象模型关于一个性质是强保持的,若性质在抽象模型中为真,当且仅当该性质在原始模型中也为真。

定义 5(弱保持, Weak Preservation) 抽象模型关于一个性质是弱保持的,若性质在抽象模型中为真,那么该性质在原始模型中也为真。反之则不成立。性质的弱保持能够极大地降低抽象模型对空间的需求。

本文考虑 ACTL* 公式描述的系统性质。ACTL* 是将计算树逻辑(CTL*-Computation Tree Logic)公式的路径量词限制为路径量词 A(for all computation paths)得到的子逻辑,计算树逻辑结合了线性时间和分支时间操作,假设系统在每个状态上具有特定的性质,路径量词 A 表示从该状态出发的所有路径具备某些性质。

要使抽象模型能够保证性质的真伪,就需要在抽象模型和原始模型之间建立一种等价关系。互模拟和模拟是最常用的两种等价关系。

定义 6(互模拟, Bisimulation) $M_1=(AP, S_1, I_1, R_1, L_1)$ 和 $M_2=(AP, S_2, I_2, R_2, L_2)$ 是 AP 上的两个 Kripke 结构,二元关系 $B \subseteq S_1 \times S_2$ 是 M_1 和 M_2 之间的一个互模拟关系,当且仅当对所有的 $s_1 \in S_1$ 和 $s_2 \in S_2$,如果 $B(s_1, s_2)$,则以下条件成立:

- 1) $L_1(s_1) = L_2(s_2)$;
- 2) 对于 $\forall t_1 \in S_1, R_1(s_1, t_1) \rightarrow \exists t_2 \in S_2, R_2(s_2, t_2) \wedge B(t_1, t_2)$;
- 3) 对于 $\forall t_2 \in S_2, R_2(s_2, t_2) \rightarrow \exists t_1 \in S_1, R_1(s_1, t_1) \wedge B(t_1, t_2)$ 。

如果存在一个互模拟关系 B ,使得对于 M_1 中的每一个初始状态 $s_{10} \in I_1$,在 M_2 中都存在一个初始状态 $s_{20} \in I_2$ 满足 $B(s_{10}, s_{20})$,而且对于 M_2 中的每一个初始状态 $s_{20} \in I_2$,在 M_1

中都存在一个初始状态 $s_{10} \in I_1$ 满足 $B(s_{10}, s_{20})$,则称 M_1 与 M_2 互模拟等价,记做 $M_1 \equiv M_2$ 。

定义 7(模拟, Simulation) $M_1=(AP_1, S_1, I_1, R_1, L_1)$ 和 $M_2=(AP_2, S_2, I_2, R_2, L_2)$ 是两个 Kripke 结构,其中, $AP_2 \subseteq AP_1$,二元关系 $H \subseteq S_1 \times S_2$ 是 M_1 和 M_2 之间的一个模拟关系,当且仅当对于所有的 $s_1 \in S_1$ 和 $s_2 \in S_2$,如果 $H(s_1, s_2)$,则以下条件成立:

- 1) $L_1(s_1) \cap AP_2 = L_2(s_2)$;
- 2) 对于 $\forall t_1 \in S_1, R_1(s_1, t_1) \rightarrow \exists t_2 \in S_2, R_2(s_2, t_2) \wedge H(t_1, t_2)$ 。

如果存在一个模拟关系 H ,使得对于 M_1 中的每一个初始状态 $s_{10} \in I_1$,在 M_2 中都存在一个初始状态 $s_{20} \in I_2$ 满足 $H(s_{10}, s_{20})$,则称 M_2 模拟 M_1 ,记做 $M_1 \leq M_2$ 。

互模拟具有自反性、对称性和传递性,是模型之间的一种等价关系,而模拟关系只具有自反性和传递性,并不是真正意义上的等价关系,只是模型之间的一种偏序关系,它通过限制逻辑以及放松结构必须满足恰好相同的公式集的要求,有可能获得较大的状态缩减,而且通过模拟关系建立的抽象模型是弱保持的,因此在实际中比互模拟应用得更多。

4 TDA 的正确性与合理性

TDA 的正确性是指 TDA 模型相对原始模型关于单索引 ACTL* 公式弱保持,因此在 TDA 模型中成立的单索引 ACTL* 公式在原始模型中一定成立。TDA 的合理性是指在 TDA 模型中成立的单索引 ACTL* 公式,在任意规模的原始模型中也成立,这一点从根本上减少了参数化系统验证工作的工作量,为提高验证效率提供了理论依据。定理 1、定理 2、定理 3 保证了 TDA 的正确性和合理性。

