多样性冗余的容侵系统可靠性分析

周 华,孟相如,张 立,乔向东
ZHOU Hua,MENG Xiang-ru,ZHANG Li,QIAO Xiang-dong

空军工程大学 电讯工程学院,西安 710077
Institute of Telecommunication Engineering,Air Force Engineering University,Xi'an 710077,China
E-mail:zhoumiaomiao_2005@126.com

ZHOU Hua,MENG Xiang-ru,ZHANG Li,et al.Reliability in intrusion-tolerance system of diverse redundancy.Computer Engineering and Applications,2009,45(15):20-23.

Abstract: The hypothesis of independent failure is incomplete to evaluate the reliability in intrusion-tolerance system of diverse redundancy.This paper analyzes the reliability in intrusion-tolerance system based on the probability methodology.The results show that the system reliability relies on the subsystems' reliabilities and their inner relations under attacks.An evaluation model is also proposed.Compared with the system reliability under independence hypothesis,this model includes three possible cases,and the evaluation results in examples demonstrate the completeness of our model.

Key words: intrusion-tolerance;diversity;redundancy;reliability

摘 要: 在评估多样性冗余的容侵系统可靠性时,通常假设各个子系统的失效是相互独立的,从而使得评估结果存在片面性。针对这一问题,使用概率的方法对多样性冗余的容侵系统可靠性进行了分析。结果表明,容侵系统的可靠性不仅与子系统的可靠性有关,而且还依赖于在攻击行为下子系统之间的内在联系。在此基础上,提出了容侵系统可靠性的评估模型。该模型对系统可靠性的评估结果涵括了大于、等于以及小于相互独立假设条件下系统可靠性三种情况。最后通过实例分析验证了模型评估结果的全面性。

关键词: 入侵容忍;多样性;冗余;可靠性
DOI: 10.3778/j.issn.1002-8331.2009.15.006 **文章编号:** 1002-8331(2009)15-0020-04 **文献标识码:** A **中图分类号:** TP309.2

1 前言

入侵容忍是在容错技术基础上发展起来的一种安全技术,但是与传统的安全技术不同,它主要考虑的是在受到入侵的情况下系统的生存能力。为了提高容侵系统的生存能力和可靠性,在构建容侵系统时通常采用节点多样性冗余的方法,如SITAR[1],HACQIT[2]等。

目前,容侵系统安全性和可靠性的定量评估受到了研究者的重视。文献[3]分析了系统冗余多样性与系统安全性的内在联系。文献[4]从可操作系统安全的评估方法角度讨论了可靠性与安全性的共同点。文献[5]对入侵容忍系统的安全性进行了量化分析。主要对多样性冗余的容侵系统可靠性进行了分析,认为子系统之间因攻击行为失效是相关而不是相互独立的,由此得出了系统可靠性的评估模型,并在实例中利用该模型分析了系统可靠性存在的三种可能情况。

2 模型分析

在容错领域评估多样性冗余系统的可靠性时,通常假设各个不同子系统的失效是相互独立的。但是,相关研究[6-7]表明相互独立假设的观点是不准确的。由于攻击行为的智能性和不可控性,使得容侵系统在遭受攻击时子系统之间的相关性更为紧密,因此容侵系统中各个子系统的失效也不是相互独立的。一般认为,多样性冗余的容侵系统比由单一子系统构成的系统可靠性更高,但这取决于子系统之间因攻击而失效的相互关联程度,而不仅仅是依赖于它们各自的可靠性。

由于攻击者的攻击行为对于容侵系统而言是不确定的,因而可以将攻击行为认为是一种随机过程,这个随机过程的本质反映了容侵系统所面临的安全威胁。所以在分析多样性冗余的容侵系统可靠性时,可以使用概率的方法进行讨论。

假定所有不同子系统的开发过程是相互独立的,这些子系统构成一个子系统集合$\vartheta=\{\pi_1,\pi_2,\cdots\}$,其中一些子系统会因攻击行为而失效。构建容侵系统时,从ϑ中随机选择一个子系统π,即这个随机选择的子系统是一个随机变量$\prod$:

$$P(\prod=\pi)=S(\pi) \quad (1)$$

$S(\cdot)$表示随机选择子系统的概率。

基金项目: 国家自然科学基金(the National Natural Science Foundation of China under Grant No.60774091);陕西省自然科学基金(the Natural Science Foundation of Shaanxi Province of China under Grant No.SJ08F14)。

