基于文本水印的纸质文档泄密追踪系统

北京电子科技学院　林晶 周正一

1. 北京电子科技学院 信息安全系 信息与计算科学专业，北京市 107000；

2. 北京电子科技学院 信息安全系 信息与计算科学专业，北京市 107000；

刘芳 副教授

【摘要】针对纸质涉密文件非法传播，涉密责任无从追溯。对亓文法提出的基于字符翻转的抗打印扫描文本水印算法，进行改进与优化，实现基于文本水印的纸质文档泄密追踪系统。设计针对该水印算法的字符切分算法、添加预处理环节、增加去噪模块，以提高算法的鲁棒性。并进行大量实验测试，采集数据，分析各个物理量（打印机扫描仪型号、字体字号、打印扫描使用的分辨率等）对水印提取率的影响，找到最大误差区间，验证系统是否满足用户的需要。

【Abstract】For Paper-related document illeglly spread and secret responsibility can not be traced on, this paper improve and optimize the algorithm posed by QiWenFa which is based on character-flipping method and can resist duplicate print and scan.The group implement the ducument leakage tracking system which is based on text watermark,design the character segmentation algorithm for this watermark algorithm,add pre-treatment,increase de-noising module,and improve therodustness of the algorithm,By doing a large number of experimental tests,collecting data,analyzing various physical quanities (printers, scanners, models Font size Print scanning using resolution, etc.) which have an effect on watermark extraction yield,this paper finds the maximum error range to authenticate system whethere to meet the needs of the user.

【关键词】数字水印;二值图像;字符切分;纸质文档;泄密追踪

国家级大学生创新创业训练计划支持项目（2016003）

林晶：女，福建省，北京电子科技学院本科生

周正一：男，河北省，北京电子科技学院本科生

1 产品概述

（一）研究背景

随着信息化的发展和计算机的普及，电子文档成为人们日常办公的主要形式。但很多文档主要还是以纸质文档的形式存在。目前对于重要文件的打印主要采用限制打印，复印次数，或指定专人负责，打印文档时需要经过批准，审批，登记等步骤，并定期对纸质文档进行销毁或归档处理。特别是关键文档的泄露，往往会对一个企业乃至国家带来极大的威胁和风险。

虽然现在市面上已经出现了大量的水印嵌入的算法，但是嵌入水印的不可见性和鲁棒性并不是很理想。这一定程度上影响了嵌入信息的有效隐藏和正确提取。本系统基于亓文法等提出的基于字符翻转的抗打印扫描文本水印算法，对字符分割、水印嵌入算法部分进行了优化。同时，增加了去噪算法，优化了水印提取的算法，大幅度提高了水印提取的正确率。

（二） 产品功能

该系统具有较高的普适性。适用于各种党政机关或商界传收纸质文件及纸质文本泄密溯源的场合。通过对纸质文档嵌入抗打印扫描的不可见文本水印信息(打印者的身份信息、打印日期、文档的密级)，实现当截获非法传播的涉密文件时，可以通过水印准确追踪到何人何时打印了该文件，解决泄密源头追溯的问题；增加了纸质文件在传输过程中的安全性问题。

该系统具有很好的可操作性。用户登录系统后，选择需要打印的文件，按正常进行打印，无需进行额外的操作，系统自动截获需要打印的文件，对文件嵌入该用户的相关信息，然后发送给打印机，打印进进行打印。

该系统具有较高的实用性。通过优化核心算法，在大量的实验测试保证水印提取率达到 95%，并加入校验码，进行译码自动纠错，使打印扫描后，通过该系统可以准确追溯泄密源头。

