基于 DWT-SVD 域的彩色图像自适应水印算法*

方旺盛, 张 蓉
(江西理工大学 信息工程学院, 江西 赣州 341000)

摘 要: 为了保护数字彩色图像版权,提出了一种结合离散小波变换(DWT)和矩阵奇异值分解(SVD)的彩色图像自适应水印算法。其主要设计思想是:先将原 RGB 彩色图像的各颜色分量进行小波分解;再将得到的中、低频带的小波系数与原水印图像分别进行奇异值分解,水印信息的奇异值重复嵌入到三通道中、低频带的小波系数奇异值中,且利用临界视觉阈值与奇异值之间的关系对水印嵌入强度作自适应调节,从而达到增强水印鲁棒性和确保水印透明性的目的。本算法适用于二值及灰度水印,在二值水印的提取过程中需设定一个提取阈值,以保证提取水印的完整性。仿真结果说明本算法对水印系统的透明性与鲁棒性作了较好的协调,是一种较稳健的算法。

关键词: 离散小波变换; 奇异值分解; 彩色图像; 人类视觉系统; 视觉临界阈值
中图分类号: TP391.41 **文献标志码**: A **文章编号**: 1001-3695(2012)11-4323-04
doi:10.3969/j.issn.1001-3695.2012.11.083

DWT-SVD based adaptive color image watermarking

FANG Wang-sheng, ZHANG Rong
(*School of Information Engineering*, *Jiangxi University of Science & Technology*, *Ganzhou Jiangxi* 341000, *China*)

Abstract: This paper proposed a color image adaptive watermarking algorithm combined DWT and SVD for copyright protection of digital color image. Firstly decomposing the color component of the original RGB color image using discrete wavelet transform respectively, it applied the SVD to HL, LL band and the watermarking alone, then embedded the same watermarking data into three channel by modifying the two band's singular values. The additional advantage of the proposed technique was taking advantage of the relationship between HVS and JND which could adaptively regulate the watermark embedding strength, so as to achieve the purpose of enhance the robustness and ensure transparency of watermark. The algorithm was suitable for binary and grayscale watermark, an extraction threshold value should be set in the binary watermark extraction process, to ensure the integrity of the extracted watermark. Simulation results show this algorithm is a more robust algorithm and better coordination the transparency and robustness of the watermarking system.

Key words: discrete wavelet transform(DWT); singular value decomposition(SVD); color image; human visual system(HVS); just noticeable distortion(JND)

0 引言

数字彩色图像种类繁杂,数量繁多,但是有许多图像处理工具能够方便快捷地对这些数据进行非法复制和修改。为防止这一现象的发生,必须采用一些机制来保护数字彩色图像数据。其最主要的方式就是采用图像数字水印技术。

国内外不少学者提出了结合 DWT 和 SVD 的图像水印算法。林旭亮等人[1]提出了一种将水印的奇异值嵌入到载体图像的小波域系数中从而得到含水印的图像。实验分析表明,该算法具有较好的透明性,对常见的 JPEG 压缩、滤波、剪切、叠加噪声等攻击具有较强的鲁棒性。Al-haj[2]提出的算法中,对图像进行三级小波分解后获得包括低频、水平、垂直、对角线等十个频段,并且分别对这十个频段进行奇异值分解,通过小幅度的修改奇异值来完成水印信息的嵌入。徐慕蓉等人[3]提出一种基于 HVS 和 SVD 的小波域的新算法,实验结果表明该算法在抗多种攻击中具有更好的鲁棒性。但上述算法都是针对灰度图像而不适合用于彩色图像,即使载体图像是彩色的,大部分也是通过提取其亮度信息或使用单色通道的信息。本文考虑到 RGB 彩色图像中所有颜色分量相关性较高故将信息重复隐藏在 RGB 三个通道中,且通过分析 SVD 与 JND 阈值之间的关系确定奇异值的修改幅度,从而对水印嵌入强度作自适应调节,以达到确保水印保真度的同时不降低水印鲁棒性的目的。

1 算法原理

就信息隐藏而言,可以被划分为两类,即一类通过改变图像的强度值,另一类则是改变图像的像素值或频率组成。前者被称为空间域技术,后者被称为频率域技术。为了获得一个图像频率成分,需要使用任何一个如离散傅里叶变换(DFT)、离散余弦变换(DCT)以及小波变换(DWT)等的变换工具。本文选定在小波域中进行水印的嵌入,因为其不仅具有多分辨率分析特点,并能很好地结合人眼视觉系统,所以可以在 DWT 域

收稿日期: 2012-04-07; **修回日期**: 2012-05-27 **基金项目**: 国家自然科学基金资助项目(11062002);江西省自然科学基金资助项目(2010GZS0083);江西省教育厅科技项目(GJJ11470)

作者简介: 方旺盛(1963-),男,江西上饶人,教授,硕导,硕士,主要研究方向为数字水印、无线传感器网络(fangwangsheng@163.com);张蓉(1986-),女,硕士,主要研究方向为数字水印.

