一种基于数字指纹在电子商务中的应用方法研究*

陈宏武[1]，赵慧民[2]
（1. 佛山科学技术学院经济管理学院，广东 佛山 528000；
2. 佛山科学技术学院电子信息工程系，广东 佛山 528000）

摘 要：数字指纹是数字权限管理（DRM）和数字内容保护的最新研究算法，而电子商务是实现DRM技术的一个重要应用领域。基于数字指纹的一种一体化实现算法，提出了一种用于电子商务的网络化应用服务技术。根据用户选择不同参数进行设置，在Peer-to-Peer服务网络下，实现了online-shop在线商务系统应用数字指纹的接口研究方案。结果表明，系统在网络环境下具有较好的鲁棒性和感官质量。

关键词：数字指纹；电子商务；接口；网络化应用
中图分类号：TN918；TP393 **文献标识码**：A **文章编号**：0529-6579（2009）03-0041-06

An Ecommerce Application Study Based on Digital Fingerprinting Technology

CHEN Hongwu[1], *ZHAO Huimin*[2]
（1. School of Business, Foshan University, Foshan 528000, China;
2. Department of Electronic & Information, Foshan University, Foshan 528000, China）

Abstract: Digital fingerprinting technology is the latest algorithm used for digital right management (DRM) and digital content protection, and ecommerce is an important application area to realize DRM technology. With integrated algorithm of digital fingerprinting technology, a network application services technology for ecommerce is proposed. Based on user selection of different parameters set, the solution for digital fingerprinting interface application on online business system (online-shop) has been implemented. The research shows that the system has better robustness and sensory quality in the peer-to-peer network environment.

Key words: digital fingerprinting; ecommerce; interface; networking application

目前在基于Internet的电子商务和电子政务应用中，系统都是以“用户ID+口令”来进行用户的身份认证和管理。这种方法具有明显缺陷：一是难以记忆，二是容易被黑客破译。随着电子商务和电子政务的越来越广泛的应用，必须有一个更好的系统来进行基于身份的权限管理技术，这就是数字权限管理（Digital rights management）DRM技术[1]。

而在DRM实现中，数字水印及其数字指纹是其焦点研究技术。其中，数字指纹是数字水印的一种重要研究分支。文献[2-3]对于DRM应用进行了深入研究，其主要设计的数字水印（或数字指纹）用于信源的嵌入和数字内容的保护。文献[4-5]针对DRM中的数字指纹和DTV条件接收问题提出了相应的编解码分析方法。这些研究实现方法，都是面向数字内容发布者和权限拥有者进行的DRM保护措施。鉴于此研究应用的局限性，并针对电子商务的安全性，本文提出一种新的基于数

* 收稿日期：2008-10-08
基金项目：广东省科技计划资助项目（2008B070800006）
作者简介：陈宏武（1972年生），男，讲师；通讯作者：赵慧民；E-mail：redcap_chen@yahoo.com.cn

字指纹的DRM技术，其主要把数字指纹嵌入到强运算之后（如DA/AD转换）的多媒体数据流中。因此，这种技术不但能够有效跟踪数字内容本身的攻击者，而且可以跟踪计算机系统之外的非法侵权者。

1 数字指纹的嵌入方法及其参数的一种自动转换算法

在许多电子商务中，数字指纹应用可以定义为三类：版权指纹；主要用于VOD系统的水印和指纹水印；对透明性有重要要求的注释指纹[6]。

考虑一个VOD传输服务，它和$n>1$个接收用户进行通信。任何条件下，服务信源（即数字内容拥有者）负责嵌入包含用户版权和所有权信息的全部指纹组标识W_s；同时，信源负责提供多媒体内容使用的密钥组K_g，K_g是对所有用户通用的密钥组。

在接收端，每个用户对服务内容必须独立解密。指纹嵌入可以出现在传输端或接收端，可以和加密机制分开或集成在一起进行。可以看到，数字指纹W_s的处理与其嵌入是不同的两种方法。

1.1 数字指纹嵌入的集成实现

在一定带宽条件下，为了克服在接收器端加入指纹的复杂性，我们提出一种解密和嵌入指纹到强运算之后的一体化集成实现—IDF（Integrating the Decryption and Fingerprinting processes）的概念，如图1。如前所述，服务器对多媒体加密使用了密钥组K_g，而对某个用户使用了唯一的密钥K_i。解密时，利用$K_i \neq K_g$，每个用户允许采用指纹的唯一性使每个解密拷贝文件不同。这时，指纹携带的信息能够用它们之间的相对熵$H(f_i)=H(K_g \mid K_i)$来表示。这里，$H(f_i)$是用户i的指纹熵，而$H(K_g \mid K_i)$是已知接收密钥时密钥组的条件熵。这种结构消除了对专用防止篡改硬件的需要，且满足了实时实现和指纹鲁棒性（尤其是群攻击）的要求。

