一类SVD域水印问题分析及改进算法

蒋天发[1] 熊祥光[2] 蒋 巍[3]
(中南民族大学计算机科学学院 武汉 430074)[1] (贵州师范大学数学与计算机科学学院 贵阳 550001)[2]
(中国软件评测中心(CSTC) 北京 100048)[3]

摘 要 分析了一类SVD域图像水印算法存在过高虚警率的原因,并给出了相应的实验结果。在此基础上,提出了一种混合DWT和SVD的图像水印算法。算法先将载体图像划分为互不重叠的块,并对每一块进行1层DWT分解,再对低频子带进行SVD分解。采用量化的方法,将Arnold置乱处理后的水印图像嵌入到SVD分解后的奇异值之中。实验表明,提出的算法克服了传统的SVD图像水印算法存在的虚警问题,对常见的信号处理如JPEG压缩、滤波、噪声等具有较好的鲁棒性。

关键词 图像水印,奇异值分解,虚警错误
中图法分类号 TP391.41 **文献标识码** A

Analysis of Problem in SVD Domain Watermarking and Improved Algorithm

JIANG Tian-fa[1] XIONG Xiang-guang[2] JIANG Wei[3]
(School of Computer Science, South-Central University for Nationalities, Wuhan 430074, China)[1]
(School of Mathematics and Computer Science, Guizhou Normal University, Guiyang 550001, China)[2]
(China Software Test Center, Beijing 100048, China)[3]

Abstract The reasons of high false-positive detection rate problem for a class of singular value decomposition(SVD) based image watermarking algorithms were analyzed and the corresponding results were given. On this basis, a novel watermarking algorithm based on discrete wavelet transform(DWT) and SVD was proposed. First the host image is divided into non-overlap blocks and each block is applied 1-level DWT, and then SVD on the low-frequency sub-band is made. The watermarking is preprocessed by Arnold transform and then is embedded into the singular values of the low-frequency sub-band based on quantization method. Experiments show that the proposed algorithm can overcome the high false-positive detection rate problem which exists in the traditional watermarking algorithm based on SVD and robust against common signal processing such as JPEG compression, filtering, and the adding of noise.

Keywords Image watermarking, Singular value decomposition, False alarm errors

1 引言

随着计算机网络技术和数字技术的飞速发展,非法的拷贝、访问和篡改数字媒体已成为一个迫切需要解决的问题[1]。为了解决这个问题,人们提出了数字水印的概念。图像奇异值分解后的奇异值由于具有良好的抗攻击能力,因此,不少学者提出了基于空域SVD或变换域SVD的水印方法。2002年,Liu和Tan最先提出基于SVD的图像水印算法,该方法将水印嵌入原始图像进行SVD分解后的奇异值中[2]。他们认为该算法数学背景清晰,是一种很有前途的方法。文献[3]提出一种基于DWT和SVD的水印算法,该算法先对载体图像进行3层小波变换,再对低频子带进行SVD分解,将混沌置乱后的水印图像的奇异值嵌入载体图像SVD分解后的奇异值中。文献[4]提出一种基于奇异值分解的水印算法,水印嵌入载体图像经奇异值分解后的奇异值之中,利用SVD的代数性质,证明了嵌入水印的图像在遭到缩放、平移、旋转、转置等几何攻击后,奇异值具有良好的不变性,为此算法提供了理论依据。文献[5]提出一种基于分块奇异值分解的数字水印算法,但该算法未生成真正的水印图像,不具备实用性。文献[6]先对载体图像进行n层离散小波分解,选择低频子带生成参考图像,再对该参考图像和水印图像分别进行SVD分解,利用水印图像的奇异值修改参考图像的奇异值,从而完成水印的嵌入。从以上文献给出的实验结果来看,该类算法对压缩、旋转、剪切等攻击具有较好的鲁棒性,具有一定的现实意义。但是,该类算法就本质而言,只是将Liu和Tan的方法简单地扩展到变换域。算法要么直接将水印图像嵌入到载体图像经奇异值分解后的奇异值向量中,要么将水印图像的奇异值向量嵌入到载体图像的奇异值向量中。水印提取时,都需要原始水印的相关信息。因此,笔者认为该类算法是有问题的。通过实验发现,利用该类方案的水印提取算法,可从未嵌