各系数中建立较为精准的视觉临界阈值,而小波基函数和小波变换分解级数的选择更是给小波变换域水印算法的设计带来了很大的灵活性和优越性。

矩阵论中基于矩阵分解理论的奇异值分解(SVD)是一种特殊的矩阵变换。图像奇异值具有以下三个特性[4]:a)SVD 图像具有很好的稳定性,这就意味着当一个较小的值被添加进图像,图像的奇异值不会有大的变化,而这并不会大范围地影响图像质量;b)SVD 图像能够有效地代表图像的内在代数性质,其中的奇异值和图像的亮度相关联,而奇异值特征向量则能够反映图像的几何特征;c)一个图像矩阵除了有最大奇异值以外还有许多小的奇异值,与最大奇异值相比即使忽略这些小奇异值的重建也不影响图像重建的质量。任何图像都可以被视为一个无损特性的几何方阵,因此,SVD 技术可以应用到任何图像。

本文将两种方法结合起来,克服了单独使用小波变换造成的不可见性下降和单独使用奇异值分解导致的鲁棒性差的问题,在各颜色通道的低频和中高频部分重复嵌入水印既保证了水印提取的完整性,也能有效地防止单色攻击。此外,本文为了提高水印系统的鲁棒性,在水印嵌入之前对其进行置乱的预处理,并引入 HVS 模型对水印的嵌入强度作自适应的调节。

2 JND 和 SVD 的关系

通过研究人类视觉系统对于图像的感知特点,建立精准的 HVS 数学模型,从而计算出准确的 JND 阈值,对于保证水印化图像的保真度及提高水印系统的稳健性都具有很重大的意义。

由于本文利用低频子带和垂直子带的奇异值矩阵中嵌入水印信息,故 JND 值不能直接当做嵌入强度使用,将阮波[5]提出的灰度图像中的奇异值修改权值的方法使用在彩色图像的三个通道。假设任意给定图像的矩阵 $\boldsymbol{A}\in \mathrm{R}^{M\times N}$,$\delta_{\sigma_i}$ 表示的是修改后的第 i 个奇异值与原奇异值之间的差值,JND(x,y) 表示的则是小波域中用于水印嵌入的子带视觉临界阈值。要保持水印化图像的透明性,必须保证奇异值的改变给原图像造成的影响不足以引起视觉感知,那么奇异值的修改幅度 $|\delta_{\sigma_i}|$ 必须符合式(1)的条件。

$$|\delta_{\sigma_i}|\leqslant\frac{\mathrm{JND}(x,y)}{|u_i v_i^{\mathrm{T}}(x,y)|}\quad(0\leqslant x\leqslant M,0\leqslant y\leqslant N) \tag{1}$$

考虑到奇异值矩阵中的最大奇异值 σ_1 拥有不可替代的重要性,因此用 σ_1 来限制嵌入强度。本文中水印的嵌入强度 α_s 计算式为

$$\alpha_s=\frac{|\delta\sigma_{s1}|}{S_{w'}(1,1)}=\frac{\min\limits_{0\leqslant x\leqslant N,0\leqslant y\leqslant M}\left\{\dfrac{\mathrm{JND}_r^s(i,j)}{|u_{s1}v_{s1}^{\mathrm{T}}|(i,j)}\right\}}{S_{w'}(1,1)} \tag{2}$$

其中:$S\in\{\mathrm{LL},\mathrm{LH},\mathrm{HL},\mathrm{HH}\}$,$\delta\sigma_{s1}$ 表示每个用于水印嵌入的各子带的最大奇异值的修改幅度;$S_{w'}(1,1)$ 表示经预处理后的隐秘信息的最大奇异值。

