基于 Shamir 秘密共享方案的数字水印算法

牛少彰 钮心忻 杨义先
(北京邮电大学信息安全中心,北京 100876)

摘 要 数字水印已成为数字作品版权保护的一种手段,而鲁棒性和不可察觉性是其基本要求.为此,提出了一种基于 Shamir 秘密共享方案的数字水印算法.该算法首先将图象分成 n 块,并将水印信息也分成 n 份,然后通过 DCT 的相邻系数比较法,将每份水印信息嵌入到图象的相应块中,提取时,只要获得其中的任意 $t(\leq n)$ 份水印信息就可以恢复出原始水印.为提高提取水印图象的精度,给出了基于模糊集的改进算法.实验结果表明,该算法的隐藏效果很好,并且对单一攻击及多种复合攻击具有很好的鲁棒性.

关键词 计算机图象处理(520·6040) 数字水印 秘密共享 模糊集
中图法分类号:TP309.9 **文献标识码**:A **文章编号**:1006-8961(2003)10-1178-05

Digital Watermarking Algorithm Based on Shamir Secret Sharing Scheme

NIU Shao-zhang, NIU Xin-xin, YANG Yi-xian
(*Information Security Center, Beijing University of Posts and Telecommunications, Beijing* 100876)

Abstract Digital watermarks have been proposed in recent literature as a means for copyright protection of multimedia data. The robustness and the imperceptibility are the basic requirements of the digital watermark. In this paper, we propose a digital watermarking algorithm based on Shamir secret sharing scheme. We divide the field of the image into parts, and then we also make the information of digital watermarking into shares by the algorithm. We embed each share of the digital watermarking in the corresponding part of the image by contrasting DCT coefficients, and only need arbitrary shares in the recovery progress. In order to enhance the precision of the extracted watermark, we improve the extracting algorithm based on fuzzy set. Experimental results show that this algorithm has a good hiding effect and is robust for single attack and even collage attacks.

Keywords Computer image processing, Digital watermarking, Secret sharing, Fuzzy set

0 引 言

在过去的几年里,数字水印已经成为用来解决数字多媒体中版权问题和内容认证的主要工具.对于图象来说,为了保护版权,在图象里加入一个水印(版权标志),并且希望不要因此而引起图象视觉上的降质.一旦需要验证图象的所有权时,可以通过算法提出水印来实现.数字水印技术的发展为解决数字作品的侵权问题提供了一个有效的解决途径[1~4].

基于 Shamir 秘密共享方案的数字水印算法,将水印信息分成 n 份,各部分之间没有任何包含关系,而只有获得其中 $t(t\leq n)$ 份以上的信息才可以恢复出原始水印.这样就可以从两方面来增强水印的安全性:一是攻击者即使知道水印的嵌入算法,也只能提取出经过共享后的水印信息,无法恢复出原始水印;二是图象被破坏一部分后,水印信息仍可以恢复出来.由于对数字水印的攻击往往并不是单一的,我们所提出的数字水印算法,可以有效地抵抗复合攻击.为提高水印提取的精度,利用该算法的独特性

基金项目:国家重点基础研究发展规划资助项目(G1999035805);国家杰出青年基金资助项目(69425001);
国家自然科学基金资助项目(69882002,60073049)
收稿日期:2002-07-22;**改回日期**:2003-06-09

能，提出了基于模糊集的提取算法，实验结果证明这种改进在很大程度上提高了水印图象的清晰程度.

1　离散余弦变换(DCT)

离散余弦变换是一种典型的数字图象变换. 数字图象可看作是一个二元函数在离散网格点处的采样值，可以表示为一个非负矩阵.

二维离散余弦变换定义为

$$F(u,v)=\alpha(u)\alpha(v)\left\{\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\times\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right]\right\}$$

逆变换定义为

$$f(x,y)=\left\{\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)F(u,v)\times\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right]\right\}$$

其中，$f(x,y)$为图象的像素值，$F(u,v)$为图象做 DCT 变换后的系数，$\alpha(0)=\sqrt{\frac{1}{N}}$，$\alpha(m)=\sqrt{\frac{2}{N}}$($1\leq m\leq N$). 基于 DCT 变换的水印嵌入算法采用 DCT 中频系数的相邻系数比较法.