二 产品设计及实现

（一）系统概述

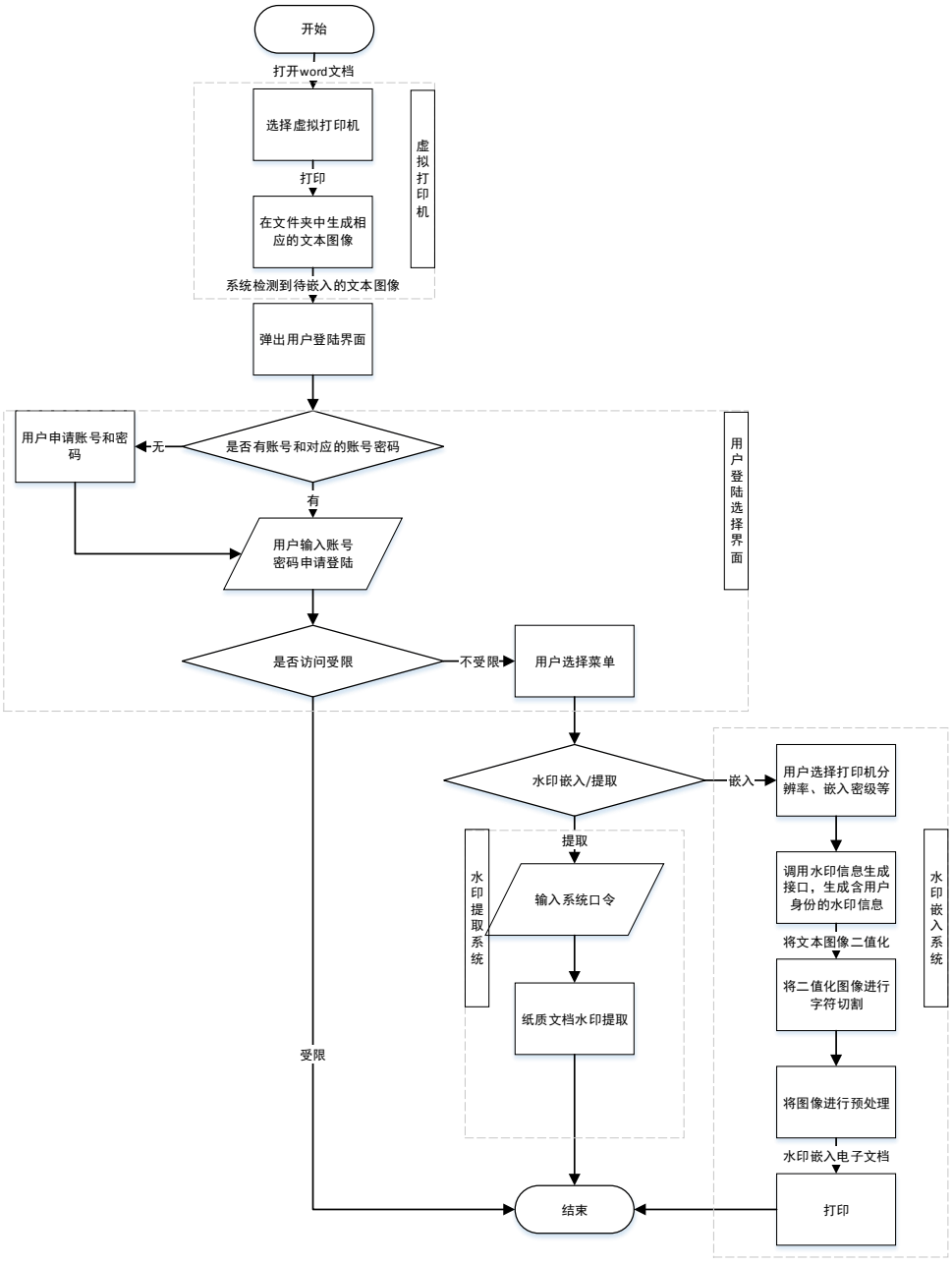

图 2.1

使用者需要申请用户名和用户密码，然后登录该系统。用户通过系统提供的用户名和密码登录。每一位使用者有其唯一的用户名与密码，也就拥有了唯一的个人信息。系统根据登录的个人信息生成嵌入信息以及对嵌入密级的要求，实现对电子文本的信息嵌入。然后通过指定的打印机打印出纸质文本。这时的纸质文本已经是经过水印嵌入之后的文本了。之后就可以进行文件的传递。