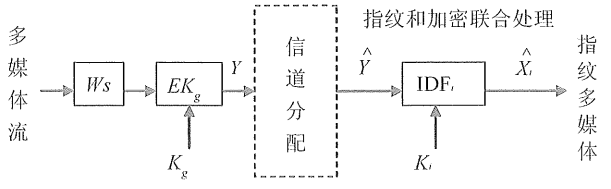

图1 指纹和加密一体化结构的应用模型

Fig. 1 Application model of integrated structure based on digital fingerprinting and encryption

这种结构是建立在Internet多播或广播信道环境下的chameleon加密技术的改进结构之上的[7]。信源从多媒体内容X中提取感官上有用的特征，并用K_s选择对它们加密，如图2所示。基于此模型，信源把加密的内容Y以多播形式给n（$n>1$）个用户。预定节目的每个用户从信源端接收密钥K_i。其解密密钥必须和K_s联系设置，可以表示为$K_R=\{K_1,K_2,\cdots,K_n\}$。

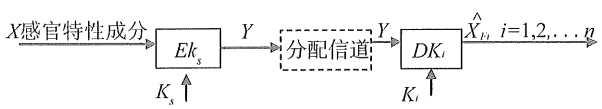

图2 数字指纹的实现结构

Fig. 2 Implementation structure of digital fingerprinting technology

对于用户i，指纹信息本质上包含在不对称密钥对（K_s，K_i）中，并且他只对加密内容$\hat{Y}=EK_s[X]$进行访问，接收用户并不知道K_s。这里，指纹就是加密和解密密钥之间的相关性函数。假设加密和解密密钥之间随机可变相关，加密的信源主要来自扰码过程[8]。定义指纹嵌入在给定多媒体对象上的最大长度负荷容量为

$$C_{Fi} \triangleq H(K_s \mid K_i) = H(K_s) - I(K_s;K_i) \quad (1)$$

这里，$H(K_s)$，$I(K_s;K_i)$和$H(K_s \mid K_i)$分别代表了加密密钥的熵，加密和解密密钥的交互信息以及在已知解密密钥时加密密钥的条件熵。由于指纹的嵌入在解密结构内进行，嵌入指纹帧的感官质量可以描述为K_s和K_i之间的相关函数。可以直观地说，相关性越强，感官质量越好。但是，可以看到，$I(K_s;K_i)$的值越大（由于相关性增大），指纹负荷容量C_{Fi}也越小。所以，（1）式说明了系统的指纹载荷容量与用户的感官质量之间的一种内在联系。

1.2 数字指纹的用户实现条件方法

利用上述结构，根据用户提供的接收条件要求，初始化本实现系统设置并转换成为服务参数。这些参数是：

- 冗余度（SR）：说明了水印怎样嵌入的信息；
- 强健度（SS）：说明了在原始数据中变换的伸缩性能；
- 加密（SE）：定义了应该使用的加密方法；
- 纠错（SC）：定义了应该应用的纠错编码；
- 可视模型（SM）：给出了感官模型的使用

信息。

在本文研究的 eCommerce 方案中，用户能够选择 1—5 范围内要求的鲁棒性（UR），保密性（US）和透明性（UT）。这里 1 表示最低的性能；而 5 是最高级的性能。对于条件接收的 VOD 用户，想要在 MPEG－1/2 压缩视频中嵌入一个版权信息。为此，需要一个高的鲁棒性和保密性以及中等透明性的算法，其分别设置为 UR＝5，US＝5，UT＝3。

实现算法分 7 步进行。

第 1，验证媒体类型。在加入指纹服务中，对媒体的某种类型选择一种可行的方式。如果找到了这种方式，算法转到第 3 步；

第 2，转换媒体类型。如果要求的 UT 满足，算法把全部资料转换为一种可行的指纹媒体类型（如 MPEG AVI）；否则，算法停止；

第 3，转换算法开始识别选择指纹的各种参数。同时，对 US，UR 和 UT，引入方法变量 MS，MR 和 MT（这里，M 代表方法 Method）。算法的初始值是 MS＝0，MR＝0，MT＝4；