为了验证本文中嵌入强度的普遍适用性,JND 的值利用最经典的小波域视觉模型来计算[6]。

将不同 $r(r=1、2、3、4)$ 层和不同子图像 $s(s$ 为 LH 中频分量,HL 次高频分量,HH 高频分量)对噪声的掩盖因子记为 $F(r,s)$,则频率掩蔽因子如下所示:

$$F(r,s)=\begin{Bmatrix}\sqrt{2} & \text{if } s=HH\\ 1 & \text{otherwise}\end{Bmatrix}*\begin{cases}1.00 & \text{if } r=1\\ 0.32 & \text{if } r=2\\ 0.16 & \text{if } r=3\\ 0.10 & \text{if } r=4\end{cases} \tag{3}$$

亮度掩蔽因子 $L'(r,i,j)$ 可由式(4)和(5)计算得出:

$$L'(r,i,j)=\begin{cases}1-L(r,i,j) & \text{if } L(r,i,j)<0.5\\ L(r,i,j) & \text{otherwise}\end{cases} \tag{4}$$

$$L(r,i,j)=\frac{1}{256}D_3^3\left(1+\left\lfloor\frac{i}{2^{3-r}}\right\rfloor,1+\left\lfloor\frac{j}{2^{3-r}}\right\rfloor\right) \tag{5}$$

纹理掩蔽因子 $T(r,i,j)$ 由式(6)计算出:

$$T(r,i,j)=\sum_{k=1}^{3-r+1}16^{-k}\sum_{s=\{1,2,3\}}\sum_{m=0}^{1}\sum_{n=0}^{1}\left[D_{k+r-1}^s\left(m+\left\lfloor\frac{i}{2^{k-1}}\right\rfloor,n+\left\lfloor\frac{j}{2^{k-1}}\right\rfloor\right)\right]^2\times\mathrm{var}\left\{D_N^{\mathrm{LL}}\left(\{1,2\}+\left\lfloor\frac{i}{2^{3-r}}\right\rfloor,\{1,2\}+\left\lfloor\frac{j}{2^{3-r}}\right\rfloor\right)\right\} \tag{6}$$

结合以上四种掩蔽特性,最终可由式(7)得出小波域中的视觉阈值:

$$\mathrm{JND}_r^s(i,j)=0.5F(r,s)L'(r,i,j)T(r,m,n)^{0.2} \tag{7}$$

3 算法实现

3.1 水印预处理

为了加强水印的安全性及水印系统的抗攻击能力,先对二值水印进行 K_1 次 Arnold 变换得到 W_1,其变换关系为

$$\begin{pmatrix}m'\\ n'\end{pmatrix}=\begin{pmatrix}m\\ n\end{pmatrix}\times\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}(\bmod N) \tag{8}$$

3.2 嵌入算法

一般图像的绝大多数能量集中在中、低频系数域内,而高频部分的信息往往在量化时丢失。因此,为了同时满足透明性与鲁棒性,更有利于版权保护,将水印信息重复嵌入三通道的中、低频系数内。算法在三个独立分量中都嵌入水印信号。下面仅以 R 分量为例给出详细的过程,G、B 分量具有类似的过程。

a)提取原始彩色图像的 R 分量。

b)对置乱后的水印图像 W_1 进行 SVD 分解,$\boldsymbol{S}$、$\boldsymbol{U}$、$\boldsymbol{V}$ 分别表示水印图像的奇异值、左奇异值矩阵和右奇异值矩阵。

c)对 R 分量进行三级小波变换,并对其中的 HL 系数及 LL 低频系数进行奇异值分解,$\boldsymbol{S}_{\mathrm{HL}}$、$\boldsymbol{S}_{\mathrm{LL}}$、$\boldsymbol{U}_{\mathrm{HL}}$、$\boldsymbol{U}_{\mathrm{LL}}$、$\boldsymbol{V}_{\mathrm{HL}}$、$\boldsymbol{V}_{\mathrm{LH}}$ 分别表示各子带图像的奇异值、左奇异值矩阵和右奇异值矩阵。

d)利用式(2)(7)计算 HL 系数及 LL 的低频系数的奇异值修改权值 α_{HL} 和 α_{LH}。

e)分别按式(9)(10)进行水印信息的嵌入,R_{HL} 和 R_{LL} 分别表示嵌入水印后的两子带系数。

$$R_{\mathrm{HL}}=\boldsymbol{U}_{\mathrm{HL}}(\boldsymbol{S}_{\mathrm{HL}}+\alpha_{\mathrm{HL}}\boldsymbol{S})\boldsymbol{V}_{\mathrm{HL}} \tag{9}$$