（三） 功能模块

1. 水印嵌入模块

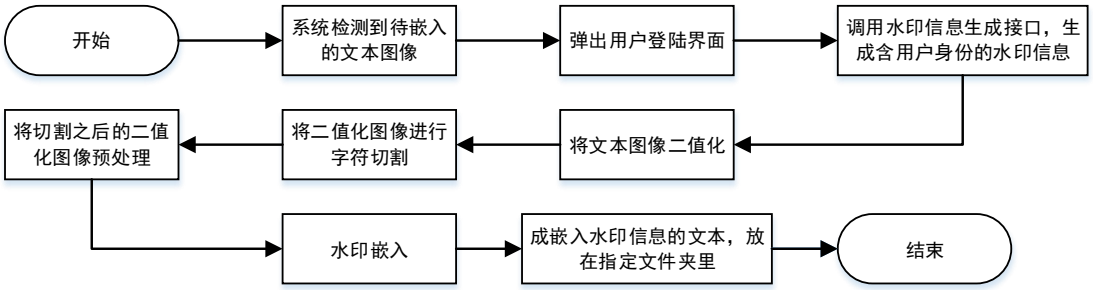

图 2.2

该模块由用户登录、字符分割、水印嵌入三个部分组成。

用户登陆选择部分主要用来通过输入搜集用户的身份信息、用户需要执行的操作和打印需要的分配率等。系统检测到文件夹里有文本图像后，自动弹出用户登录选择系统。首先，用户需要申请用户名和用户名密码来登陆此系统。接着，系统会根据用户的合法性来设置用户访问控制的权限。用户成功登陆系统后，系统根会据登录的个人信息生成嵌入水印信息，为电子文本的信息嵌入作准备。

2. 水印提取模块

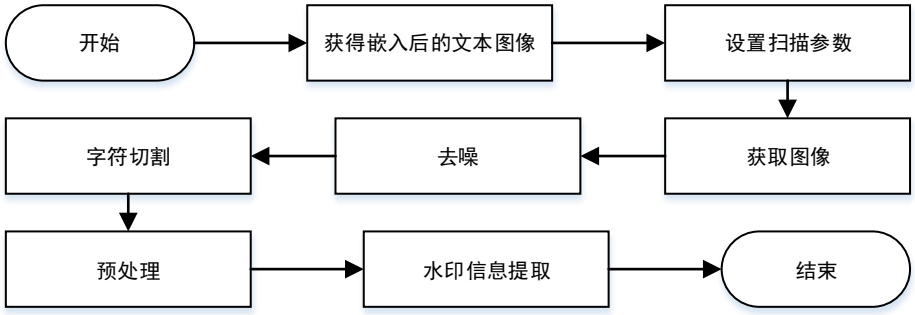

图 2.3

该模块由用户登录、传入文件预处理及水印提取三个部分。传入文件预处理的模块主要用于降低因为由于打印，扫描等处理导致文本的破坏，影响文本水印提取的因素，保证水印提取的成功率；水印提取模块则是用于提取嵌入的信息，并呈现给操作者。