作者简介: 周华(1981-),男,博士研究生,主要研究方向为计算机网络安全;孟相如(1963-),男,博士后,教授,博士生导师,研究方向为宽带网络和信息处理;张立(1981-),男,博士研究生,研究方向为计算机网络故障诊断;乔向东(1974-),男,博士,副教授,研究生导师,研究方向为计算机网络安全。

收稿日期: 2008-12-30 **修回日期:** 2009-02-25

假定所有的攻击行为组成一个攻击行为空间$\chi=\{x_1,x_2,\cdots\}$,那么一个随机发生的攻击行为x也是一个随机变量X:

$$P(X=x)=Q(x) \tag{2}$$

$Q(\cdot)$表示攻击行为发生的概率。

一个子系统遭受一个攻击行为时产生的后果可以用一个结果函数表示:

$$v(\pi,x)=\begin{cases}1 & \text{系统 } \pi \text{ 因攻击行为 } x \text{ 而失效}\\ 0 & \text{系统 } \pi \text{ 在攻击行为 } x \text{ 下未失效}\end{cases} \tag{3}$$

那么随机变量$v(\prod,X)$则表示了一个随机的子系统遭到一个随机的攻击行为时产生的后果。

一个随机选择的子系统因一个确定的攻击行为x而失效的概率为:

$$P(\prod \text{ fails on } x)=\theta(x)=\sum_{\pi\in\vartheta}v(\pi,x)S(\pi) \tag{4}$$

那么对于一个随机选择的攻击行为X,$\theta(X)$则为随机变量,令为Θ。

一个确定的系统π因一个随机的攻击行为而失效的概率为:

$$P(\pi \text{ fails on } X)=\varphi(\pi)=\sum_{x\in\chi}v(\pi,x)Q(x) \tag{5}$$

那么$1-\varphi(\pi)$则是子系统π的可靠性。对于一个随机选择的子系统$\prod$,$\varphi(\prod)$则为随机变量,令为Φ。

一个随机选择的子系统遭到一个随机的攻击行为而失效的概率:

$$E(\Theta)=E(\Phi)=\sum_{\pi\in\vartheta}\sum_{x\in\chi}v(\pi,x)S(\pi)Q(x) \tag{6}$$

由于子系统本身的开发过程和使用中遭到攻击的不确定性,式(6)表示了容侵系统平均失效的可能性。假定随机选择两个不同的子系统π_1、π_2的过程是相互独立的,即:

$$P(\prod_1=\pi_1,\prod_2=\pi_2)=P(\prod_1=\pi_1)P(\prod_2=\pi_2) \tag{7}$$

那么子系统π_1、π_2因一个确定的攻击行为x而同时失效的概率为:

$$P(\prod_1 \text{ fails on } x,\prod_2 \text{ fails on } x)=$$

$$\sum_{\pi\in\vartheta}\sum_{\pi\in\vartheta}v(\pi_1,x)v(\pi_2,x)P(\prod_1=\pi_1,\prod_2=\pi_2)=$$

$$\sum_{\pi\in\vartheta}\sum_{\pi\in\vartheta}v(\pi_1,x)v(\pi_2,x)P(\prod_1=\pi_1)P(\prod_2=\pi_2)=$$

$$\sum_{\pi\in\vartheta}v(\pi_1,x)P(\prod_1=\pi_1)\sum_{\pi\in\vartheta}v(\pi_2,x)P(\prod_2=\pi_2)=$$

$$P(\prod_1 \text{ fails on } x)P(\prod_2 \text{ fails on } x) \tag{8}$$

那么条件概率:

$$P(\prod_2 \text{ fails on } x|\prod_1 \text{ failed on } x)=$$

$$\frac{P(\prod_1 \text{ failed on } x,\prod_2 \text{ fails on } x)}{P(\prod_1 \text{ failed on } x)}=P(\prod_1 \text{ fails on } x) \tag{9}$$