定理 1 异步合成运算 $\parallel_a$ 关于 $\leq$ 单调,即: $M_k \leq M_k^y (1 \leq k \leq n) \Rightarrow PS^s(n) \leq PS^y(n)$ 。

证明: n 个进程组成的异步并发参数化系统的原始模型为 $PS^s(n) = (AP^s, S^s, I^s, R^s, L^s) = \parallel_{k=1}^n M_k$, 其中, $M_k = (AP_k^s, S_k^s, I_k^s, R_k^s, L_k^s)$ 。 $PS^s(n)$ 经过 Y-抽象后的模型为 $PS^y(n) = (AP^y, S^y, I^y, R^y, L^y) = \parallel_{k=1}^n M_k^y$, 其中, $M_k^y = (AP_k^y, S_k^y, I_k^y, R_k^y, L_k^y)$ 。

根据定义 1 有 $M_k \leq M_k^y$, 则 $AP_k^y \subseteq AP_k^s$, 由异步合成的定义可得:

$$AP^y = \bigcup_{k=1}^n AP_k^y \subseteq \bigcup_{k=1}^n AP_k^s = AP^s \quad (1)$$

抽象算子 H_k^y 是 S_k^s 与 S_k^y 之间的一个模拟关系: $H_k^y(S_k^s) = S_k^y$, 因此, 对于 $\forall s^y \in S^y$, 下列等式成立:

$$\begin{aligned} s^y &= \langle s_{1a}^y, s_{2b}^y, \dots, s_{kl}^y, \dots, s_{ng}^y \rangle \\ &= \langle H_1^y(s_{1a}^s), H_2^y(s_{2b}^s), \dots, H_k^y(s_{kl}^s), \dots, H_n^y(s_{ng}^s) \rangle \quad (2) \end{aligned}$$

即原始状态空间 S^s 与抽象状态空间 S^y 之间的二元关系 $H^y \subseteq S^s \times S^y$ 的含义是“对状态 s^s 中的每一个分量分别同时运用抽象算子 $H_k^y (1 \leq k \leq n)$ ”。

下面证明 $H^y \subseteq S^s \times S^y$ 是 $PS^s(n)$ 与 $PS^y(n)$ 之间的一个模拟关系。设任意的原始状态 $s^s = \langle s_{1a}^s, s_{2b}^s, \dots, s_{kl}^s, \dots, s_{ng}^s \rangle \in S^s$, 经过 Y-抽象后的状态向量为 $s^y = \langle s_{1a}^y, s_{2b}^y, \dots, s_{kl}^y, \dots, s_{ng}^y \rangle \in S^y$, 即 $H^y(s^s) = s^y$, 根据定义 7, 需要证明下列两个条件同时成立:

$$1) L^s(s^s) \cap AP^y = L^y(s^y);$$

2) $\forall t'. t' \in S \wedge R^c(s^c, t') \Rightarrow \exists t^y. t^y \in S^y \wedge R^y(s^y, t^y) \wedge H^y(t', t^y)$ 。

证明条件 1): $L^c(s^c) \cap AP^y = L^y(s^y)$

$$\begin{aligned} L^c(s^c) \cap AP^y &= L^c(\langle s_{1a}^c, s_{2b}^c, \dots, s_{kl}^c, \dots, s_{ng}^c \rangle) \cap AP^y \\ &= \bigcap_{k=1}^n L_k^c(s_{kl}^c) \cap AP^y \\ &= \bigcap_{k=1}^n (L_k^c(s_{kl}^c) \cap AP_k^y) \end{aligned} \quad (3)$$

根据定义 1 和异步合成的定义, 有 $AP^y = \bigcup_{k=1}^n AP_k^y$, 将其带入式(3)得到:

$$L^c(s^c) \cap AP^y = \bigcap_{k=1}^n (L_k^c(s_{kl}^c) \cap \bigcup_{k=1}^n AP_k^y) \quad (4)$$