本文受国家民委重点科研项目(Mzy02004)和湖北省教育厅科研项目(B20110804,B20110807)资助。
蒋天发(1954—),男,教授,研究生导师,主要研究方向为网络信息安全和数字水印,E-mail:jiangtianfa@163.com;熊祥光(1984—),男,硕士,助教,主要研究方向为网络信息安全和数字水印;蒋 巍(1980—),男,硕士,主要研究方向为信息安全评测以及数字水印技术。

入任何水印的载体图像中提取出高度相关的水印信号，即水印的虚警率偏高，由提取算法提取出来的水印信号不具有真实性。

鉴于此，本文先简要描述该类算法和分析该类算法存在漏洞的原因，并给出相应的实验结果，然后提出一种混合 DWT 和 SVD 的数字图像水印算法。算法先将载体图像进行 1 层 DWT 分解，再对低频子带 LL 进行 SVD 分解。嵌入时，采用量化的方法，将 Arnold 置乱处理后的水印图像嵌入到 SVD 分解后的奇异值之中。实验表明，提出的算法解决了传统的 SVD 图像水印算法虚警率过高的问题，能抵抗常见的信号处理攻击。

2 一类 SVD 域图像水印算法及伪提取分析

基于 SVD 的水印算法最先是由 Liu 和 Tan 提出的。虽然在实际的应用中，可能会先对载体图像和水印信号进行某种变换后再选择某个子带进行 SVD 分解，但此处忽略此类变换的描述，只对水印算法的关键过程进行描述，因此可将基于 SVD 的图像水印算法分为：

1）只对载体图像进行 SVD 分解，水印直接按加性或乘性（限于篇幅，这里只介绍加性的嵌入方式）的叠加方式嵌入到奇异值矩阵之中。按加性叠加方式嵌入水印的过程为：

$$\begin{cases} I \Rightarrow USV^T \\ S+\alpha W \Rightarrow U_W S_W V_W^T \\ I_W \Leftarrow US_W V^T \end{cases} \tag{1}$$

文献[2]中的水印算法属于此类，相应的提取过程为：

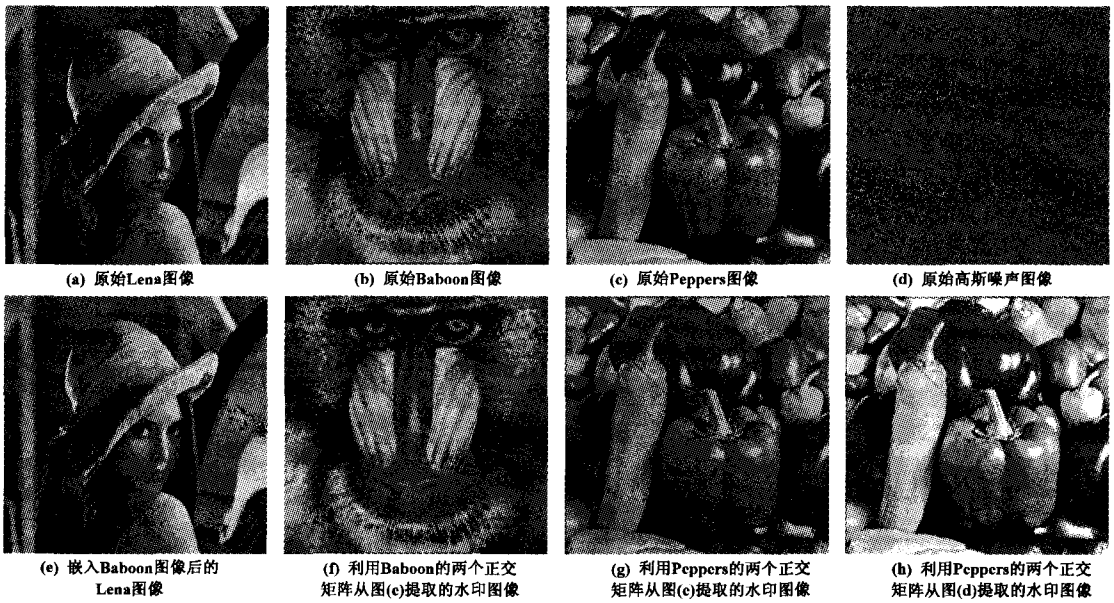
$$\begin{cases} I_W^* \Rightarrow U_W^* S_W^* V_W^{*T} \\ D^* \Leftarrow U_W S_W^* V_W^T \\ W^* \Leftarrow (D^* - S)/\alpha \end{cases} \tag{2}$$