（四） 实现原理

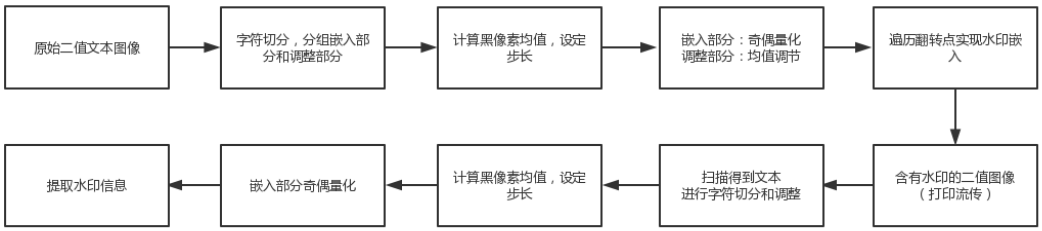

图 2.4

针对抗打印扫描的文本水印算法的核心思想是通过找到打印扫描前后的一个不变量，并利用该不变量实现水印嵌入。

亓文法等提出的基于字符翻转的抗打印扫描文本水印算法，把打印扫描过程对图像带来的转变描述为一个卷积过程，即

$$F_w(x) = K * F(x) \quad (1)$$

其中K是某个核函数，它只依赖于打印过程而不依赖于具体的字符，$\mathbf{x}$表示图像像素点。假定I是字符图像区域，对于（1）左右两端做积分，得到

$$\int_I F_w(x)\,dx = \int_I \mathrm{K}\,dx \int_I F(x)\,dx \quad (2)$$

则由（2）可以得到

$$\frac{\int_I F(x)\,dx}{A} = \frac{\int_I F_w(x)\,dx}{A_w}$$

即每个字符所包含的黑像素与全部字符的黑像素的平均值的比值在打印扫描前后是不变的。这也是该算法可以实现抗打印扫描的关键技术。

1. 字符切分算法

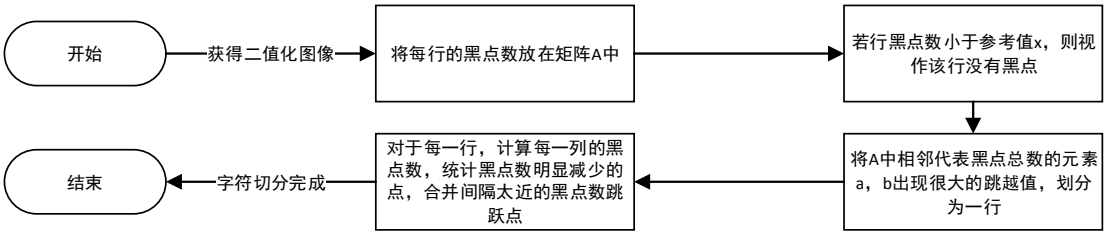

图 2.5

基于垂直投影、字体大小估计、轮廓分析或切分识别组合。

2. 图片预处理算法

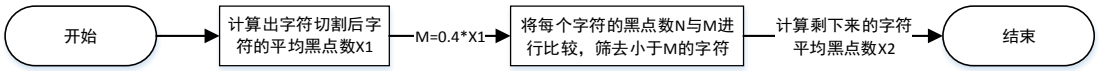

图 2.6

图片的预处理就是将黑点数比较少的标点符号或者‘一’之类的字符先筛去。因为这些字符的可翻转点很少，可以直接忽略。

3. 水印嵌入算法

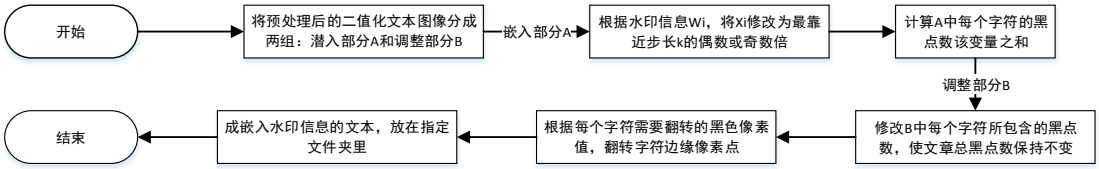

图 2.7

第一步：对二值文本图像进行字符切分后将切分出的字符分为两组：嵌入部分 A 和调整部分 B。设分组 A 和调整部分 B。设分组 A 和 B 中每个字符图像所包含的黑点数分别为$x_1, x_2, \ldots, x_{N_A}$和$y_1, y_2, \ldots, y_{N_B}$，然后计算所有字符图像所包含的黑点数的平均值

$$\mathrm{m} = \frac{1}{N_A + N_B}\left(\sum_{i=1}^{N_A} x_i + \sum_{i=1}^{N_B} y_i\right)$$

第二步：假定水印信息为$w_1, w_2, \ldots, w_{N_A}$根据$w_i$为 0 或 1，将$x_i$修改为$\tilde{x}_i$,使得$\tilde{x}_i/m$是最靠近某个选定步长 K>0 的偶数倍或者奇数倍。 接着计算嵌入部分 A 中的每个字符的黑点数的改变量$\Delta_i = \tilde{x}_i - x_i$,并计算所有改变量之$\Delta = \sum_{i=0}^{N_A}\Delta_i$。

第三步：将调整部分 B 中每个字符所包含的黑点数y_i修改为$\tilde{y}_i$，使得

$$\sum_{i=0}^{N_B}\tilde{y}_i - \sum_{i=0}^{N_B} y_i = -\Delta$$

在算法中通过 A 的嵌入部分像素变化及 B 的调整部分的像素补偿使得 m 保持不变。

第四步：由(2)和(3)可以得到每个字符需要翻转的黑色像素值：$\Delta_{x_i} = \tilde{x}_i - x_i$和$\Delta_{y_i} = \tilde{y}_i - y_i$，按照翻转量的正负来翻转字符图像边缘相应数目的白色或黑色的像素点。

4. 去噪算法

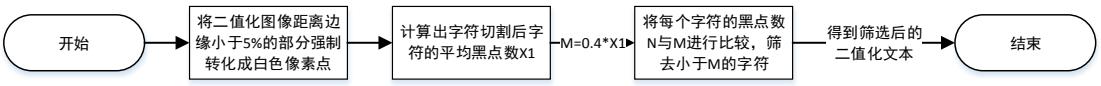

图 2.8

第一步：将扫描产生的黑边强制转化成白色。黑边分布在二值化图像距离边缘小于 5%的部分。

第二步：先算出字符切割后字符的平均黑点数 x_1 ，此时计算出一个筛选的标准 $M=x_1*0.4$ 。

第三步：如果小于这个标准的字符就不被考虑在可翻转字符内。筛选后的二值化文本图像用来进行下一步的水印提取。

5. 水印提取算法

图 2.9

第一步： 将嵌入水印的纸质文本文件通过扫描得到文本图像,并在保证得到与嵌入部分相同的字符序列的基础上,将所有字符分为嵌入部分 A 和调整部分 B。

第二步： 分别计算和 B 中字符所包含的黑像素数,设其分别$x_1, x_2, \dots, x_{N_A}$和$y_1, y_2, \dots, y_{N_B}$，则整个字符图像所包含的黑色像素平均值为