注意, $L_k^c(s_{kl}^c)$ 表示状态 s_{kl}^c 上取值为真的 AP_k^c 中的原子命题的集合, 只与 AP_k^c 有关, 与 $AP_j^c (1 \leq j \leq n, j \neq k)$ 无关, 且 $AP_k^c \subseteq AP_k^y$, 所以有:

$$\begin{aligned} L_k^c(s_{kl}^c) \cap \bigcup_{k=1}^n AP_k^y &= L_k^c(s_{kl}^c) \cap (AP_1^y \cup \dots \cup AP_k^y \cup \dots \cup AP_n^y) \\ &= L_k^c(s_{kl}^c) \cap AP_k^y = L_k^y(s_{kl}^y) \end{aligned} \quad (5)$$

将式(5)带入式(4), 得到:

$$L^c(s^c) \cap AP^y = \bigcap_{k=1}^n L_k^y(s_{kl}^y) = L^y(s^y) \quad (6)$$

至此, 条件 1) 成立。

证明条件 2):

$$\forall t'. t' \in S \wedge R^c(s^c, t') \Rightarrow \exists t^y. t^y \in S^y \wedge R^y(s^y, t^y) \wedge H^y(t', t^y)$$

对于 $\forall t' = \langle t_{1a}', t_{2b}', \dots, t_{kl}', \dots, t_{ng}' \rangle, R^c(s^c, t')$ 说明在原始模型中至少存在一个进程发生状态迁移。假定前 $k (1 \leq k < n)$ 个进程发生了状态迁移, 后 $n-k$ 个进程未发生状态迁移。进程发生迁移可能改变进程的当前状态, 也可能不改变进程的当前状态。考虑在 $t' \neq s^c$ 时, 迁移 $R_k^c(s_{kl}^c, t_{kl}')$ 不改变进程当前状态的情况下局部迁移对全局迁移的影响。

因为 $M_k \leq M_k^y$, 则有:

$$R_k^c(s_{kl}^c, t_{kl}')$$

$$R_k^y(s_{kl}^y, t_{kl}^y) \wedge H_k^y(t_{kl}', t_{kl}^y)$$

按照异步合成的定义构造 t^y :

$$\begin{aligned} t^y &= \langle t_{1a}^y, \dots, t_{kl}^y, t_{(k+1)r}^y, \dots, t_{ng}^y \rangle \\ &\triangleq \langle t_{1a}^y, \dots, t_{kl}^y, s_{(k+1)r}^y, \dots, s_{ng}^y \rangle \\ &= \langle H_1^y(t_{1a}'), \dots, H_k^y(t_{kl}'), s_{(k+1)r}^y, \dots, s_{ng}^y \rangle \\ &= \langle H_1^y(t_{1a}'), \dots, H_k^y(t_{kl}'), H_{k+1}^y(s_{(k+1)r}^y), \dots, H_n^y(s_{ng}^y) \rangle \end{aligned} \quad (8)$$

因为原始模型中后 $n-k$ 个进程未发生状态迁移, 其状态不变, 故 $s_{(k+1)r}^y = t_{(k+1)r}^y, \dots, s_{ng}^y = t_{ng}^y$, 将其带入式(8)得到:

$$t^y = \langle H_1^y(t_{1a}'), \dots, H_k^y(t_{kl}'), H_{k+1}^y(t_{(k+1)r}^y), \dots, H_n^y(t_{ng}^y) \rangle \quad (9)$$

此公式表示 t^y 是对 t' 中的每一个分量同时运用抽象算子 H_k^y 得到的, 因此 $(t', t^y) \in H^y$ 。

又由式(7)可知, 状态向量 s^y 和 t^y 中至少有一个分量满足 $R_k^y(s_{kl}^y, t_{kl}^y)$, 因此 $(s^y, t^y) \in R^y$ 。

$t' \neq s^c$ 时, 迁移 $R_k^c(s_{kl}^c, t_{kl}')$ 改变进程当前状态和 $t' = s^c$ 两种情况的证明过程相同。

至此, 条件 1) 和条件 2) 均成立, 证明了 $H^y \subseteq S \times S^y$ 是 $PS^c(n)$ 与 $PS^y(n)$ 之间的一个模拟关系。根据定义 7 可得, $PS^c(n)$ 中的每一个初始状态 $s_0 \in I$, 在 $PS^y(n)$ 都存在一个初始状态 $s_0^y \in I^y$ 并且满足 $H^y(s_0, s_0^y)$, 从而结论成立。