2）对载体图像和水印都先进行 SVD 分解，然后按加性或乘性的嵌入方式将水印的奇异值叠加到载体图像的奇异值上。即：

$$\begin{cases} I \Rightarrow USV^T \\ W \Rightarrow U_W S_W V_W^T \\ S+\alpha S_W \Rightarrow S_W' \\ I_W \Leftarrow US_W' V^T \end{cases} \tag{3}$$

文献[3,5,6]中的水印算法属于此类，相应的提取过程为：

$$\begin{cases} I_W^* \Rightarrow U_W^* S_W^* V_W^{*T} \\ D^* \Leftarrow U_W S_W^* V_W^T \\ W^* \Leftarrow (D^* - U_W S V_W^T)/\alpha \end{cases} \tag{4}$$



(a) 原始Lena图像　(b) 原始Baboon图像　(c) 原始Peppers图像　(d) 原始高斯噪声图像

(e) 嵌入Baboon图像后的Lena图像　(f) 利用Baboon的两个正交矩阵从图(e)提取的水印图像　(g) 利用Peppers的两个正交矩阵从图(c)提取的水印图像　(h) 利用Peppers的两个正交矩阵从图(d)提取的水印图像

图 1　一类 SVD 水印算法伪提取结果

注意到上述算法在水印的提取过程中都需要 U_W，V_W，S 和 α。众所周知，奇异值分解后的 S 矩阵仅仅是个对角矩阵，而正交矩阵 U_W 和 V_W 几乎包含了图像的所有结构信息，同时奇异值向量与图像之间不存在一一对应的关系，不能刻画图像的几何结构，只是决定了图像在不同特征图像下的亮度信息。若将 U_W 和 V_W 的列向量分别记为 $U_W^{(p)}$ 和 $V_W^{(p)T}$，则式(2)和式(4)中的 D^* 可改写为：

$$D^* \Leftarrow \sum U_W^{(p)} V_W^{(p)T} s_n^* \tag{5}$$

式中，s_n^* 是 I_W^* 的奇异值。式(5)表明，U_W 和 S_W 决定了 D^* 的几何结构，s_n^* 只决定了特征图像 $U_W^{(p)} V_W^{(p)T}$ 在重构 D^* 时的权重[7]。因此，若在提取水印时需要两正交矩阵，则与任意图像的奇异值向量合成，总可重构出一幅与原始水印图像结构非常相似的图像。也就是说，这类水印算法存在的虚警率问题是显而易见。下面将以文献[2]中的算法进行实验验证（因为其他文献中的算法都是在文献[2]的基础上进行扩展的）。实验选取标准测试图像 Lena 和由[0,255]区间的均匀分布噪声生成的图像作为载体图像，Peppers 和 Baboon 作为水印图像，如图 1(a)－图 1(d)所示，其大小都为 512×512。嵌入 Baboon 后的 Lena 图像如图 1(e)所示，满足不可感知性的要求，图 1(f)是利用 Baboon 的两个正交矩阵从图 1(e)提取的水印图像，图 1(g)和图 1(h)是利用 Peppers 的两个正交矩阵分别从图 1(e)和图 1(d)提取的水印图像。

从实验结果我们看到，使用某幅图像（图 1(c)，该图像不是嵌入的水印图像）奇异值分解后的两个正交矩阵，该类算法会从一幅（图 1(a)）已嵌入另一幅水印图像（图 1(b)）的图像中提取出该图像（图 1(c)）的近似版本（图 1(g)）或从一幅未

嵌入任何水印的图像(图 1(d))中提取出某幅图像(图 1(c))的近似版本(图 1(h))。这显然不符合水印信息只能从真正嵌入了水印的载体作品中提取出的要求。因此,该类算法存在致命的漏洞,这与理论分析是相一致的,类似的问题也出现在文献[8]中。不过,并不是所有基于 SVD 的水印算法都具有过高虚警率。下面将提出一种克服了过高虚警率问题的混合 DWT 和 SVD 的图像水印算法。

