一种新颖的复合型盲水印算法

陈 琼 伍祥生
(湖南师范大学信息技术系,长沙 410081)

摘 要 针对很多数字水印设计方案都是单水印嵌入的状况,提出了一种新的复合型图像水印技术。在图像作品里同时嵌入鲁棒水印和脆弱水印。这样,既对图像作品进行了版权保护,又能知道作品内容是否被篡改,实现了版权保护和内容认证的双重功能。两种水印的提取和检测工作都不需要原始图像就可以完成,是一种盲水印算法。仿真实验表明,该算法比较有效,具有很好的应用前景。

关键词 奇异值分解 鲁棒水印 混沌序列 脆弱水印
中图法分类号: TP309 **文献标识码**: A **文章编号**: 1006-8961(2008)03-0415-04

A New Algorithm of Compound Blind Watermarking

CHEN Qiong, WU Xiang-sheng
(*The Department of Information Technology, Hunan Normal University, Changsha* 410081)

Abstract To change the situation that many methods about watermarking were based on embedding one single watermark, we presented a new compound image watermarking method, which was embedding both robust watermark and fragile watermark to one image, so that we can not only convey the ownership, but also justify whether the source image is tampered. Therefore, a multipurpose watermarking system has been designed in this paper. In addition, both the watermarks need not the source image information during the process of extracting or detecting. That is to say, our algorithm is a blind one. Simulation results show that the algorithm we present is very effective, and can be widely used in practice.

Keywords singular value decomposition(SVD), robust watermarking, chaotic sequence, fragile watermarking

1 引 言

随着现代通信技术和网络技术的飞速发展,数字化产品的传播和交易变得越来越便捷,同时信息安全问题也日益显露出来。例如数字产品的侵权、盗版和任意篡改将对版权所有者造成不可估量的损失。如何有效地防范对数字产品的非法拷贝和传播,是保护知识产权中的一个重要问题。数字水印技术为保护多媒体信息的版权和保证多媒体信息的安全使用提供了一种很有效的手段。

最近这些年来,很多数字水印设计方案都是单水印的嵌入[1,2],即把一种水印信息嵌入到原始图像中,这种水印方案要么是实现版权保护,要么是实现内容认证。当我们既要对图像作品进行版权保护,又要知道作品内容是否被窜改时,就得设计一个多功能的数字水印系统,在图像作品中同时嵌入两种水印:一种用于版权保护,另一种用于内容认证。

本文提出了一种新的复合型水印技术。首先将原始载体图像进行分块,随机选取若干小块后,对每个小块进行奇异值分解(SVD),然后将经过置乱处理后的鲁棒水印嵌入到分解所得的酋矩阵中;接着,基于载体图像内容生成脆弱水印,使用混沌序列将其进行置乱处理后嵌入到载体图像的小波域高频系数中。无论是鲁棒水印还是脆弱水印,在水印的检测与提取过程中都不需要原始载体图像,这样,更利于实际中的应用。实验结果表明,该水印方案具有较好的不可见性,实现了版权保护和内容认证的双重功能。

基金项目:湖南省教育厅项目(04C204)
收稿日期:2006-06-19;**改回日期**:2006-09-07

第一作者简介:陈琼(1981~),女。湖南师范大学计算机软件与理论专业硕士研究生。研究方向为图像处理和数字水印。E-mail: cqwelldone@163.com

2 水印图像的生成

为了确保水印的安全性,通常需要对待嵌入的水印图像进行置乱。对图像进行置乱实际上就是对图像进行某种处理,使之出现混乱状态以消除图像的轮廓,然而,为了使图像复原,必须有严格的算法来记录置乱的过程。这里使用了混沌序列来完成水印的置乱处理。

2.1 混沌序列的产生

混沌序列[3]是非线性动力系统中具有确定性的序列,其统计特性类似随机过程,具有很好的遍历性,对初值敏感性高,更有利于信息的安全。在混沌动力系统中,Logistic 以它的遍历性和高度敏感性而备受关注,它可定义为

$$\chi_{k+1} = \mu\chi_k(1-\chi_k) \quad \mu \in (0,4], \chi_k \in (0,1) \tag{1}$$

式中,μ 为系数,k 代表时间。取初值 χ_0 为 0.75,μ 值为 3.93,其中可以将初值 χ_0 作为密钥 k_1,以提高系统的安全性。为了将产生的实数序列 $\boldsymbol{\chi}$ 转化为二值序列 $\boldsymbol{p}$,可以采用以下的方法将实数值序列分成两个部分:

$$\begin{cases} p_k = 1 & \chi_k > T \\ p_k = 0 & \text{其他} \end{cases} \tag{2}$$