MS＝0	MR＝0	MT＝4

第 4，选择 SM。为了嵌入指纹，算法选择一个感官模型来确保一个好的透明性。如果找到了此模型，那么，MS 和 MR 按照 4 增加，而 M 用 8 增加。

MS＝4	MR＝4	MT＝12

第 5，选择 SC。转换算法现在要选择一个纠错编码机制。如果 UR＝3 或 US＝4，那么需要设计应用纠错编码。以下描述参数的变化情况：

If UR＞2　　AND（No SC）：Decrease MR by（UR－2）＊2

If US＞3　　AND（No SC）：Decrease MS by（US－3）＊2

If SC：　　Increase MR by 4 and MS by 2

因为 US＝5 和 UR＝5，我们需要应用纠错编码。

MS＝6	MR＝8	MT＝12

第 6，选择 SE。选择一个加密方法。如果 US≥3，系统需要一个加密机制。参数变化如下：

If US＞2　　AND（No SE）：NO embedding possible. EXIT

If US＞2　　AND SE：Increase MS by 6or more，decrease MR by 3

If US＜＝2：　　NO encrytion

MS＝12	MR＝5	MT＝12

第 7，选择 SR 和 SS。最后一步，服务器端对 SR 和 SS 进行选择。为此，进行下列的循环操作运算：

If（MR＞MS）OR（MR＞MT）AND（UR＜US）OR（UR＜UT）：

Not possible to increase MR

While（MR/2）＜UR AND（（MR＜MS AND UR＞US）OR（MR＜MT AND UR＞UT））：

Increase SR，SS and MR and Decrease MS，MT.

这个方法的变化将和用户给定的要求比较。第 7 步增加了鲁棒性要求，但保密性和透明性要求降低。因为高的鲁棒性，这种应用的参数按照如下的变化修改：

表 1　参数变化选择表

Table 1　Selection of altered parameters

MS	MR	MT	SR	SS
11	6	11	1	1
10	7	10	2	2
9	8	9	3	3
8	9	8	4	4

转换算法按照这种参数选择完成。我们应用的结果是冗余度是 4，指纹强健度是 4，并应用了纠错编码、加密和感官模型。版权信息按照要求的鲁棒性，保密性和透明性嵌入到了压缩视频流中。转换算法满足了用户和计算参数之间的相关选择[9]。

2　数字指纹实现算法的一种电子商务应用方案

根据部分 1 的实现算法，提出一种 online-shop 的水印和指纹技术应用问题。其应用模型如图 3 所示。

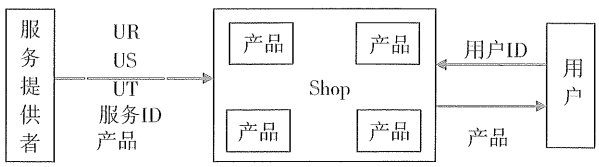

图 3　一种 online-shop 的指纹技术应用

Fig. 3　Digital fingerprinting technology application of online-shop

在 online-shop 的指纹技术应用中[10]，需要进

行三步识别操作：

（1）服务内容提供者（Content Provider，CP）：使用 online-shop 告诉媒体数据和附加的水印功能以保护他的产品，他上传媒体文件并选择水印参数；

（2）用户（Customer）：用户浏览 online-shop 媒体文件，并键入一个用户 ID。这个 ID 注册并标识出了他要买商品的文件数据。嵌入 ID 到媒体数据中作为一个水印，水印使用的参数由 CP 确认的用户标识提供；

（3）online-shop：作为一种水印服务器。根据其功能，它负责提供对于 CP 的水印接口；同时，当用户下载要买的媒体文件内容时，它也要进行水印转换操作。

图 4 是目前实现的该系统一个界面说明。

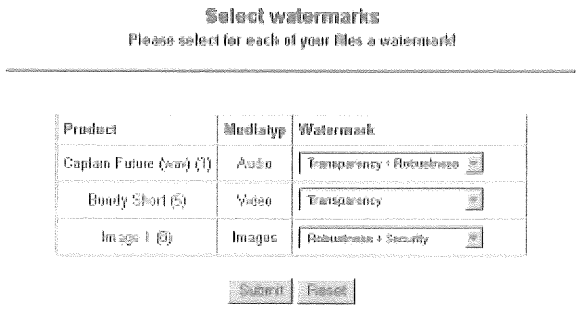

图 4 目前实现的系统一个界面

Fig. 4 Interface of the system

3 数字指纹接口的网络化应用方法

对于每个指纹或水印算法，由于其特定的应用情况不同，所以较难测试和评价它们的技术性能。所以，研究人员必须给出一些参数，满足鲁棒性、保密性和透明性之间的综合要求。这里，提出一种在 Peer-to-Peer（P2P）对等网络上进行的数字指纹服务方案。