$$\mathrm{m} = \frac{1}{N_A + N_B}\left(\sum_{i=1}^{N_A} x_i + \sum_{i=1}^{N_B} y_i\right)$$

第三步：使用类似嵌入部分中的奇偶量化方法实现水印提取,若$\mathrm{round}\left(\frac{\check{x}_i}{K\bar{m}}\right)$是偶数,则判断水印信息$w_i$为 0,反之则为 1。

三 产品测试与分析

（一）测试目的

为保证基于纸质文本的泄密追踪系统的设计与开发质量和可靠性，有必要对系统进行测试。系统测试的目的在于找到最大误差区间，验证系统是否满足用户的需要。

（二）测试设备

打印机：HP P2015d
扫描仪：方正 founderT400h

（三）算法测试

1. 打印扫描前后不变量测试

通过对比打印扫描前后单个字符图像内的黑像素与均值的比例关系，即比较$\frac{x_i}{\bar{x}}$与$\frac{y_i}{\bar{y}}$的拟合曲线，如图 3.3 与图 3.4 得到了两条曲线基本一致。

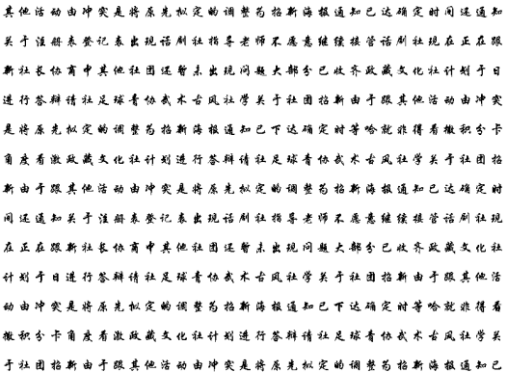

图 3.2 打印扫描前文本

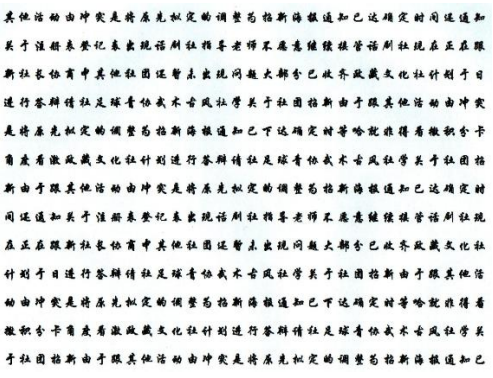

图 3.3 打印扫描后文本

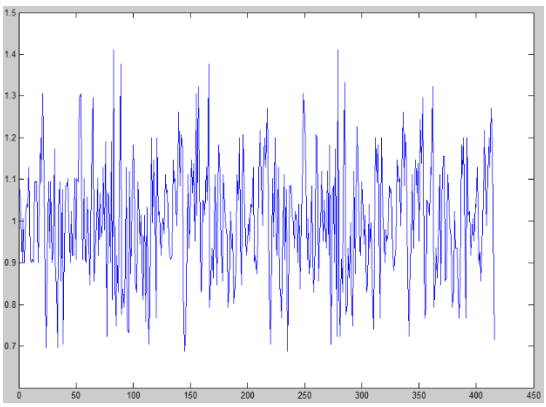

图 3.4 打印扫描前$\frac{x_i}{\bar{x}}$

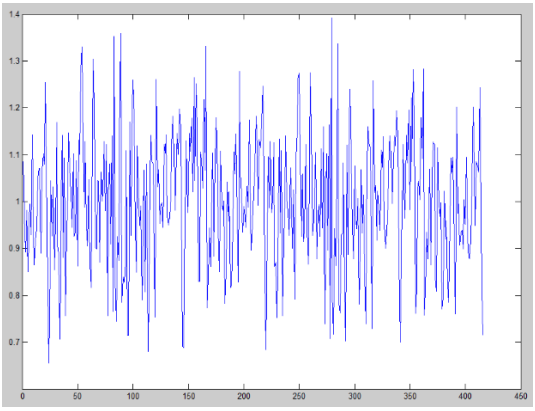

图 3.5 打印扫描后$\frac{y_i}{\bar{y}}$

2. 水印算法不可见性测试

由图 3.5 可知，使用的基于字符边缘像素点翻转策略不可见性良好。（灰色点为水印嵌入需要翻转的点）通过人眼观察图 3.6 与图 3.7 得出，水印嵌入后的图像的视觉效果良好，很难看出字符被修改的痕迹。