可以看到如果在子系统开发过程与选择过程中是相互独立的,那么多样性子系统在确定的攻击行为下的失效也是相互独立的,不会受到彼此的影响。但是,当系统遭受一个随机的攻击行为X时,系统失效的概率为:

$$P(\prod_1 \text{ fails on } X,\prod_2 \text{ fails on } X)=$$

$$\sum_{x\in\chi}\sum_{\pi\in\vartheta}\sum_{\pi\in\vartheta}v(\pi_1,x)v(\pi_2,x)P(\prod_1=\pi_1,\prod_2=\pi_2)Q(x)=$$

$$\sum_{x\in\chi}\left(\sum_{\pi\in\vartheta}v(\pi,x)P(\prod=\pi)\right)^2Q(x)=\sum_{x\in\chi}(\theta(x))^2Q(x)=E(\Theta^2) \tag{10}$$

由 Jensen 不等式[7]可得:

$$P(\prod_1 \text{ fails on } X,\pi_1,\prod_2 \text{ fails on } X)\geqslant$$

$$\left(\sum_{x\in\chi}\theta(x)Q(x)\right)^2=(E(\Theta))^2=(P(\prod \text{ fails on } X))^2 \tag{11}$$

进一步可得:

$$P(\prod_1 \text{ fails on } X,\prod_2 \text{ fails on } X)=E(\Theta^2)=$$

$$\text{var}(\Theta)+(E(\Theta))^2=\text{var}(\Theta)+(P(\prod \text{ fails on } X))^2 \tag{12}$$

其中 var(Θ)表示方差。那么条件概率:

$$P(\prod_2 \text{ fails on } X|\prod_1 \text{ failed on } X)=$$

$$\frac{P(\prod_1 \text{ failed on } X,\prod_2 \text{ fails on } X)}{P(\prod_1 \text{ failed on } X)}=$$

$$P(\prod_2 \text{ fails on } X)+\text{var}(\Theta)/E(\Theta)\geqslant P(\prod_2 \text{ fails on } X) \tag{13}$$

式(13)表明,在一个子系统因一个随机的攻击行为而失效的情况下,另一个子系统因同样的攻击行为失效的概率要大于单个该子系统失效的概率。这说明,虽然这两个子系统的开发与选择是相互独立的,但在遭到不确定的攻击行为时,它们是存在相互联系的,即它们因攻击行为而生成的结果函数是相关的。在构建容侵系统时,选择多样性冗余子系统是确定的,不确定的是容侵系统所面临的攻击行为。以两个确定的子系统π_1、π_2构成的容侵系统为例,假定只要存在一个子系统没有发生失效,容侵系统就可以正常工作。由式(5)可以得到:

$$P_{\pi_1}=(\pi_1 \text{ fails on } X)=\sum_{x\in\chi}Q(x)v(\pi_1,x) \tag{14}$$

$$P_{\pi_2}=(\pi_2 \text{ fails on } X)=\sum_{x\in\chi}Q(x)v(\pi_2,x) \tag{15}$$

子系统π_1、π_2结果函数的协方差为:

$$cov(v(\pi_1,X),v(\pi_2,X))=$$

$$\sum_{x\in\chi}(v(\pi_1,x)-P_{\pi_1})\cdot(v(\pi_2,x)-P_{\pi_2})\cdot Q(x) \tag{16}$$

那么一个随机的攻击行为X使得系统π_1、π_2同时失效的概率为:

$$P(\pi_1 \text{ fails on } X,\pi_2 \text{ fails on } X)=P(X|v(\pi_1,X)=$$

$$v(\pi_2,X)=1)=P_{\pi_1}\cdot P_{\pi_2}+cov(v(\pi_1,X),v(\pi_2,X)) \tag{17}$$

式(17)表明,对于一个确定的容侵系统,分析其可靠性不仅需要知道各个子系统在随机攻击行为下的失效概率,还要知道各个子系统在攻击行为下失效的内在联系。为了简化评估模型,可以将攻击行为进行分类[8]。

对已知的攻击行为进行分类,即将攻击行为空间χ分为一系列子域的集合$\{\chi_1,\chi_2,\cdots,\chi_n\}$,其中$\chi=\chi_1\cup\chi_2\cup\cdots\cup\chi_n$,$\chi_i\cap\chi_j=\phi$,$i,j\in\{1,2,\cdots,n\}$。属于子域$\chi_i$的一种攻击行为发生概率为$P(\chi_i)$,以及子域$\chi_i$内的攻击行为导致子系统$\pi_1$和$\pi_2$失效的概率分别为$P(\pi_1|\chi_i)$,$P(\pi_2|\chi_i)$。为了简便起见,用$P(\pi_1,\pi_2)$表示$P(\pi_1 \text{ fails on } X,\pi_2 \text{ fails on } X)$,用$P(\pi_1,\pi_2|\chi_i)$表示$P(\pi_1 \text{ fails on } X\in\chi_i,\pi_2 \text{ fails on } X\in\chi_i)$。