3.1 数字指纹和 Peer-to-Peer 网络

Internet 的发展使各种不同类型的网络都可以进行交互。其中的一种形式是基于网络的服务，而另一种是 Peer-to-Peer 网络组[11-12]。Peer-to-Peer 网络支持文件共享的结果并不好。在 Peer-to-Peer 网络中，文件共享的主要问题就是内容的非法分配。音频，视频和图像经常通过这样的工具可以在 Peer-to-Peer 网络下载。由于此原因，多媒体内容提供者和商品服务商损失较大。而另一方面，用户却喜欢使用 Peer-to-Peer 网络。图 5 说明了一种 Peer-to-Peer 网络的组织结构。

在这种结构中，Peer-to-Peer 网络不关心是否某一端被丢失，因为，服务内容不只存储在一个机器中，它可以通过许多端口进行服务内容分配。一个重要的问题是在 Internet 上如何找到数字指纹标识的文件和如何识别非法复制拷贝。如果一个服务商用用户 ID 标识了每个文件，那么就可以识别用户。在 Peer-to-Peer 网络中，很容易找到一个特殊文件，因为它对其它用户也共享。服务商通过文件在网络位置返回的一个结果列表，他能下载 Peer-to-Peer 客户文件并能检测数字水印。如果数字指纹能被检测到并能正确恢复，因为有了嵌入的信息，服务商就知道了这个用户。

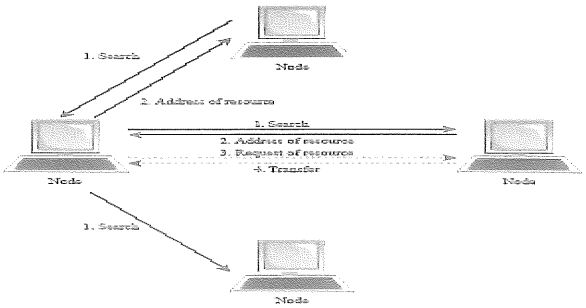

图 5 一种 Peer-to-Peer 网络服务应用

Fig. 5 Application of peer-to-peer network service

3.2 数字指纹身份网络认证过程与协议分析

在 P2P 网络指纹认证系统中，为了保证指纹特征值这一重要信息不被非法用户所获得，采用数字签名技术来解决的。为了方便描述，我们在此对协议中采用的符号做如下定义：A 为用户，AS 为认证服务器，KU_{AS}为认证服务器公钥，T_{AS}为认证服务器的时限，N_A 为 A 的现时数据，F_A 为 A 的指纹特征值，ID_A 为 A 的标识。还需说明的是这里采用的是单向认证协议。基本协议如下：

（2）A 用自己标识的签名向认证服务器 AS 请求认证。使用签名技术能有效地阻止一个虚假认证服务器对用户 A 的欺骗性连接。因为只有合法的认证服务器才保存有用户的公钥，从而能验证这个签名来获得 ID_A 来为下面的认证过程来使用。

（3）认证服务器产生时限 T_{AS}，现时数据 N_A，并将自己的公钥 KU_{AS}、N_A 和时限 T_{AS}用用户 A 的公钥 KU_A 加密后返回给客户端的 A 用户。

（4）客户端 A 接受到认证服务器公钥、时限和现时数据 N_A，同时在客户端的指纹传感器读取

用户的指纹灰度图像，并获得指纹特征 F_A，把元组 $\{T_{AS}, N_A, F_A\}$ 用认证服务器的公钥 KU_{AS} 加密后发送给认证服务器。

安全性、数据的完整性、抗否认性和信息保密性是网络身份认证方案设计所必需考虑的问题。基于秘密信息的身份认证协议：保证通信认证可以防止第三方的重放攻击，但由于客户端密钥存储和管理存在问题（比如加密密钥用的口令容易被人窥视到，通信用的多个密钥管理难等）。基于生物特征的身份认证：能解决口令窥视和密钥管理难等问题，但很难阻止第三方的重放攻击。因而，本文提出的电子商务身份认证系统的解决方案，就是综合了前面所述的水印和指纹识别技术以及加密技术（数字签名）之后得到的。