为了证明定理 2, 首先引入以下引理。

引理 1 设 $H^y \subseteq S \times S^y$ 是一个模拟关系, 对于 $\forall s^c \in S, s^y \in S^y$, 如果 $H^y(s^c, s^y)$, 则每一条从 s^c 出发的路径, 都存在一条从 s^y 出发的路径与其对应。

证明: 假设从 s^c 出发的路径为 $\pi^c = s_0^c s_1^c s_2^c \dots$ (其中 $s_0^c = s^c$), 我们通过归纳法构造一条从 s^y 出发的路径 $\pi^y = s_0^y s_1^y s_2^y \dots$ (其中 $s_0^y = s^y$) 与 π^c 对应。显然, $H^y(s_0^c, s_0^y)$ 。假定 $\exists i, H^y(s_i^c, s_i^y)$, 因为 $R^c(s_i^c, s_{i+1}^c)$, 则存在一个 s_i^c 的后继 t^y 使得 $H^y(s_{i+1}^c, t^y)$ 成立, 选择 $s_{i+1}^y = t^y$ 即可构造出 π^y 。

定理 2 对于每一个 ACTL* 公式 $f, PS^c(n) \models f \Rightarrow PS^y(n) \models f$ 。

证明: 由定理 1 知 $PS^c(n) \leq PS^y(n)$, 并且存在一个模拟关系 $H^y \subseteq S \times S^y$, 对于 $\forall s_0 \in I, \exists s_0^y \in I^y$ 满足 $H^y(s_0, s_0^y)$ 。由引理 1, 从 s_0 出发的每一条路径 $\pi^c = s_0^c s_1^c s_2^c \dots$, 都存在一条从 s^y 出发的路径 $\pi^y = s_0^y s_1^y s_2^y \dots$ 与其对应, 并且满足 $H^y(s_i^c, s_i^y)$, 下面进行归纳证明。

1) 如果 $f = p, p \in AP^y$ 。因为 $PS^c(n) \models f$ 当且仅当 $\forall s_0 \in I^y, s_0^y \models f$, 由 $H^y(s_0, s_0^y)$ 可知, $L^c(s_0) \cap AP^y = L^y(s_0^y)$, 即 s_0^y 的标记是 s_0 的标记的子集, 于是 $s_0 \models f$ 。由 s_0^y 的任意性, 可得 $PS^c(n) \models f$ 。

2) 如果 $f = \neg f_1$ 是状态公式。

$$\begin{aligned} PS^c(n) \models f &\Rightarrow \forall s_0 \in I^y, s_0^y \models f \\ &\Rightarrow \forall s_0 \in I^y, s_0^y \neq f_1 \\ &\Rightarrow \forall s_0 \in I^y, s_0^y \neq f_1 \\ &\Rightarrow PS^c(n) \models f \end{aligned}$$

此推理过程适用于 f 是路径公式的情况。

3) 如果 $f = f_1 \wedge f_2$ 是状态公式。

$$\begin{aligned} PS^c(n) \models f &\Rightarrow \forall s_0 \in I^y, s_0^y \models f \\ &\Rightarrow \forall s_0 \in I^y, s_0^y \models f_1 \wedge f_2 \\ &\Rightarrow \forall s_0 \in I^y, (s_0^y \models f_1 \wedge s_0^y \models f_2) \\ &\Rightarrow \forall s_0 \in I^y, (s_0^y \models f_1 \wedge s_0^y \models f_2) \\ &\Rightarrow \forall s_0 \in I^y, s_0^y \models f_1 \wedge f_2 \\ &\Rightarrow PS^c(n) \models f \end{aligned}$$

此推理过程适用于 f 是路径公式的情况。

4) 如果 $f = f_1 \vee f_2$ 是状态公式。推理与 3) 类似。

5) 如果 $f = f_1 U f_2$ 是路径公式。对于任意一条从 s^y 出发的路径 $\pi^y = s_0^y s_1^y s_2^y \dots$, 必定存在 $i \geq 1$, 使得 $s_i^y \models f_2$ 并且对任何 $1 \leq j < i$ 满足 $s_j^y \models f_1$ 。由 $H^y(s_i^c, s_i^y)$ 可知, $L^c(s_i^c) \cap AP^y = L^y(s_i^y)$, 则有 $s_i^c \models f_2$ 并且对任何 $1 \leq j < i$ 满足 $s_j^c \models f_1$, 因此 $PS^c(n) \models f$ 。