系统失效的概率为:

$$P(\pi_1,\pi_2)=\sum_i P(\pi_1,\pi_2|\chi_i)\cdot P(\chi_i)=$$

$$\sum_i (P(\pi_1|\chi_i)\cdot P(\pi_2|\chi_i)+cov_i(v(\pi_1,X),v(\pi_2,X)))\cdot P(\chi_i)=$$

$$\sum_i (P(\pi_1|\chi_i)\cdot P(\pi_2|\chi_i)\cdot P(\chi_i)+$$

$$\sum_i cov_i(v(\pi_1,X),v(\pi_2,X))\cdot P(\chi_i) \quad (18)$$

系统的可靠性为：

$$R(\pi_1,\pi_2)=1-P(\pi_1,\pi_2) \quad (19)$$

从式(18)中可以看到系统失效的概率存在三种情况：(1)如果其中一个子系统受到某个子域中的所有攻击行为时，其$v(\pi,X)$为常数(0或1)时，那么协方差项就为0。系统失效概率等效于相互独立假设下系统的失效概率；(2) 如果协方差项小于0，那么系统失效概率小于相互独立假设下系统的失效概率；(3)如果协方差项大于0，即子系统受到攻击行为的影响是正相关的，那样系统失效概率会大于相互独立假设下系统的失效概率。相应地，系统可靠性的评估结果则会出现等于、大于和小于相互独立假设下系统的可靠性。

上述评估模型充分考虑到了可靠性存在的三种可能情况，比简单地相互独立假设更加全面，增加了对系统分析评估的准确性。

3 实例分析

采用实验数据与估值相结合的方法进行量化分析系统的可靠性。虽然估值的方法与实际数据并不一定相符，但它反映了系统可靠性变化的一种趋势。

实验数据采用KDD Cup99数据集的子集1999 kddcup.data_10_percent[9]，在这个数据集中共有22种攻击行为，可以分为四类，即攻击空间χ={*Probing*,*DOS*,*U2R*,*R2L*}，子集分别为：

Probing={*portsweep*,*ipsweep*,*nmap*,*satan*}

DOS={*neptune*,*smurf*,*pod*,*teardrop*,*land*,*back*}

U2R={*buffer_overflow*,*loadmodule*,*perl*,*rootkit*}

R2L={*ftp_write*,*guess_passwd*,*imap*,*phf*,*multihop*,*warezmaster*,*warezclient*,*spy*}

将各类攻击行为在数据集中出现的频率作为对这类攻击行为发生概率的估值，如表1所示。

表1 四类攻击行为发生的概率

	Probing	DOS	U2R	R2L
$P(\chi_i)$	0.010 03	0.974 86	0.003 07	0.012 05

将子域中每一种攻击行为出现的频率作为对这种攻击行为发生概率的估值，如表2所示。

表2 子域内各种攻击行为发生的概率

portswep	ipsweep	nmap	satan	neptune	smurf	pod	teardrop
0.261 4	0.281 0	0.058 1	0.399 4	0.274 7	0.716 6	0.000 9	0.002 3
land	back	buffer_overflow	rootkit	perl	load-module	spy	imap
0.000 05	0.005 4	0.793 8	0.008 2	0.084 6	0.113 4	0.000 4	0.002 5
warez-master	ftp_write	guess_passwd	warez-client	phf	multihop		
0.004 2	0.001 7	0.775 5	0.213 4	0.000 8	0.001 5		

实例1 子系统π_1、π_2在各种攻击行为下的结果函数如表3所示。

表3 子系统π_1、π_2的结果函数

	portswep	ipsweep	nmap	satan	neptune	smurf	pod	teardrop
π_1	0	0	0	0	1	1	1	1
π_2	0	0	1	0	1	0	0	1
	land	back	buffer_overflow	rootkit	perl	load-module	spy	imap
π_1	1	1	0	0	0	0	1	1
π_2	0	1	0	1	0	1	0	1
	warez-master	ftp_write	guess_passwd	warez-client	phf	multihop		
π_1	1	1	1	1	1	1		
π_2	1	1	0	0	1	1		