$$R_{\mathrm{LL}}=\boldsymbol{U}_{\mathrm{LL}}(\boldsymbol{S}_{\mathrm{LH}}+\alpha_{\mathrm{LL}}\boldsymbol{S})\boldsymbol{V}_{\mathrm{LL}} \tag{10}$$

g)将得到的含水印两子带和为嵌入水印的两子带分量进行三级小波逆变换,最终得到含水印信息的 R 分量。

利用上述步骤 a)~g)分别可得新的 G、B 分量,然后将得到的三分量组合成新的 RGB 彩色图像 I'。

3.3 提取算法

水印的提取大致为嵌入过程的逆过程。下面给出 R 分量的具体过程:

a)提取已嵌入水印图像 I' 的 R 两个分量,经过奇异值分解得到奇异值矩阵 $\boldsymbol{S}'_{\mathrm{HL}}$、$\boldsymbol{S}'_{\mathrm{LL}}$。

b)用嵌入水印(待检测)图像中的 HL、LL 子带的奇异值和原始图像中 HH、LL 子带的奇异值提取两子带中嵌入水印的奇异值 $\boldsymbol{S}'_1$、$\boldsymbol{S}'_2$。

$$\boldsymbol{S}'_1=\frac{\boldsymbol{S}'_{\mathrm{HL}}-\boldsymbol{S}_{\mathrm{HL}}}{\alpha_{\mathrm{HL}}} \tag{11}$$

$$\boldsymbol{S}'_2=\frac{\boldsymbol{S}'_{\mathrm{LL}}-\boldsymbol{S}_{\mathrm{LL}}}{\alpha_{\mathrm{LL}}} \tag{12}$$

c)对 R 层中提取出的两个水印奇异值结合原水印的 U、V 矩阵进行奇异值逆变换,得到 R 层中提取出的两个水印。

d)用密钥 K_1 对两水印图像进行 Arnold 逆变换并与原始水印图像进行归一化相关系数的计算,取值较大者为 R 层中提取的水印。

利用同样的方法可分别从 G、B 分量中提取出水印 water2、water3。为了提高鲁棒性,对提取出来的三个水印图像分别与原始水印图像进行归一化相关系数的计算,取值最大者为最终提取的水印图像。

4　仿真实验

4.1　二值水印仿真与分析

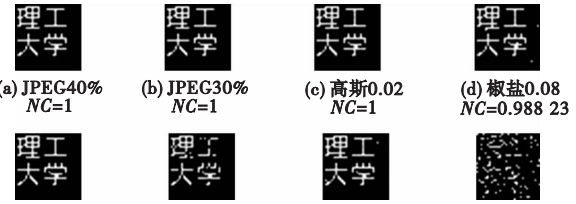
实验中,宿主图像选用大小为 256×256×24 的标准彩色图像 girl(图 1(a)),水印采用尺寸为 32×32 可辨识的字样为理工大学的二值图像(图 1(b)),根据对将阈值从 0~1 的仿真实验结果的分析选定效果最佳的 0.3 为提取阈值,实验平台是 MATLAB R2010a。

图 1(c)为嵌入水印后的 gril 图像,不难发现嵌入算法具有很好的不可见性,其峰值信噪比为 60.468 2 dB;(d)为无任何攻击的情况下提取出的水印,其 $NC=1$。

(a) 原始girl图　(b) 原始水印　(c) 水印化girl图　(d) 提取的水印

图1　girl图像嵌入水印的测试情况

图 2 给出了各种攻击下提取出的水印图像。对图像进行了强度为 20% ~90% 的 JPEG 压缩攻击,均能提取出完整的水印信息,水印相似度 $NC=1$,这说明算法对 JPEG 压缩具有很强的鲁棒性。对图像叠加方差为 0.005、0.01 和 0.02 的高斯噪声以及强度为 0.02、0.04 和 0.08 的椒盐噪声,实验结果表明本算法对噪声攻击也有很强的鲁棒性,针对前五项噪声均能提取出 $NC=1$ 的水印,在强度为 0.08 的椒盐噪声下水印信息仍然有较高的辨识度,$NC=0.988\ 23$。对图像进行从 2×2 到 5×5的中值滤波处理,在强度小于 4×4 时均能提取出较完整的水印信息只有在强度大于 6×6 时水印清晰度无法辨识。将图像剪切为 1/16、1/8、1/4 和 5/16,当剪切范围较小时对水印的提取没有影响,当剪切掉图像的 1/4 以上时水印信息不完整,说明算法在抗剪切攻击上具有一定的鲁棒性。