4　基于 Peer-to-Peer 网络服务的指纹检测的实验结果

研究应用的指纹检测是在 Peer-to-Peer 网络服务中，利用有参考标识列表的拷贝中各个子设置参数之间的相关性进行操作的。设在加密帧 Y 中，n 个子设置的符号标识可表示为 $S_{\mathrm{REF},n} = [\hat{s}_1\ \hat{s}_2 \cdots\cdots \hat{s}_n]^{\mathrm{T}}$，$\hat{X}_{\mathrm{test}}$ 是修正恢复的拷贝。从 $\hat{X}_{\mathrm{test}}$ 中，建立一个符号矩阵 $S_{\mathrm{TEST},n}$，并使 $S_{\mathrm{TEST},n} = [\hat{s}_1\ \hat{s}_2 \cdots\cdots \hat{s}_n]^{\mathrm{T}}$。那么，其完全可以形成一个相关矩阵 R：

$$R = \frac{1}{M_B}[S_{\mathrm{REF},n} \cdot S^{\mathrm{T}}_{\mathrm{TEST},n}] \tag{2}$$

和一个自相关矢量：

$$C = |\ \mathrm{diag}(R)\ | = [\rho_1\rho_2 \cdots\cdots \rho_n]^{\mathrm{T}}, 0 \leqslant \rho_i \leqslant 1 \tag{3}$$

其中，M_B 是每个子设置中的平均系数数量。如果，$\rho_i \geqslant T_i$，那么子设置加密，其相应的视频帧内用“1”隐藏；否则，用“0”隐藏。这些连续隐藏的位置就构成了水印和指纹，它们和数据栈入口地址比较来确定可能的攻击非法用户。其门限就是设计参数 n，k，M_B 的一个函数。

对于 256×256 的灰度 Lena 图像，设 $n=25$，$k=6$，$M_B=200$。相应的加密和指纹嵌入图像的 PSNR 值分别是：$\delta_{p1}=22$ dB，$\delta_{p2}=34$ dB。把这些设置可以分别作为图像模糊和无法感觉细节性的低部和上部边界。图 6 显示了实验进行的原始图像，扰码图像和水印指纹图像。

图 6　原始图像，加密图像和嵌入水印指纹的图像（$n=25$，$k=6$，$M_B=200$）

Fig. 6　Original image, encryption image and imbedded digital fingerprinting image

表 2 说明了感官细节性 PSNR（$\hat{X}_{Fi}$），鲁棒性和载荷（C_k^n）之间的折中关系。水印指纹嵌入的图像应用了 JPEG 压缩（$Q=60$）；鲁棒性用误差检测的隐藏标识（P_e）的分数表示；载荷量通过增加 k 或 n 来实现；其差异性通过增加 M_B 实现。由表可见，增加 k 和 M_B 对嵌入指纹的图像质量有严重影响。为了在不损害鲁棒性前提下获得最低的保密性能（$\mathrm{PSNR}(Y) \leqslant \delta_{p1}=22$ dB），子设置宽度必须大于 100。而当 M_B 超过一定值，错误率迅速增加，这是由于子设置重叠引起的伪特征成分导致的结果[13]。

表 2　载荷量、鲁棒性和感官质量之间结果说明

Table 2　Results explanation between capacity, robustness and sensory quality

	$K=5$	$K=7$	$K=10$	PSNR (Y) /dB
	P_e, PSNR$(\hat{X}_{Fi})$	P_e, PSNR$(\hat{X}_{Fi})$	P_e, PSNR$(\hat{X}_{Fi})$	
$n=25$, $M_B=100$	1/5, 41	1/7, 37	1/10, 34	26
$n=25$, $M_B=200$	1/5, 38	1/7, 36	1/10, 29	22
$n=25$, $M_B=300$	1/5, 33	2/7, 33	1/10, 28	21
$n=25$, $M_B=400$	2/5, 31	2/7, 31	2/10, 26	20

5　结　论

本文在电子商务方案中引入了一种数字指纹一体化实现算法，并根据 DRM 对 VOD 服务要求，能够把单个和多个用户要求转换为适合用户的水印指纹参数进行设置。作为研究结果，描述了 online-

shop 的水印指纹技术应用方式和数字水印指纹在 Peer-to-Peer 网络中应用的方式。为了数字水印指纹在多用户环境下合理应用，需要进一步研究算法来设置查找表 Look-Up 的实现策略。未来的这一领域将会是重要的和有趣的。

参考文献：

[1] MICHAEL Miller. Discovering P2P, sybex-verlag[M]. USA: John Wiley & Sons, Inc. , 2001.