在表3中，假定子系统π_1在受到各个子域内的攻击行为时，结果函数保持一致，即要么全部为1，要么全部为0。那么每一个子域内攻击行为导致子系统失效的概率如表4所示。

表4 子系统的失效概率

	Probing	DOS	U2R	R2L
$P(\pi_1\|\chi_i)$	0	1	0	1
$P(\pi_2\|\chi_i)$	0.058 1	0.282 4	0.121 6	0.010 7

由此可以计算出容侵系统失效概率为$P(\pi_1,\pi_2)$=0.275 4，系统的可靠性$R(\pi_1,\pi_2)$=0.724 6；在相互独立假设条件下容侵系统的失效概率为$P'(\pi_1,\pi_2)$=0.275 4，系统的可靠性$R'(\pi_1,\pi_2)$=0.724 6。因此，系统可靠性与相互独立假设条件下系统的可靠性是相同的。

实例2 子系统π_1、π_2在各种攻击行为下的结果函数如表5所示。

表5 子系统π_1、π_2的结果函数

	portswep	ipsweep	nmap	satan	neptune	smurf	pod	teardrop
π_1	1	0	1	0	1	0	0	0
π_2	0	0	1	0	1	0	0	1
	land	back	buffer_overflow	rootkit	perl	load-module	spy	imap
π_1	1	0	1	1	1	0	1	0
π_2	0	1	0	1	0	1	0	1
	warez-master	ftp_write	guess_passwd	warez-client	phf	multihop		
π_1	0	1	0	1	0	0		
π_2	1	1	0	0	1	1		

每一个子域内攻击行为导致子系统失效的概率如表6所示。

表6 子系统的失效概率

	Probing	DOS	U2R	R2L
$P(\pi_1\|\chi_i)$	0.319 5	0.274 8	0.092 8	0.215 5
$P(\pi_2\|\chi_i)$	0.058 1	0.282 4	0.121 6	0.010 7

容侵系统失效的概率为$P(\pi_1,\pi_2)$=0.268 4，系统的可靠性$R(\pi_1,\pi_2)$=0.731 6；在相互独立假设下容侵系统失效概率为$P'(\pi_1,\pi_2)$=0.075 8，系统的可靠性$R'(\pi_1,\pi_2)$=0.924 2。此时，系统可靠性小于相互独立假设条件下系统的可靠性。

实例3 子系统π_1、π_2在各种攻击行为下的结果函数表7所示。

表 7　子系统π_1、π_2的结果函数

	portswep	ipsweep	nmap	satan	neptune	smurf	pod	teardrop
π_1	1	0	1	0	0	1	1	0
π_2	1	0	0	0	1	0	1	0
	land	back	buffer_ overflow	rootkit	perl	load- module	spy	imap
π_1	1	1	1	0	0	0	1	0
π_2	0	1	0	1	1	0	0	1
	warez- master	ftp_write	guess_ passwd	warez- client	phf	multihop		
π_1	0	1	0	1	1	1		
π_2	1	1	0	1	0	0		

每一个子域内攻击行为导致子系统失效的概率如表 8 所示。

表 8　子系统的失效概率

	Probing	DOS	U2R	R2L
$P(\pi_1\|\chi_i)$	0.319 5	0.722 9	0.793 8	0.217 8
$P(\pi_2\|\chi_i)$	0.261 4	0.281 1	0.092 8	0.222 7

容侵系统失效的概率 $P(\pi_1,\pi_2)$=0.013 3,系统的可靠性 $R(\pi_1,\pi_2)$=0.986 7;在相互独立假设下容侵系统的失效概率为 $P'(\pi_1,\pi_2)$=0.201 7,系统的可靠性 $R'(\pi_1,\pi_2)$=0.798 3。因此,在这种情况下系统可靠性可以优于相互独立假设条件下系统的可靠性。

由上述实例的结果可以看出,在评估容侵系统的可靠性时,子系统失效是相互独立的假设并不全面。一般认为,在相互独立假设条件下系统的可靠性是最理想的,实际的容侵系统可靠性要小于该假设条件下的可靠性。但是,通过评估模型可以看出,在独立假设条件下系统的可靠性并不一定是最优的。如果在遭到攻击行为时,子系统之间表现为负相关的联系,那么系统的可靠性可以更高。因此,该评估模型可以对容侵系统的可靠性进行更加全面地分析,增加系统可靠性评估结果的准确性。