(a) JPEG40% $NC=1$　(b) JPEG30% $NC=1$　(c) 高斯0.02 $NC=1$　(d) 椒盐0.08 $NC=0.988\ 23$

(e) 中值3×3 $NC=1$　(f) 中值4×4 $NC=0.950\ 89$　(g) 剪切1/8 $NC=0.994\ 07$　(h) 剪切1/4 $NC=0.480\ 87$

图2　水印化girl遭受各种攻击后提取出的水印

此外,本文将实验结果与文献[7]进行了对比,其实验结果如表 1 所示。

从表 1 可以看出,本文算法在压缩、高斯噪声、椒盐噪声等攻击中具有更强的鲁棒性,并且噪声攻击在加大强度后仍然能提取出较清晰的水印。但是本文算法在剪切攻击上不如文献[7],由于大范围剪切图像的重要部分后造成水印的丢失。

表 1　本文与文献[7]鲁棒性实验结果对比

攻击方式	NC	
	本文	文献[7]
未受攻击	1	1
高斯 0.005	1	0.826 4
高斯 0.001	1	0.812 6
高斯 0.02	1	–
椒盐 0.002	1	0.975 1
椒盐 0.005	1	0.920 9
椒盐 0.008	1	0.899 0
椒盐 0.08	0.988 23	–
剪切 70×70	0.403 84	0.86 21
JPEG30%	1	–
中值滤波 4×4	0.950 89	–

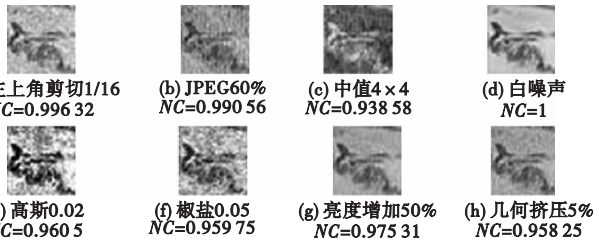
4.2　灰度水印仿真与分析

仿真过程中选用大小为 256×256×24 的 RGB 彩色图像 Lena 为宿主图像(图 3(a)),水印采用大小为 32×32 可辨识的灰度水印图像 plane(图 3(b))。灰度水印与二值水印不同,即使在遭受攻击后,提取出水印的奇异值发生的改变仍然是在灰度范围内,所以提取时不需要阈值的参与。仅通过人眼对原始彩色图像(图 3(a))和水印化图像(图 3(c))进行观察是无法发现两图之间存在的差异,即水印化图像的保真度并未有所下降,保持了良好的感官特性;另一方面采用峰值信噪比(PSNR)对图像进行客观评价,水印化图像高达 56.327 dB 的峰值信噪比充分说明了本文算法拥有较好的不可见性。

(a) 原始Lena图　(b) 原始水印　(c) 水印化Lena图　(d) 提取水印

图3　Lena 图像嵌入水印的测试情况

为了对本章算法的鲁棒性进行评估,分别对水印化图像进行了一系列的包括剪切、JPEG 有损压缩、滤波、添加噪声、分色处理、挤压等攻击和处理,得到的实验结果如图 4 所示。从图 4 可以看出,算法对常见的攻击都具有较强的鲁棒性。



(a) 左上角剪切1/16 $NC=0.996\ 32$　(b) JPEG60% $NC=0.990\ 56$　(c) 中值4×4 $NC=0.938\ 58$　(d) 白噪声 $NC=1$

(e) 高斯0.02 $NC=0.960\ 5$　(f) 椒盐0.05 $NC=0.959\ 75$　(g) 亮度增加50% $NC=0.975\ 31$　(h) 几何挤压5% $NC=0.958\ 25$

图4　水印化Lena遭受各种攻击后提取出的水印

为了说明本算法的优越性,将对含水印的 Lena 图像进行的一系列攻击的实验结果与徐国荣等人[8]的实验结果进行对比(表 2)。从表 2 可以看出,本文算法在应对 JPEG 压缩攻击上和抵抗噪声攻击的能力上更具鲁棒性,即使在加强攻击强度的情况下依然能够提取很清晰的水印信息;在诸如剪切、旋转等几何攻击方面较文献[8]相差无几。