3 混合 DWT 和 SVD 的图像水印算法

根据上述对该类水印算法的详细分析,可知引起该类算法虚警率过高原因是在水印的提取过程中需要用到 U_W 和 V_W 矩阵。因此,如果在设计水印提取算法时不使用 U_W 和 V_W,那么是可以解决此类算法过高虚警率问题的。在此,提出一种混合 DWT 和 SVD 的新的水印算法。该算法首先对载体图像进行离散小波分解,选取低频子带 LL 作为待嵌入水印的区域,其次对该区域进行 SVD 分解,将 Arnold 置乱处理后的水印图像嵌入到 LL 子带 SVD 分解后的奇异值中。具体的水印嵌入过程如下:

1)为了增强水印图像 W 抵抗恶意攻击的能力,水印图像嵌入前先采用 Arnold 变换进行置乱处理,进而提高水印信息的安全性和增强恶意攻击的能力。

2)将载体图像划分成互不重叠的大小为 16×16 的子块,对每一子块进行 1 层小波分解,选取低频子带 LL 作为待嵌入水印的子带,并对该子带进行 SVD 分解。

3)按如下的规则修改 LL 子带 SVD 分解后的最大的奇异值 $\lambda(i)$:

$$\begin{cases} \lambda(i)=\lambda(i)-\mathrm{mod}(\lambda(i),Q)-Q/4, \\ \quad \text{if } w(i)=1, \mathrm{mod}(\lambda(i),Q)<=Q/4 \\ \lambda(i)=\lambda(i)-\mathrm{mod}(\lambda(i),Q)+3*Q/4, \\ \quad \text{if } w(i)=1 \ \mathrm{mod}(\lambda(i),Q)>Q/4 \\ \lambda(i)=\lambda(i)-\mathrm{mod}(\lambda(i),Q)+5*Q/4, \\ \quad \text{if } w(i)=0 \ \mathrm{mod}(\lambda(i),Q)>=3*Q/4 \\ \lambda(i)=\lambda(i)-\mathrm{mod}(\lambda(i),Q)+Q/4, \\ \quad \text{if } w(i)=0 \ \mathrm{mod}(\lambda(i),Q)<3*Q/4 \end{cases} \tag{6}$$

式中,Q 是水印的嵌入强度,影响水印的不可感知性和鲁棒性,mod(·)是求余运算。

4)使用修改后的奇异值进行逆 SVD 变换,得到嵌入水印后的 LL 子带,再使用逆 DWT 变换,得到每一子块图像,最后将这些字块图像合成为最终嵌入水印后的图像。

水印的提取过程与嵌入过程很相似,是嵌入过程的逆过程。具体的提取过程如下:

1)将含水印的图像 I^*(可能已受到某种攻击)划分成互不重叠的大小为 16×16 的子块,对每一子块进行 1 层小波分解,选取低频子带 LL 作为待提取水印的子带,并对该子带进行 SVD 分解。

2)按下式提取水印:

$$\begin{cases} w(i)^*=1, & \text{if } \mathrm{mod}(\lambda(i)^*,Q)>Q/2 \\ w(i)^*=0, & \text{else} \end{cases} \tag{7}$$

3)使用 $w(i)^*$ 重构水印图像,并使用相应的密钥解调即得到最终提取的水印图像。

4 实验结果与分析

为了验证所提算法的性能,我们在 Windows XP 操作系统和 Matlab7.1 环境下进行了实验。实验采用的原始图像为 512×512 的 Lena 图像和 Peppers 图像,如图 2(a),图 2(b)所示。原始水印采用了 32×32、带有"中南民大"和"IT"标识的二值图像,如图 3(a),图 3(b)所示。图 2(c)是嵌入图 3(a)水印后的图像,图 2(d)是嵌入图 3(b)水印后的图像。从主观视觉上看,两者几乎没有差异,水印的不可感知性良好。采用峰值信噪比(PSNR)来客观评价嵌入水印图像的质量,实验表明,PSNR 都在 40 以上。