6) 对于 $Af_1, Xf_1, Ff_1, Gf_1, f_1 R f_2$, 可用类似方法证明。

定理 3 对于单索引 ACTL* 公式 $\forall x. \varphi(x), \varphi(x)$ 的原子公式是 L 中的标记, 那么 $PS^c \models \varphi(x) \Rightarrow \forall n. PS^y(n) \models \forall x. \varphi(x)$ 。

证明: 覆盖性和一致性^[7] 保证了对任意规模的系统 $PS^y(n) (n > 1)$, 均能够找到一个中间抽象模型 PS_n^y , 满足 $PS^y(n) \leq_{h/k} PS_n^y$ 和 $PS_n^y \leq PS^c$, h 表示 hub , $\leq_{h/k}$ 表示选择第 k 个进程作为 hub 时建立的模拟关系。根据模拟关系的传递性有 $PS^y(n) \leq PS^c$, 因此若 $PS^c \models \varphi(x)$, 则 $PS^y(n) \models \varphi(x)$ 。由 n 和 k 的任意性, 则有 $PS^c \models \varphi(x) \Rightarrow \forall n. PS^y(n) \models \forall x. \varphi(x)$, 结论成立。

结束语 二维抽象对参数化系统包含的进程数目和进程间的交互方式没有严格限制, 因而更适合处理一般意义上的

并发系统。二维抽象首先对所有进程单独进行抽象,然后利用参数化系统的设计思想,隐藏系统参数建立全系统的抽象模型,最大限度地剔除了原始系统中的冗余信息。TDA 模型关于 ACTL* 公式弱保持,而且在 TDA 模型中成立的单索引 ACTL* 公式,在任意规模的原始模型中也成立,为简化参数化系统验证提供了理论依据,也为相关研究工作奠定了良好的基础。

参考文献

- [1] 屈婉霞,李墩,郭阳,等.谓词抽象技术研究[J].软件学报,2008,19(1):27-38
- [2] Shuvendu K L, Randal E B. Indexed Predicate Discovery for Unbounded System Verification[C]//Proc. of the 16th International Conference on Computer Aided Verification(CAV'04). Boston,

USA; Springer, 2004; 276-289

- [3] Amir P, Jessica Xu, Lenore Z. Liveness with $(0; 1; \infty)$ Counter Abstraction[A]//Proc. of the 14th International Conference on Computer Aided Verification(CAV'02)[C]. Copenhagen, Denmark; Springer, 2002; 61-70
- [4] Muralidhar T. Abstraction Techniques for Parameterized Verification[D]. Pittsburgh; Carnegie Mellon University, 2006
- [5] 曾红卫,缪淮扣.构件组合的抽象精化验证[J].软件学报,2008,19(5):1149-1159
- [6] Konnov I V, Zakharov V A. An Invariant-Based Approach to the Verification of Asynchronous Parameterized Networks[C]//the 1st workshop on Invariant Generation(WING2007). Hagenberg, Austria; Springer, 2007; 41-55
- [7] 屈婉霞,庞征斌,郭阳,等.参数化系统二维抽象框架[J].国防科技大学学报,2010,32(1):95-100

(上接第 281 页)

表 1 提出的水印算法和基于 Zernike 矩算法的运行时间(单位:ms)

	压缩	裁剪	加噪	平移	旋转	缩放
k=5	0.352	0.380	0.316	0.288	0.339	0.197
k=3	0.686	0.749	0.563	0.597	0.655	0.290
k=1	1.89	2.26	1.78	1.86	2.06	0.950
Zernike	297	360	302	282	348	153

结束语 本文首先研究了图像不变质心的特点和性质。为了使不变质心对几何攻击以及其他攻击具有更好的抵抗能力,对不变质心的提取方法进行了改进,不对整个图像求不变质心,而是对图像进行小波分解后,对小波低频域提取不变质心,取得了良好的效果。接着根据水印图像的大小自适应地对载体图像进行适当级的小波分解,将水印嵌入到对干扰不敏感的最后一级小波低频域,兼顾了水印的嵌入容量和不可见性。将含水印图像用改进的方法对小波域低频子图求得一系列基于不变质心的不变量后,基于这些不变量对攻击所具有的稳定性,定义了含水印图像的不变特征矩阵,并联合 Rijndael 加密技术实现了版权的认证,在提高水印算法可靠性的同时,使算法具有很好的鲁棒性。