通过对以上二值和灰度水印的仿真结果的观察不难得出以下结论:

a)对于小波域的水印系统来说,奇异值分解是一种很好的工具。通过实验结果分析,奇异值的修改具有使用范围广的

特点,可对低频奇异值进行修改,也可应用到中高频中。

b)在大多数小波域的水印算法中,通常不会利用低频子带完成水印的嵌入,因为这样会造成水印系统的透明性下降。在本文的DWT-SVD算法中,尽管修改了低频子带的系数,但是水印化图像仍能维持较好的视觉效果,说明本算法较好地协调了不可感知性和鲁棒性。

c)本文还做了单独提取两个子带中的水印的实验。实验结果表明,嵌入在低频子带的水印在应对如高斯噪声、压缩等处理时具有较强的鲁棒性,而中频子带的水印则对旋转、剪切攻击具有很强的鲁棒性。

d)本算法对两种形式的水印均适用,尽管在灰度图像水印的鲁棒性上稍差于二值水印,但相比其他算法来讲,仍然有其可取之处。

表2 本文与文献[8]鲁棒性实验结果对比

攻击方式	*NC*	
	本文	文献[8]
未受攻击	1	1
0.05 椒盐噪声	0.959 75	0.945 63
0.08 椒盐噪声	0.923 68	–
0.01 高斯噪声	0.985 28	0.889 07
0.02 高斯噪声	0.960 5	–
中值滤波 5×5	0.886 5	0.992 14
平移 5×5	0.808 17	0.816 05
剪切	0.878 17	0.829 9
旋转 30°	0.501 26	0.481 42
JPEG90%	0.998 32	–
JPEG80%	0.995 65	0.982 45
JPEG50%	0.989 1	–
JPEG20%	0.975 82	–
亮度增强 50%	0.975 31	–

5 结束语

本文提出一种基于DWT-SVD域的自适应彩色图像水印算法。该算法先对原始图像进行三级离散小波变换;然后对得到的R、G、B三通道的各子带以及用Arnold置乱后的水印图像进行奇异值分解,利用人类视觉系统(HSV)特性自适应地调整水印嵌入强度,将水印的奇异值加入到原始图像子带的奇异值上。人类视觉系统模型的应用保证了水印的隐蔽性。仿真实验结果表明,本文提出的算法具有较强的鲁棒性,在经受了压缩、噪声、剪切等常见的信号处理后,仍能提取出较完整的水印。在今后的研究中,应该加强对盲水印算法的研究,使算法更具实用性。

参考文献:

[1] 林旭亮,孙燮华,万里红. 一种基于DWT和SVD图像水印的新算法[J]. 微计算机信息,2010,26(6):96-97.

[2] AL-HAJ A. Non-invertible copyright protection of digital images using DWT and SVD[J]. Proc of the 2nd International Conference on Digital Information Management. 2007:448-453.

[3] 徐慈蓉,樊锁海. 一种新的基于奇异值分解的图像数字水印算法[J]. 计算机仿真,2011,28(5):291-341.

[4] SANTHI V,Dr THANGAVELU A. DWT-SVD combined full band robust watermarking technique for color image in YUV color space[J]. International Journal of Computer Theory and Engineering,2009,1(4):424-429.

[5] 阮波. 一种基于DWT-SVD的数字水印算法研究[D]. 成都:西南交通大学,2008.

[6] BARNI M,BARTOLINI F,PIVA A. Improved wavelet-based watermarking through pixel-wise masking [J]. IEEE Trans on Image Processing,2001,10(5):783-791.

[7] 杨卫民,谭骏珊,金正. 基于奇异值分解的彩色图像水印算法[J]. 计算机工程与设计,2008,29(23):6152-6153.

[8] 徐国荣,王礼平. 基于奇异值与提升小波的彩色图像水印算法[J]. 计算机应用研究,2011,28(5):1981-1986.

(上接第4322页)实用性。但是,文中对节点信任值的计算在系统中的开销、时效性等没有深入研究,只是作了简单的一些分析和说明,对分布式环境下协同决策[13,14]、信任衰减[15]等问题研究不是很透彻,希望在今后的工作中作进一步改进。

参考文献:

[1] CARONNI G. Walking the Web of trust[C]//Proc of the 9th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. Washington DC: IEEE Computer Society, 2000:153-159.

[2] CHEN R,YEAGER W. Poblano:a distributed trust model for P2P networks TR-I4-02-08[R]. Palo Alto: Sun Microsystem,2002.

[3] YU Ding-guo, CHEN Nan, TAN Cheng-xiang. Research on trust cloud-based subjective trust management model under open network environment[J]. Information Technology,2011,10(4):759-768.