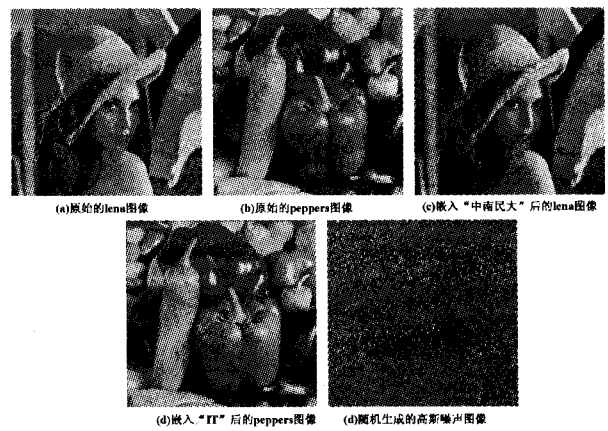


图 2 原始图像和嵌入水印后的图像

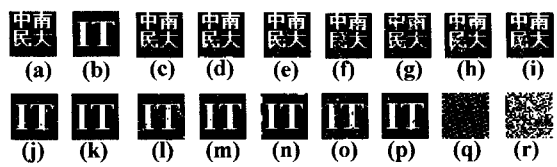


图 3 原始的水印和提取的水印

为了考察算法的鲁棒性能,分别对嵌入水印后的图像分别进行不同品质百分数的 JPEG 2000 压缩、滤波、添加噪声等处理。对图 2(c)和图 2(d)分别作品质百分数 10%、20%～80%的 JPEG 2000 有损压缩,图 3(c)和图 3(d)是图 2(c)JPEG 压缩(品质百分数分别为 30%,50%)处理后提取的水印图像,图 3(j)和图 3(k)是图 2(d)JPEG 压缩(品质百分数分别为 30%,50%)处理后提取的水印图像。图 3(e)－3(g)是对图 2(c)分别进行中值滤波、维纳滤波和高斯滤波攻击后提取的水印图像。图 3(l)－3(n)是对图 2(d)分别进行中值滤波、维纳滤波和高斯滤波攻击后提取的水印图像。图 3(h)－3(i)是对图 2(c)分别进行椒盐噪声和乘性噪声处理后提取的水印图像。图 3(o)和 3(p)是对图 2(d)分别进行椒盐噪声和乘性噪声处理后提取的水印图像。图 3(q)和图 3(r)分别是解调时密钥不正确和从图 2(e)中提取的水印。从以上实验结果可以看出,密钥不正确是不能正确提取出水印的,在未嵌入水印的载体图像中也是不能提取出水印的,算法的虚警率低,同时对普通的图像处理具有较好的鲁棒性。

结束语 本文对一类 SVD 域数字图像水印算法存在虚警率过高的问题进行了分析,并指出了该问题存在的根本原

因是在提取水印时需要利用在嵌入水印时生成的两个决定图像几何结构的正交矩阵，而奇异值只是决定了特征图像在重构图像中的权重。因此为了克服该类算法存在较高的虚警率问题，后续的水印算法设计应另辟蹊径，而不应再沿用这类算法思想。改进的水印算法采用量化的嵌入方式将预处理后的水印图像嵌入原始图像经 DWT 和 SVD 分解后的奇异值中，提取时不需要原始水印的参与，是一种盲水印技术。实验表明，改进算法解决了典型的 SVD 水印算法过高虚警率的问题，具有较高的安全性、透明性及抗攻击的能力。

参 考 文 献

[1] 熊祥光，杨锦尊，崔巍，等. 基于三维小波变换和 HVS 的视频水印算法[J]. 武汉大学学报：工学版，2010，43(3)：357-360

[2] Liu R，Tan T. An SVD-based watermarking scheme for protecting rightful ownership [J]. IEEE Transactions on Multimedia，2002，4(1)：121-128

[3] 张秋余，李凯，袁占亭. 基于混沌和 SVD-DWT 的稳健数字图像水印算法[J]. 计算机应用研究，2010，27(2)：718-720

[4] 周波，陈健. 基于奇异值分解的、抗几何失真的数字水印算法[J]. 中国图象图形学报，2004，9(4)：506-512

[5] Shieh J-M，Lou D-C，Chang M-C. A semi-blind digital watermarking scheme based on singular value decomposition [J]. Computer Standards and Interfaces，2006，28：428-440

[6] Bhatnagar G，Raman B. A new robust reference watermarking scheme based on DWT-SVD [J]. Computer Standards & Interfaces，2009，31：1002-1013

[7] Roman R. Comment on an SVD-based watermarking scheme for protecting rightful ownership[J]. IEEE Transactions on Multimedia，2007，9(2)：421-423

[8] 周鹏颖，沈磊，田小林，等. 基于小波—奇异值分解的数字水印新算法[J]. 计算机应用研究，2010，27(5)：1896-1897

(上接第 52 页)