[2] KUNDUR D, KARTHIK K. Video fingerprinting and encryption principles for digital rights managrment[J]. proceedings of the IEEE, 2004, 92(6): 918 - 932.

[3] BLOOM Cox, Miller. Digital Watermarking[M]. San Diego: Academic Press, 2002.

[4] TRAPPE W, WU M, WANG Z J, et al. Anti-collusion fingerprinting for multimedia[J]. IEEE Trans. Signal Processing, 2003, 51: 1069 - 1087.

[5] MACQ M B, QUISQUATER J. Crytology for Digital TV broadcasting[J]. Proc. IEEE, 1995, 83: 944 - 957

[6] BLOOM J. Security rights management in digital cinema [J]. Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, 2003, 4: 712 - 715.

[7] ANDERSON R, MANIFAVAS C. Chameleon-a new kind of stream cipher[M]// Lecture Notes in Computer Science, Fast Software Encryption. E. Biham, Ed. Heidelberg, Germany: Springer-Verlag, 1997: 107 - 113.

[8] CHANG Y, HAN R, LI C, et al. Secure transcoding of internet content[C]//Proc. Int. Wor-kshop Intelligent Multimedia Computing and Networking(IMMCN), 2004: 940 - 943.

[9] DITTMANN J, BEHR A, STABENAU M, et al. Combining digital watermarkings and collusion secure fingerprints for digital image[C]// In proc. SPIE. Conf. Electronic Imaging99. Security and Watermarking of Multimedia Contents, 1999, 41: 171 - 182.

[10] WANG Z J, WU Min, ZHAO Hong, et al. Resistance of orthogonal gaussian fingerprints to collusion attacks[C]. IEEE International Conference on Acoustics, speech & Signal Processing, 2003: 6 - 10.

[11] COX I, KILLIAN J, LEIGHTON F, et al. Secure spread spectrum watermarking for multimedia[J]. IEEE Trans. On Image Processing, 1997, 6(12): 1673 - 687.

[12] WANG Z J, WU M, TRAPPE W, et al. Group-oriented fingerprinting for multimedia forensics[J]. EURASIP Journal on Applied Signal Processing, 2004, 14: 2153 - 2173.

[13] HARTUNG F, GIROD B. Digital watermarking of MPEG - 2 coded video in the bitstream domain[J]. Proc. Int. Conf. Acoustics, Speech and Signal Processing, 1997, 4: 2621 - 2624.

（上接第40页）

[6] GU Y, NARENDRAN N. A non-contact method for determining Junction temperature of phosphor converted white LEDs[C]// Third international conference on solid state lighting. Proceedings of SPIE, 2004, 5187: 107 - 114.

[7] EDILSON M, FERNANDO L, ANTUNES M. Junction temperature estimation for high power light-emitting diodes [C]. IEEE 2007: 3030 - 3035.

[8] XI Y S. Junction-temperature measurement in GaN ultraviolet light-emitting diodes using diods forward voltage method[J]. Appl Phys Lett, 2004, 85 (12): 2163 - 2165.

[9] JAYASINGHE L, GU Y, NARENDRAN N. Characterization of thermal resistance coefficient of high-power LEDs [C]//Sixth international conference on solid state lighting. Proceedings of SPIE, 2006, 6337: 10 - 20.

[10] HONG E, NARENDRAN N. A method for projecting useful life of LED lighting systems[C]// Third international conference on solid state lighting. Proceedings of SPIE, 2004, 5187: 93 - 99.

[11] NARENDRAN N, GU Y, HOSSEINZADEH R. Estimating junction temperature of high-flux white LEDs[C]// Light-Emitting Diodes: research, manufacturing, and application VIII. Proceedings of SPIE, 2004, 5366: 158 - 161.

[12] 苗庆海，朱阳君，张兴华，等. pn 结中的小电流过趋热效应及理论模拟计算[J]. 半导体学报, 2006, 27(9): 1595 - 1599.
MIAO Qinghai, ZHU Yingjun, ZHANG Xinghua, et al. Excessive thermotaxis effect of low current in pn junction and theoretical analog calculation[J]. China J. Semicond, 2006, 27(9): 1595 - 1599.