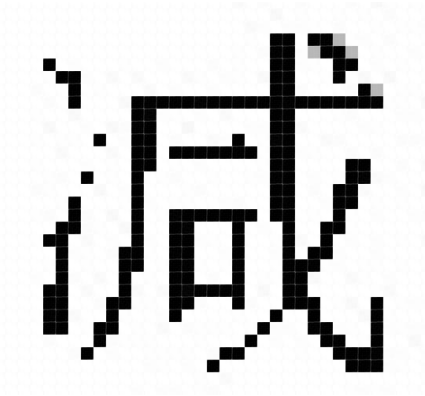

图 3.6 可翻转的边界点

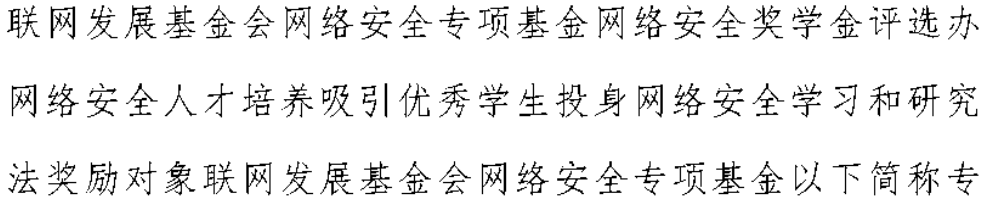

图 3.7 不含水印文本

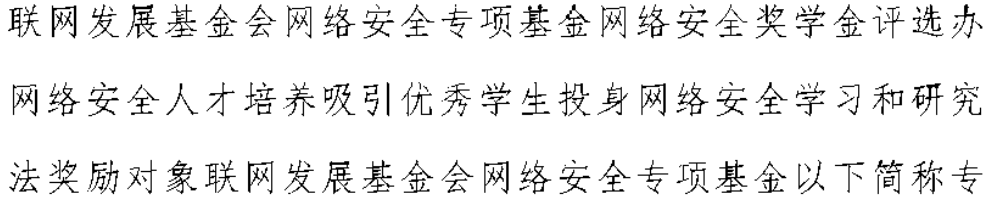

图 3.8 含水印文本

3. 测试不同字体对不可见性的影响

黑体、仿宋这两种字体虽然在肉眼上都很难发现水印的嵌入，对于黑体比较图 3.8 与图 3.9，对于仿宋比较图 3.10 与图 3.11。仿宋的不可见性较好。

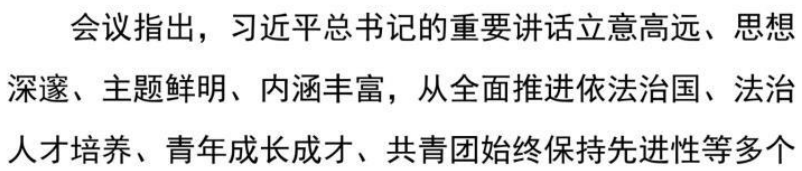
会议指出，习近平总书记的重要讲话立意高远、思想
深邃、主题鲜明、内涵丰富，从全面推进依法治国、法治
人才培养、青年成长成才、共青团始终保持先进性等多个

图 3.9 黑体不含水印图像

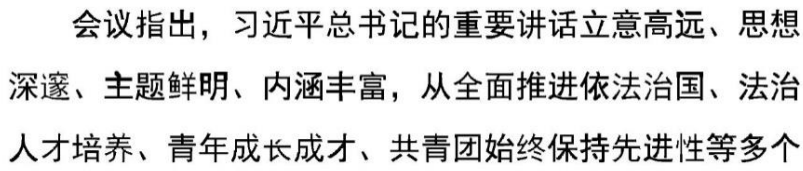
会议指出，习近平总书记的重要讲话立意高远、思想
深邃、主题鲜明、内涵丰富，从全面推进依法治国、法治
人才培养、青年成长成才、共青团始终保持先进性等多个