[4] LI Xiao-yong, ZHOU Feng, YANG Xu-dong. A multi-dimensional trust evaluation model for large-scale P2P computing[J]. Journal of Parallel and Distributed Computing,2011,71(6):837-847.

[5] 胡智,尹继元,鲁军. P2P网络中基于推荐与用户行为的信任模型研究[J]. Computer Knowledge and Technology,2011,12(7):2787-2788.

[6] ABERER K, DESPOTOVIC Z. Managing trust in a peer-to-peer information system [C]//Proc of the 10th International Conference on Information and Knowledge Management. New York: ACM Press, 2001:310-317.

[7] TEACY W T,JIGAR P,JENNINGS N R. TRAVOS: trust and reputation in the context of inaccurate information sources[J]. Autonomous Agents and Multi-agent Systems,2006, 12(2): 183-198.

[8] KAMVAR S D, SCHLOSSER M T. EigenRep: reputation management in P2P networks [C]//Proc of the 12th International World Wide Web Conference. New York: ACM Press,2003:123-134.

[9] 郭成,李明楚,姚红岩,等. P2P网络下基于推荐的信任模型[J]. 计算机工程,2008,34(24):157-159.

[10] XIONG Li,LIU Ling. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities [J]. IEEE Trans on Knowledge and Data Engineering,2004,16(7):843-857.

[11] 窦文. 信任敏感的P2P拓扑构造及其相关技术研究[D]. 长沙:国防科技大学,2003:53-70.

[12] 窦文,王怀民,贾焰,等. 构造基于推荐的peer-to-peer环境下的trust模型[J]. 软件学报,2004,15(4):571-583.

[13] 朱友文,黄刘生,陈国良,等. 分布式计算环境下的动态可信度评估模型[J]. 计算机学报,2011,34(1):55-64.

[14] 彭涛,窦万峰,曲永花. 协同决策支持系统中的信任模型研究[J]. 计算机工程,2011,37(7):136-138.

[15] 李季,李刚. 一种基于信任衰减向量的P2P网络信誉模型[J]. 计算机工程与应用,2011,47(9):86-88.

R_j 表示由网络中其他节点对节点 j 的反馈信息而得到的推荐信任度，$R_j \leqslant 1$；μ 表示为节点 i 根据自身交易经验而设定的权重因子，在这里分为三种情况进行讨论。

a）若 $\mu = 0$，表示节点本身没有任何主见，仅仅依赖于其他节点的推荐反馈而与交易节点进行信息互动。

b）若 $\mu = 1$，表示节点自身只相信自己与交易节点以往的历史经验，对推荐信任度持有怀疑态度，不肯也不愿去相信反馈节点的推荐信息。

c）若 $0 < \mu < 1$，当节点 i 第一次与节点 j 进行交易时，由于直接信任度是由历史交易经验决定的，所以信任值是有限的，它更依赖于其他节点的推荐信任度，所以权重因子 μ 的比重会比较大；但是随着交易次数的不断累积，节点更愿意相信根据自身的交易经验来衡量节点的信任度，其他节点的推荐信息作为参考，因此权重因子 μ 的比重会随之下降，随着交易次数的增加而逐步加大。因此，权重因子是处于动态变化的过程中，即

$$\mu = 1 - \sigma^{k/n} \tag{11}$$

其中：σ 的取值是 $0.5 < \sigma < 1$；k 为节点 i 与 j 在某固定时间段 $[t_{start}, t_{end}]$ 内的第 k 次交易；n 为交易的总次数，取值是 $n \in \{1, 2, 3\cdots\}$。由式(11)看出，随着交易次数的增加，k 越大，μ 的值也会越大。这样得到的权重因子更符合实际交易中的情况和模式。

因此，可以得到关于节点 j 的综合信任度的计算式为

$$G_j = \mu D_{ij} + (1 - \mu) \sum_x R_{x \to j} \times A(x) - R(x) \tag{12}$$

最后根据得到的综合信任值与系统设定的阈值 G_{j0} 作比较。若是 $G_j > G_{j0}$，则表示节点是可信的，可以进行交易；若是 $G_j < G_{j0}$，则意味着节点的信任度有待商酌，这次交易暂不进行，为下次交易留作参考。

2 仿真实验与分析

2.1 仿真实验

通过仿真实验来检测该信任模型。为了更清晰地分析实验结果，将 EigenTrust、PeerTrust 模型与本文的信任模型放在同一个实验环境中进行比较。本文使用的场景以文件下载共享应用为例，用户的最终目标是下载所需文件，判断本次交易成功与否的唯一标准就是——下载文件的真实性。