表 3 存储开销

	GKMP	HFMKM
GC 存储开销	$(n+1)K$	$(N+1)K+C_p$
成员存储开销	$2K$	$2K+\frac{C_p}{n}$

其中，n 为组规模(成员数量)，C_e 为一次加/解密的计算开销，C_r 为 GC 生成一个新密钥的计算开销，C_p 为计算 $S(t_{i,j})$和 $T_{i,j}(r)$组成的数据包的平均计算开销，C_s 为成员更新一次组密钥的计算开销，K 为密钥大小(比特)。

从以上分析可以看出，HFMKM 方案在更新开销和计算开销方面有一定优势；存储开销方面，组成员的开销稍微增加可以带来 GC 的存储开销的减少，从而在一定程度上减轻 GC 的负担。

4.3 方案优势

与典型的集中式组播密钥管理[4]不同，方案中 GC 与各个成员之间的关系不是简单的主次关系，组密钥由 GC 以及每个合法成员各自对等地产生，而不是由 GC 产生后再由会话密钥加密分发给各成员，这样就避免了组密钥在传输过程中的泄漏。

对于每个组成员，其组密钥的生成依赖于自身存储的哈希值(或哈希种子)和密钥更新因子，融合了集中式与分布式组密钥管理的双重特性，从而极大地提高了安全性，非常适合于安全需求较高的组播通信。

在组密钥生成阶段和每个成员的加入过程中都仅使用一次会话密钥就可确保后续的安全组播通信，这也使得通信开销有所降低。对多项式求值的运算由 GC 完成，不给成员节点带来负担；在成员节点的运算开销方面，对哈希函数和二元单向函数的运算具备很好的单向性，而且其计算开销不大，带来更好的安全性，同时不增加过多的计算开销。

另外，删除成员的组密钥更新方法的一个显著优点是：可以很方便地一次性删除多个成员。例如，若一次性要删除的成员为 $P_1, P_2, \cdots, P_l$，则只需将 $I(r)$更新为 $I'(r)=I(r)\cdot(r-r_1)\cdot(r-r_2)\cdots(r-r_l)$即可。

结束语 组密钥管理是安全组播通信的前提。传统的许多集中式平面型组密钥管理方案将几乎所有计算、更新、传输等操作任务归于 GC，在带来管理方便的同时也存在一定风险。本文正是基于此，设计出另一种由各组成员与 GC 平等地生成组密钥的密钥管理模型，旨在探索出一种新的组密钥管理体制。本方案体现出集中式、分布式与验证性的统一，是一种新型的、安全可靠的集中式平面型组播密钥管理方案。当然，如何将 GC 的各项开销继续缩小以及如何优化对数据的分组接收模式，是需要进一步研究的问题。

参 考 文 献

[1] 王琳，解冲锋，杨明川. IP 组播的关键技术 [J]. 信息网络，2003(01)：28-33

[2] 赵膺，宋佳兴，徐万鸿，等. 安全组播综述 [J]. 小型微型计算机系统，2003，24(10)：1873-1877

[3] Eskicioglu A M. Multimedia security in group communications：Recent progress in key management，authentication，and watermarking [J]. ACM Multimedia Systems，Special Issue on Multimedia Security，September 2003：239-248

[4] Harney H，Muckenhirn C. Group key management protocol (GKMP) specification[S]. RFC2093. 1997

[5] Suvo M. Iolus：A framework for scalable secure multicasting [J]. ACM SIGCOMM Computer Communication Review，1997，27(4)：277-288

[6] 李国民，何大可. 基于身份的认证群密钥协商协议 [J]. 计算机科学，2009，36(01)：60-64

[7] 孙海波，张权，唐朝京. 基于密钥矩阵的组播密钥管理方案 [J]. 计算机工程，2008，34(21)：112-114

[8] 柳秀梅，周福才，常桂然，等. 使用双线性配对实现组播密钥管理协议 [J]. 东北大学学报：自然科学版，2009，30(08)：1119-1123

[9] 吕远方. 基于秘密共享的无线传感器网络组密钥管理方案 [J]. 微计算机应用，2010，31(03)：35-41

[10] 许建真，董永先，梁克会. 一种高效的动态组播密钥管理方案 [J]. 计算机应用研究，2010，27(03)：1061-1063