图 3.10 黑体含水印图像

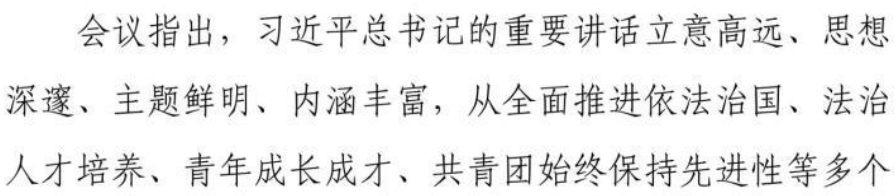
会议指出，习近平总书记的重要讲话立意高远、思想
深邃、主题鲜明、内涵丰富，从全面推进依法治国、法治
人才培养、青年成长成才、共青团始终保持先进性等多个

图 3.11 宋体不含水印图像

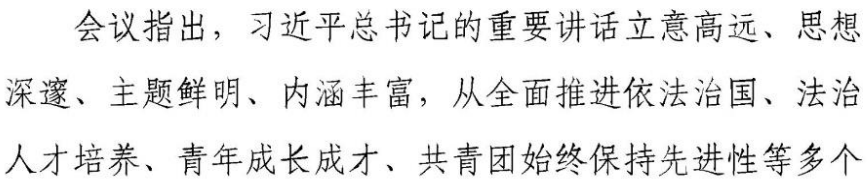
会议指出，习近平总书记的重要讲话立意高远、思想
深邃、主题鲜明、内涵丰富，从全面推进依法治国、法治
人才培养、青年成长成才、共青团始终保持先进性等多个

图 3.12 宋体含水印图像

4. 电子版水印提取率分析

对于嵌入的 147bit 水印信息，在没有打印扫描的物理噪声干扰下。进行 5 组实验，每组进行 10 次重复性试验，统计每组平均提取率，电子版提取率都达到 100%。

表 3.1 电子版提取率

	第一组	第二组	第三组	第四组	第五组
平均提取率	100.00%	100.00%	100.00%	100.00%	100.00%

5. 不同字体对水印提取率的影响

在 DPI 为 600, k 取 0.2 测试字体对提取率的影响，对于五种字体进行水印提取测试，发现黑体的水印提取率最高比其次的仿宋提取率高了 1.48%

表 3.2 不同字体水印提取率

	黑体	仿宋	楷体	行楷	隶书
平均提取率	97.46%	95.98%	95.67%	95.48%	95.88%

6. 扫描分辨率 DPI 对提取率的影响

每组为 10 次重复性实验，取提取率的平均值。扫描分辨率对提取率的影响也很大。根据实验数据分析可知：DPI 为 600 的时候，提取率比 DPI 为 200 时高 8.17%，比 DPI 为 300 时高出 6.93%，甚至多次达到 100%。

表 3.3 DPI=200 水印提取率

	第 1 组	第 2 组	第 3 组	第 4 组	第 5 组	平均
平均提取率	87.71%	95.92%	85.71%	98.96%	85.71%	90.80%

表 3.4 DPI=300 水印提取率

	第 1 组	第 2 组	第 3 组	第 4 组	第 5 组	平均
平均提取率	89.80%	89.80%	91.84%	98.96%	89.80%	92.04%

表 3.5 DPI=200 水印提取率

	第 1 组	第 2 组	第 3 组	第 4 组	第 5 组	平均
平均提取率	97.96%	99.87%	98.96%	97.97%	97.96%	98.54%

7. 步长 K 对提取率的影响

每组为 10 次重复性实验，取提取率的平均值。发现选定步长$k = 0.2$时的提取率普遍比步长$k = 0.1$的提取率要高 8%左右。

表 3.6 DPI=600

	第 1 组	第 2 组	第 3 组	第 4 组	第 5 组	平均
0.2	97.96%	99.98%	99.87.%	99.95%	97.96%	99.14%
0.15	91.84%	87.76%	81.63%	97.96%	95.92%	91.02%

8. 算法改进前后水印提取率的改变

每组为 10 次重复性实验，取提取率的平均值：

表 3.7 算法改进前水印提取率

	第 1 组	第 2 组	第 3 组	第 4 组	第 5 组	平均
改进前	81.23%	84.58%	89.92%	80.32%	84.92%	84.19%
改进后	91.01%	92.25%	99.18%	91.02%	97.96%	94.28%