实验环境设置为：模拟网络中的节点数是 100 个，文件总数是 1 000。将 1 000 份文件随机分配到 100 个节点中，保证每个节点至少拥有一份文件。每次交易时节点会从从不拥有的文件中任意选取其中一个进行下载。若下载成功，则节点拥有该文件，交易成功；若下载失败，则节点的文件拥有数不会增加，意味着交易失败。假设在模拟网络中诚实节点的数目多于恶意节点的数目，并且一次交易请求是由诚实节点发起的。实验结果如图 1 和 2 所示。

2.2 实验分析

图 1 所示为交易次数对目标节点综合信任值的影响。由于 EigenTrust 模型对推荐节点本身的准确性未加考虑，所以前 500 次的交易信任度没有很高，只是随着交易次数的增加使得直接信任度比重增大，从而增加信任度。PeerTrust 模型则完全依赖其他节点的推荐评价来判断目标节点的信任度，没有参考个人交互历史经验，开始交易时由于依赖推荐信任，比重较大，信任值较高；之后随着交易次数的累积，直接信任度的主要作用导致综合信任值涨幅不是很大。本文模型通过节点自身的交易记录作参考，并结合其他节点的推荐信息，引入偏移因子和随机数，可以忽略推荐信任度较低的节点推荐，这样计算出的节点信任值更能接近其真实值。实验验证了该模型的准确性和有效性。

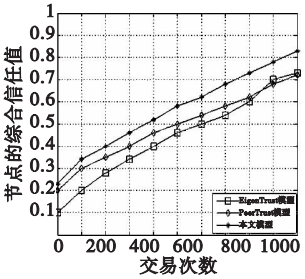


图1 交易次数对信任度的影响

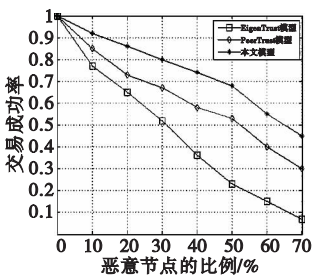


图2 不同恶意节点比例下的交易成功率

图 2 所示为不同恶意节点下交易成功率的情况。本文设置平均每个节点作 100 次交易后进行节点之间的互相评价，由诚实节点对其他节点进行信任度的评价。从结果中可以看出，随着恶意节点比例的逐渐增加，各个模型的交易成功率都有不同程度的下降。由于 EigenTrust 模型对恶意节点缺乏惩治措施，当恶意节点比例超过 40% 时，EigenTrust 模型计算错误率高，交易成功率随之下降迅速，若在恶意节点数目很多的环境下几乎难以运行；而无论恶意节点比例的大小，PeerTrust 和本文模型还能保持相对较高的交易成功率，证实该模型具有一定的安全性，在实际应用中更能发挥作用。

2.3 时效性和开销性分析

在 EigenTrust 模型中，由于缺乏对一些恶意节点的惩治机制，对协同作弊、提供虚假信息的合谋节点没有具体的惩罚措施，因此模型的时效性不是很明显，模型中在计算节点的全局可信值时要经过连续两次的迭代，其复杂度是 $O(n^2)$。在 PeerTrust 模型中，因为忽略了交易节点自身的历史经验，只是依赖于推荐节点的反馈信息，所以计算得到的综合信任值不是很合理，时效性不能真实地反映节点的信任程度，其计算的复杂度是 $O(n)$。在本文模型中，不仅增加惩罚机制对恶意节点的不实交易进行惩罚，同时注重交易双方的历史交互经验和推荐节点的反馈信息，随时都能更为准确真实地反映目标节点的综合信任值，因此时效性相对 EigenTrust、EigenTrust 模型来讲更为优越一些，并且计算的复杂度是 $O(n)$。

3 结束语

本文针对 EigenTrust 信任模型中存在的问题作了一些改进，提出了在 P2P 网络环境下基于推荐的信任模型。该模型通过惩罚因子来调节历史信任度作为以后进行交易的依据，使得直接信任值更接近其交易的真实值；在计算推荐信任度时，考虑了推荐节点本身的可信性，利用生成的随机数来判断节点的可信程度，可以有效防止恶意节点的协同作弊；最后计算目标节点的综合信任值时参考风险因子的影响，来决定这次交易是否可行。文中用仿真实验来验证推荐信任模型的可行性，得到较好的仿真结果，证明了该模型的有效性和 （下转第 4326 页）