该算法可嵌入实际的比特序列。实验结果表明,本文提供的水印算法能够抵抗包括平移、旋转、缩放等几何攻击在内的各种攻击,在提取水印时不需要原始载体图像和原始水印图像,从水印的透明性、水印嵌入容量和水印鲁棒性以及算法复杂度等指标来看,均具有较好的实效性。

参考文献

- [1] Lee C H, Lee H K, Suh Y G. Image Watermarking Resistant to Combined Geometric and Removal Attacks[J]. International

Journal of Image and Graphics, 2005, 5(1): 37-66

- [2] 金聪,彭嘉维.基于图像投影序列的盲数字水印鲁棒检测方法[J].软件学报,2005,16(2):295-302
- [3] Lin P L, Hsieh C K, Huang P W. A Hierarchical Digital Watermarking Method for Image Tamper Detection and Recovery[J]. Pattern Recognition, 2005, 38(12): 2519-2529
- [4] Kim H S, Lee H K. Invariant Image Watermark Using Zernike Moments[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 766-775
- [5] 李雷达,郭宝龙,刘雅宁.基于伪 Zernike 矩的抗几何攻击图像水印[J].光电子·激光,2007,18(2):231-235
- [6] 沃焱,韩国强.基于修改的 Zernike 矩的抗几何攻击的数字水印方法[J].计算机科学,2009,36(5):247-250,281
- [7] Liu Jun, Yang Huijuan, Kot A C. Relationships and Unification of Binary Images Data-hiding Methods[C]//IEEE International Conference on Image Processing. 2005, 1: I-981-4
- [8] Ji Z, Jiang L, Jin J. An Improved Second Generation Digital Image Watermarking Scheme[C]//Mathematics of Data/Image Coding, Compression, and Encryption VI, with Applications. 2004, 5208: 218-223
- [9] 凌贺飞,卢正鼎,邹复好.抗几何攻击的数字水印技术综述[J].计算机工程与科学,2006,28(11):42-47,50
- [10] 钟桦,张小华,焦李成.数字水印与图像认证——算法及应用[M].西安:西安电子科技大学出版社,2006
- [11] Seo J S, Yoo C D. Image Watermarking Based on Invariant Regions of Scale-space Representation[J]. IEEE Transactions on Signal Process, 2006, 54(4): 1537-1549
- [12] Jamil T. The Rijndael Algorithm[J]. IEEE Potentials, 2004, 23(2): 36-38
- [13] 王炳锡.数字水印技术[M].西安:西安电子科技大学出版社,2003

(上接第 294 页)

- [5] Do M N, Vetterli M. The Contourlet transform: an efficient directional multiscale image representation [J]. IEEE Trans on Image Proc, 2005, 14(12): 2091-2106
- [6] Zhou Jian-ping, Cunha A L, Do M N. Nonsubsampled contourlet transform: construction and application in enhancement[C] // Proceedings of International Conference on Image Processing (ICIP). Piscataway, NJ; IEEE, 2005, 1: 469-472
- [7] Cunha A L, Zhou Jian-ping, Do M N. The nonsubsampled contourlet transform: theory, design and applications [J]. IEEE Trans on Image Proc, 2006, 15(15): 3089-3101

- [8] 罗子娟,吴一全.基于 contourlet 变换的红外图像序列小目标检测技术[J].信号处理,2008,24(4):676-679
- [9] 吴一全,罗子娟,吴文怡.基于 NSCT 的红外图像小目标检测技术[J].中国图象图形学报,2009,14(3):477-481
- [10] 唐志航,黄哲,张东衡,等.基于尺度相关性的自适应图像增强新算法[J].计算机应用,2006,26(9):2084-2086
- [11] 韩敏,刘云侠.改进的双小波空域相关混沌信号降噪方法[J].系统仿真学报,2009,21(15):4743-4747
- [12] 徐军,周翔,梁昌洪.红外序列图像弱小目标检测算法[J].红外与激光工程,2003,32(4):390-393
- [13] 曾明,李建勋.基于自适应形态学 Top-Hat 滤波器的红外弱小目标检测方法[J].上海交通大学学报,2006,40(1):90-97