4 总结

虽然现在市面上已有大量的数字水印的算法，但是针对于纸质文档的数字水印算法在其不可见性和抗打印扫描的效果上并不是很理想。这在很大程度上影响了嵌入信息的不可见性和水印提取正确性。基于以上原因，本系统基于亓文法等提出的基于字符翻转的抗打印扫描文本水印算法，对字符分割、水印嵌入算法部分进行了优化。同时，增加了去噪算法，优化了水印提取的算法，大幅度提高了水印提取的正确性，实现了基于文本水印的纸质文档泄密追踪系统。

（一）核心算法的改进

1. 嵌入后视觉效果好。

在嵌入算法中设计了过滤类似“一”、“二”及标点符号等笔画过于简单的字符的算法，避免嵌入后字符“少笔画”的问题，而后对亓文法等文献提出的可翻转点模板做出了改进，使得嵌入后用肉眼更加难以观察是否嵌入了水印信息。

2. 提取正确率较高。

亓文法更注重文字视觉效果，从而忽视了提取的正确率（实测在 80%至 90%之间），但在实际应用中，即使提取后错误 1bit 的信息都可能产生严重的影响，所以在牺牲部分字的视觉效果的前提下改进了嵌入及提取算法，可以避免上述问题并大幅提高提取正确率，经实验证明，改进算法可以将提取正确率提高 10%左右。

3. 去噪能力较强。

扫描后产生的图片几乎不能避免大噪音（黑边、断裂线）的干扰，这些会破坏文本结构，大大降低水印信息提取正确率，根据公文格式要求设计了较为完善的去噪算法，在不影响文本内容的前提下可以较好的处理打印及扫描过程产生的噪音，提高了系统鲁棒性。

4. 贴近应用环境。

在实际应用中需要嵌入的信息量一般大于 50bit，而亓文法的测试信息量多为 25bit 至 27bit，远低于实际需求，测试信息一般大于 140bit，更满足实际需求；另外用于测试亓文法的扫描仪全部使用至少 600DPI 的分辨率，但在实际环境中很多为 300DPI 甚至 200DPI，改进的算法比亓文法更适应这种实际环境。

参考文献

[1] 亓文法，李晓东，杨斌.用于信息追踪的文本水印算法.通信学报，Vol.29,2008.10.183-187

[2] 孙圣和，陆哲明，牛夏牧.《数字水印技术及应用》.北京:科学出版社，2004

[3] 杨义先.《数字水印基础教程》.北京:人民邮电出版社，2007.6

[4] 杨义先，钮心忻.《数字水印理论与技术》.北京:高等教育出版社，2006: 15-21

[5] Brassil J. Low S. Maxemchuk N F .Electronic marking and identification techniques to discourage document copying 1995(08)

[6] 黄华，齐春，李俊一种新的文本数字水印标记策略和检测方法.西安交通大学学报，2002.2:35-39

[7] 王丽娜，张焕国、信息隐藏技术与应用〔M].武汉大学出版社.2003.

[8] J. Brassil, S. Low, N. R Maxemuchuk. Copyright Protection for the Electronic Distribution of Text Documents[C]. Proceedings of the IEEE. 1999.

[9] 李浩峰.基于二值图像的文本水印技术研究. 贵州大学.[硕士学位论文].2008.

[10] 韩猛.基于文本的数字水印技术研究. 安徽理工大学.[硕士学位论文]，2009.

[11] 张弛.二值文本图像数字水印技术研究.重庆大学.[硕士学位论文].2007.

[12] 黄华，齐春，李俊一种新的文本数字水印标记策略和检测方法.西安交通大学学报，2002,2: 35-39.

[13] 魏宝荣.用于信息认证的二值文本图像数字水印算法的研究.西安电子科技大学.[硕士学位论文].2014.

[14] D. Huang, H. Yan. Interword Distance Changes Represented by Sine Waves for Watermarking Text Images[J]. IEEE Trans. on Syst. Video Technol. 2001,11(12).

[15] 王丽娜，郭迟，叶登攀等.信息隐藏技术实验教程.武汉：武汉大学出版社. 2012,9.

[16] 钟桦，张小华，焦李成.数字水印与图像认证:算法及应用.西安:西安电子科技大学.2006,8.

[17] 陈砚鸣.面向文档安全的数字水印技术研究.兰州大学.[硕士学位论文].2011, 5.

[18] 仲崇山.现代汉字字符切分的分离性原则和理据性原则[[J].北京:北京国际汉字研究会.2009, 5. 21-24.