2　数字水印算法

2.1　数字水印的嵌入

所谓密钥共享就是将一个密钥分解成 n 份，只有知道了其中的至少 $t(t\leq n)$份才能恢复出原来的秘密信息. Shamir 提出了一种基于 Lagrange 插值公式的密钥共享方案[5].

设 $GP(q)$是一个有限域，且 $q>n$. 现在想将密钥 k^*分成 n 份，交给 n 个人保管，且其中任意 $t(t\leq n)$个人合作可以得到密钥 k^*. 任取 $a_1,a_2,\cdots,a_{t-1}\in GP(q)$. 构造一个多项式

$$f(x)=k^*+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}$$

其中，k^*为密钥.

令 α 是 $GP(q)$域的本原元素，作

$$k_i=f(\alpha^i),i=1,2,\cdots,n$$

称 k_i 为子密钥，将 k_i 交给合作者 A_i 保管. 设有 t 个合作者，不失一般性，设为 $A_1,A_2,\cdots,A_t$ 分别提供了各自的子密钥 l_i 以及各自的序号 $1,2,\cdots t$. 利用 Lagrange 插值公式

$$p^*(x)=\sum_{j=1}^{t}l_j\prod_{i\neq j}\frac{(x-\alpha^i)}{(\alpha^j-\alpha^i)}$$

得一个 $t-1$ 次多项式. 由于 $f(x)=p^*(x)$，从而密钥 k^*得以恢复：

$$k^*=f(0)=p^*(0)$$

但是若只有 $s(x<t)$个合作者，则不足以确定 $f(x)$.

将基于 Lagrange 插值公式的密钥共享思想应用于数字水印. 取 $n=9,t=3,q=11$，则 $GP(q)$是一个有限域，且 $q>n$，构造一个多项式

$$f(x)=k^*+a_1x+a_2x^2$$

将载体图象按下面的方式分成 9 份.

1	2	3
4	5	6
7	8	9

数字水印为二值图象文件，对水印图象进行加密处理，其目的是使水印信息接近随机噪声. 对加密后的水印信息进行适当的分组，使得分组后转化为十进制数时，每组的数据介于 $0\sim q-1$ 之间. 分组后转化为十进制的数即为 k^*，令

$$l_i=f(i)(\mathrm{mod}q),i=1,2,\cdots,9$$

将 $l_1,l_2,\cdots,l_9$ 转化为二进制数后，对图象的每一子块按 8×8 像素分块，对其做 DCT 变换后，得到 8×8 像素块的 DCT 系数. 用 DCT 中频系数的相邻系数比较法将 l_i 隐藏在图象的第 i 块中($i=1,2,\cdots,9$).

2.2　数字水印的提取

水印的提取并不需要获得全部 9 份水印信息，而只要获得其中的 3 份就可以恢复出原始水印.

设已经知道了图象的 $i,j,k(1\leq i<j<k\leq9)$块. 在这 3 块中通过 DCT 逆变换，比较相邻的 DCT 系数，可取出隐藏的二进制数，再将其转化为十进制数后就得到了 l_i,l_j,l_k. 使用 Lagrange 插值公式

$$p^*(x)=l_i\frac{(x-k)(x-j)}{(i-k)(i-j)}+l_j\frac{(x-k)(x-i)}{(j-k)(j-i)}+l_k\frac{(x-j)(x-i)}{(k-j)(k-i)}$$

将所得到的多项式记为 $p^*(x)=a_0+a_1x+a_2x^2$，若记

$$n_i=[(i-k)(i-j)]^{-1}$$
$$n_j=[(j-k)(j-i)]^{-1}$$
$$n_k=[(k-j)(k-i)]^{-1}$$

则有

$$a_0=kjn_il_i+kin_jl_j+ijn_kl_k$$
$$a_1=-[n_il_i(k+j)+n_jl_j(k+i)+n_kl_k(i+j)]$$
$$a_2=n_il_i+n_jl_j+n_kl_k$$

得到 $k'=a_0$，再将 k' 转化为二进制，通过解密算法恢复出原始水印.