4　结论

分析了多样性冗余的容侵系统可靠性,认为系统可靠性不仅与子系统的可靠性有关,而且还依赖于在攻击行为下子系统之间的内在联系。在此基础上,建立了容侵系统可靠性评估模型,并在实例中运用该评估模型对系统可靠性进行了分析。结果表明,在相互独立的假设条件下系统的可靠性并不是最理想的,系统可靠性可能存在三种不同的情况。因而,该模型可以较为准确和全面地对容侵系统的可靠性进行评估。

参考文献:

[1] Wang Fei-yi,Gong Feng-min,Sargor C,et al.SITAR:A scalable intrusion-tolerant architecture for distributed services[C]//Proceedings of 2nd Annual IEEE Systems,Man,and Cybernetics Information Assurance Workshop.New York:IEEE Press,2001:1-8.

[2] Reynolds J C,Just J E,Lawson E,et al.The design and implementation of an intrusion tolerant system[C]//Proceedings of DSN 2002 International Conference on Dependable Systems and Networks,Washington,D C,USA,2002:285-292.

[3] Littlewood B,Strigini L.Redundancy and diversity in security[C]//LNCS 3139,2004:423-438.

[4] Littlewood B,Brocklehurst S,Fenton N,et al.Towards operational measures of computer security[J].Journal of Computer Security,1993,2:211-229.

[5] 周华,孟相如,张立.入侵容忍系统的状态转移模型定量分析[J].北京邮电大学学报,2008,31(3):94-97.

[6] Eckhardt D E,Lee L D.A Theoretical basis for the analysis of multiversion software subject to coincident errors[J].IEEE Transactions on Software Engineering,1985,12(11):1511-1517.

[7] Littlewood B,Miller D R.Conceptual modeling of coincident failures in multiversion software[J].IEEE Transactions on Software Engineering,1989,12(15):1596-1614.

[8] Popov P,Strigini L,May J,et al.Estimating bounds on the reliability of diverse systems[J].IEEE Transactions on Software Engineering,2003,29(4):345-359.

[9] KDD Cup 1999 Data[EB/OL].(1999-10-28).http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

(上接 10 页)

图 3　提取的足球运动关键帧

该镜头虽然只有 28 帧,但因为摄像机的快速移动,拉伸和目标人物的移动,通过本算法提取了 4 帧关键帧,可以看到通过这 4 帧反映了视频的主要内容,尤其是运动信息。

从以上的实验结果分析,可以看到不管是对目标对象运动缓慢的视频,还是对目标运动剧烈,镜头快速移动的视频。本算法都能有效的找出代表视频主要内容和运动信息的关键帧,使得提取出来的关键帧代表了视频的主要内容和运动信息,并且有着很强的稳健性。

5　结论

提出了结合主成分分析和聚类的关键帧提取算法,在一系列不同类型的视频片断上进行实验和分析,实验的提取结果与人的视觉有良好的一致性,证明了该算法能有效地提取出来关键帧,并且具有良好的鲁棒性。

参考文献:

[1] Zhang Hong-jiang,Wang J Y A,Altunbasak Y.Content-based video retrieval and compression:A unifed solution[C]//IEEE International Conference on Image Processing,Washington,DC,USA,1997:13-16.

[2] Worf W.Key frame selection by motion analysis[C]//Proceedings of the 1996 IEEE International Conference on Acoustics,Speech and Signal Processing(ICASSP),Atlanta,1996:1228-1231.

[3] Zhuang Yue-ting,Rui Yong,Huang T S.Adaptive key frame extraction using unsupervised clustering[C]//Proceedings of IEEE International Conference on Image Processing(ICIP'98),Chicago,1998:866-870.

[4] Oja E.A simplified neuron model as a principal component analyzer[J].Math Biology,1982,15:267-273.

[5] Draper B A,Kyungim B,Stewart B M,et al.Recognizing faces with PCA and ICA[J].Computer Vision and Image Understanding,2003,91(1/2):115-137.

[6] 彭天强,李弼程.一种有效的抗闪光灯新闻视频镜头检测方法[J].信息工程大学学报,2007,4(8):10-13.

[7] 袁方,孟增辉,于戈.对 k-means 聚类算法的改进[J].计算机工程与应用,2004,42(36):177-120.