2.3 基于模糊集的改进算法

为进一步提高在遭受攻击的情况下提取水印图象的精度，减少水印恢复中出现的错误，对提取出的水印图象给出基于模糊集[6]的改进算法.

由于将水印信息分成了 9 份，并且从任意的 3 份中都可以恢复出水印信息，因此在遭受除剪切和擦除攻击外的各种攻击情况下，能够将 9 份水印信息全部提出，再分成 3 组，每组均含有 3 份水印信息，那么从每组中都可以恢复出原始水印，记为 $\boldsymbol{W}_a$，$\boldsymbol{W}_b$ 和 $\boldsymbol{W}_c$. 由于使用二值黑白图象作为水印，因此水印图象实际上就是一个布尔矩阵. 把这个矩阵转化为向量，不防设

$$\boldsymbol{W}_a=[a_1,a_2,\cdots,a_i,\cdots,a_n]$$
$$\boldsymbol{W}_b=[b_1,b_2,\cdots,b_i,\cdots,b_n]$$
$$\boldsymbol{W}_c=[c_1,c_2,\cdots,c_i,\cdots,c_n]$$

其中，$a_i,b_i,c_i(i=1,2,\cdots,n)$ 为 0 或 1.

在二值黑白图象中，0 代表黑色，1 代表白色. 将 $\boldsymbol{W}_a$，$\boldsymbol{W}_b$ 和 $\boldsymbol{W}_c$ 看成是对水印图象的 3 次模糊统计，可以得到水印图象

$$\boldsymbol{W}=[w_1,w_2,\cdots,w_i,w_n]$$

上的一个关于“黑色”这一概念的模糊集 $\tilde{\boldsymbol{W}}$，水印图象中的元素对于“黑色”的隶属度定义为

$$\mu_{\tilde{W}}(w_i)=a_i,b_i,c_i \text{ 中零的个数}/3$$

通过适当选取置信水平 λ 的值，可由模糊集 $\tilde{\boldsymbol{W}}$ 的截集 $\boldsymbol{W}_\lambda$ 重建水印图象.

3 实验结果

虽然在理论上，对于有限域 $\boldsymbol{GP}(q)$，只要取 $q>9$ 就能满足要求，但在实际上，由提取出的 3 份水印信息恢复原始数据时，若其中有一个发生错误就会导致最后结果的错误，又由于水印图象为二值黑白图象，算法中涉及到十进制和二进制的相互转换，如果十进制的数据出现错误，则错误会发生扩散，q 越大，影响二进制数据的位数也就越多，因此，应取尽可能小的 q，在下面的实验中，取 $q=11$.

图 1 为原始图象，图象的尺寸为 512×512，图 2 为原始图象嵌入水印后图象，尺寸不变，图 3 为原始水印，尺寸为 90×80.

将含水印的图象进行大面积的剪切攻击(图 4)，由于剩余的图象中包含了 3 份水印信息，因此可以恢复出原始水印，提取出的水印图象与原始水印图象一样，如图 5 所示.

一般来说，对水印的攻击是以不破坏使用价值，

图 1 原始图象

图 2 嵌入水印后图象

图 3 原始水印

图 4 剪切攻击

图 5 从图 4 中恢复的水印图象

而又能将图象所携带的水印信息去掉为目的的，而大面积剪切攻击（如图 4 所示）则使图象失去了使用价值. 图 6 为嵌入水印后图象经 JPEG 压缩处理后得到的图象，取 JPEG 质量因子 $Q=97\%$，图 7 为从图 6 中选取 3 块含水印的图象提取的水印图象.

图 6　水印图象经过 JPEG 压缩（$Q=97\%$）

图 7　从图 6 中提取的水印图象

从图 7 可以看到：水印图象只有少量的错误. 如图 8 所示，加大攻击强度，取 $Q=90\%$，同样地，在图 8中选取 3 块含水印的图象，提取出水印图象，如图 9所示.

图 8　水印图象经过 JPEG 压缩（$Q=90\%$）

图 9　从图 8 得到的水印图象

从提取出的水印图象图 9 可以看到，与图 7 相比水印图象的错误明显增多. 要提高水印抗 JEPG 压缩的鲁棒性可以提高水印的嵌入强度，但水印强度的增加会引起图象的降质. 下面给出基于模糊集改进算法的实验结果，在不增加水印强度的情况下提高提取水印图象的精度.

对如图 8 所示受到 JEPG 压缩的含水印图象，将图 8 中提取出的 9 份水印信息分成 3 组，从每 3 份中恢复出水印图象，得到 3 个水印图象，计算得到模糊集 W，取置信水平 $\lambda=0.6$，得到水印图象如图 10 所示.

图 10　$\lambda=0.6$ 时从图 8 中恢复的水印图象

将图 10 的水印图象和图 9 的水印图象对比，可以发现错误明显减少，水印图象的清晰度明显提高，这充分体现了改进算法在提高水印图象提取精度上的优势.

除此之外，我们还进行了下列实验：在含水印的图象中添加高斯噪声；对含水印的图象进行低通滤波处理；以及在含水印的图象中进行 JPEG 压缩、添加高斯噪声和低通滤波复合攻击，并按改进的算法提取出了水印图象. 从 9 份的水印信息中，任 3 份进行组合就可以得到一个水印图象，一共可以得到 $C_9^3=84$ 个水印图象，得到的水印图象越多，相当于做模糊统计的次数越多，根据模糊集计算得到的最终的水印图象也就越清楚，但需要的计算量也越大，因此应根据含水印图象受攻击的程度在水印的提取精度和计算量上进行适当的选取.

4　结　语

基于 Shamir 秘密共享思想的数字水印算法对于剪切攻击具有很好的鲁棒性，使得可以仅用原作品的若干部分就可以证明数字作品的原创者，不仅能指证数字作品的盗版行为，还能对付那些利用他人作品进行剪切拼凑现象。同时该算法对在含水印的图象中进行 JEPG 压缩、添加高斯噪声和低通滤波处理均具有较好的鲁棒性，并且使用基于模糊数学原理的改进算法，可以在水印的嵌入强度不变的情况下，提高水印抗这些攻击的强度. 该算法的不足是由于将 1 份水印信息分成了 9 份，降低了水印的嵌入量. 因此研究水印的嵌入量和鲁棒性的权衡问

题,以及改进算法提高水印嵌入量和鲁棒性是今后进一步的研究方向.

参 考 文 献

1 Van Schyndel R G, Tirkel A Z, Osborne C F. A digital watermark [A]. In: Proceedings of IEEE International Conference on Image processing[C]. Los Alamitos, California, USA, 1994:86~90.

2 Wolfgang P, Delp E. A watermark for digital image[A]. In: Proceedings of IEEE International Conference on Image Processing[C]. Los Alamitos, California, USA, 1996: 219~222.

3 Cox I J, Linnartz J P M G. Some general methods for tampering with watermarks [J]. IEEE Journal on Selected Areas in Communications, 1998,16(4):587~593.

4 Cox I J. Secure spread spectrum watermarking for multimedia [J]. IEEE Transactions on Image Processing, 1997.6(12):1673~1687.

5 卢开澄. 计算机密码学[M]. 北京: 清华大学出版社, 1998.

6 汪培庄,李洪兴. 模糊系统理论与模糊计算机[M]. 北京: 科学出版社, 1996.

牛少彰 1963 年生,1985 年和 1988 年在北京师范大学分别获得理学学士和硕士学位,现为北京邮电大学教授. 主要研究领域为图象处理、信息隐藏、数字水印、网络信息安全和应用数学.

钮心忻 1963 年生,副教授,1985 年和 1988 年在北京邮电大学分别获得工学学士和硕士学位,1997 年在香港中文大学获博士学位. 主要研究领域为信息安全、信号信息处理、信息隐藏和数字水印.

杨义先 1961 年生,教授,博士生导师,1999 年 3 月至今被聘为长江学者奖励计划特聘教授. 主要研究领域为密码学、网络信息安全、信号与信息处理. 已发表论文 300 余篇,出版专著 7 部.