式中,T 是阈值,这里取 0.5。

2.2 鲁棒水印的生成

采用含有版权信息的 $n \times n$ 大小的图像 $\boldsymbol{W}$ 作为原始鲁棒水印,将调制出的混沌二值序列 $\boldsymbol{p}$ 与水印图像 $\boldsymbol{W}$ 异或,即可得到加密处理后的鲁棒水印 $\boldsymbol{W}_1$。

2.3 脆弱水印的生成

将载体图像($M \times N$)进行 L 层离散小波变换。利用其中第 L 层的近似系数 $\boldsymbol{LL}_L$ 生成基于图像内容的水印序列:从生成的混沌实值序列 $\boldsymbol{\chi}$ 中选择 $(M/2^L) \times (N/2^L)$ 个元素生成实值混沌掩蔽矩阵 $\boldsymbol{M}_t$,将近似系数 $\boldsymbol{LL}_L$ 点乘 $\boldsymbol{M}_t$,即可得到调制后的矩阵 $\boldsymbol{LL}'_L$,再用阈值 T_1 将 $\boldsymbol{LL}'_L$ 的值划分为两个部分,分别用 0,1 表示并存储于矩阵 $\boldsymbol{W}_T$ 中;将二值化后的混沌序列 p 转化为二值混沌矩阵 $\boldsymbol{M}_b$ 后,与 $\boldsymbol{W}_T$ 中的对应元素模 2 相加,所得的矩阵 $\boldsymbol{W}_2$ 即为所需的脆弱水印。

3 复合型水印的嵌入策略

在图像作品中嵌入两种甚至是多种水印时,各种水印间的相互影响肯定是存在的。在本实验中,采取的方法是先将鲁棒水印嵌入到原始图像中,再在嵌入了鲁棒水印后的图像中嵌入脆弱水印。

3.1 矩阵的奇异值分解

一幅灰度图像从线性代数的角度来看,是一个具有非负值的矩阵。假定这幅灰度图像用 $\boldsymbol{I}$ 来表示,$\boldsymbol{I} \in \mathbf{R}^{N\times N}$,$\boldsymbol{R}$ 表示实数域。那么 $\boldsymbol{I}$ 的奇异值分解[1]定义为

$$\boldsymbol{I} = \boldsymbol{USV}^{\mathrm{T}} \tag{3}$$

式中,$\boldsymbol{U}$、$\boldsymbol{V} \in \mathbf{R}^{N\times N}$,两者都是酉矩阵,$\boldsymbol{S} \in \mathbf{R}^{N\times N}$是对角阵。

3.2 鲁棒性水印的嵌入

鲁棒水印 $\boldsymbol{W}_1$ 嵌入的基本思想就是先将水印图像置乱加密,再将载体图像分成互不重叠的 $m \times m$(如本文取 $m=8$)大小的块,随机地选择适当多的分块分别进行奇异值分解(SVD)后,再嵌入处理好的水印信息,反变换后即可得到含水印的图像。该方法是对分块进行 SVD 而不是对整个图像块,所以缩短了嵌入和提取水印的时间,这对于大图像来说效果尤其明显:

水印嵌入算法描述如下:

(1)按前述方法生成加密后的鲁棒水印。

(2)将原始图像 $\boldsymbol{I}$ 分成 $m \times m$ 大小的块,用密钥 k_2 产生一个随机序列用来选择足够多个子块来嵌入水印信息。

(3)对所选择的子块 $\boldsymbol{D}\{i,j\}$ 进行 SVD 分解,即 $[\boldsymbol{U}\quad \boldsymbol{S}\quad \boldsymbol{V}] = \mathrm{SVD}(\boldsymbol{D}\{i,j\})$。

(4)根据水印信息来修改矩阵的系数值。取出分解所得矩阵 $\boldsymbol{U}$ 并求出 $\boldsymbol{U}$ 矩阵的相邻元素 U_1,U_2 间的幅度之差 d;如果幅度差值的正负与嵌入的水印信息匹配则系数不变,否则就修改系数。

为了保证图像的质量并使水印算法具有更强的鲁棒性,$\boldsymbol{U}$ 的系数还可进行进一步修改。增加一个门限值 T_d 作为相邻系数间的最小幅度差。修改系数具体过程如下:

如果差值与水印位的正负关系匹配且其差值的幅度小于 T_d,则按下式修改系数:

$$U_1 = \mathrm{sgn}(U_1) * \mathrm{abs}(\mathrm{abs}(U_1) + \mathrm{sgn}(d) * (T_d - \mathrm{abs}(d))/2) \tag{4}$$

$$U_2 = \mathrm{sgn}(U_2) * \mathrm{abs}(\mathrm{abs}(U_2) - \mathrm{sgn}(d) * (T_d - \mathrm{abs}(d))/2) \tag{5}$$

如果不匹配,则

$$U_1 = \mathrm{sgn}(U_1) * \mathrm{abs}(\mathrm{abs}(U_1) - \mathrm{sgn}(d) * (T_d + \mathrm{abs}(d))/2) \tag{6}$$

$$U_2 = \mathrm{sgn}(U_2) * \mathrm{abs}(\mathrm{abs}(U_2) + \mathrm{sgn}(d) * (T_d + \mathrm{abs}(d))/2) \quad (7)$$

(5) 循环第 2 步至第 4 步直到水印全部嵌入到原始图像中,用奇异值反变换重构图像 $\boldsymbol{I}'$,它就是嵌入鲁棒水印后的图像了。

3.3 脆弱水印的嵌入

脆弱水印是在嵌入鲁棒水印后嵌入的,其嵌入步骤如下:

(1) 让载体图像 $\boldsymbol{I}'$进行 L 层离散小波变换(这里取 L 为 3)。按前述方法生成安全的基于内容的水印信号 $\boldsymbol{W}_2$。

(2) 取第 2 层小波变换的子带 $\boldsymbol{LH}_2$ 和 $\boldsymbol{HL}_2$ 中任意一个与水印图像相同大小的连续区域来嵌入脆弱水印 $\boldsymbol{W}_2$。为实现水印的盲提取,采用基于关系的嵌入方法:比较两个子带 $\boldsymbol{LH}_2$ 和 $\boldsymbol{HL}_2$ 对应系数。当水印位为 1 时,用 $\boldsymbol{LH}_2$ 中的系数减去 $\boldsymbol{HL}_2$ 中的系数,如果所得的差值小于 T_2(给定的阈值),则分别调整各个子带中对应系数的值以保证差值大于 T_2;当水印位为 0 时,用 $\boldsymbol{HL}_2$ 中的系数减去 $\boldsymbol{LH}_2$ 中的系数,用上述方法将所得差值与 T_2 进行比较,并相应地调整系数。

(3) 对修改后的矩阵进行逆离散小波变换,就可以获得同时嵌入了鲁棒水印和脆弱水印的图像 $\boldsymbol{I}''$了。

4 复合型水印的提取策略

复合型水印的提取是相对独立的。通过不同的水印算法,可以分别从嵌入了水印的图像 $\boldsymbol{I}''$中提取出鲁棒水印和脆弱水印。

4.1 脆弱水印的提取

脆弱水印的提取方法是将含水印的图像 $\boldsymbol{I}''$(可能受到某种攻击)进行 L 层小波变换。对子带 $\boldsymbol{LH}_2$ 和 $\boldsymbol{HL}_2$:如果 $LH_2(i,j)$ 和 $HL_2(i,j)$ 的差值大于阈值 T,则提取的水印位是 1;如果小于 $-T$,则提取的水印位是 0;当差值介于 $-T$ 和 T 之间时,意味着该区域被篡改了,这样就可以提取到水印序列 $\boldsymbol{W}_2^*$。分析篡改区域的方法是:对接收到的可能遭受攻击的水印图像 $\boldsymbol{I}''$进行 L 层小波变换;按照嵌入水印时类似的方法可以重建基于图像内容的水印序列 $\boldsymbol{W}_T^*$;比较 $\boldsymbol{W}_2^*$ 和 $\boldsymbol{W}_T^*$ 的异同,就可以知道可能被篡改的区域了。

4.2 鲁棒水印的提取

鲁棒水印的提取算法和其嵌入算法是对称的。

(1) 可能损坏的含水印图像 $\boldsymbol{I}''$分成 $m \times m$ 大小的块,利用密钥 k_2 产生随机序列来检测出嵌入了水印的子块 $D^*\{i,j\}$。

(2) 对每一个子块 $D^*\{i,j\}$进行 SVD 分解,得到 $U^*\{i,j\}$、$S^*\{i,j\}$、$V^*\{i,j\}$,计算出 $U^*\{i,j\}$相邻元素之间的关系,来判断嵌入的水印信息。

(3) 利用嵌入水印时的混沌置乱技术和提供的密钥 k_1 即得到可能已经失真的水印 $\boldsymbol{W}_1^*$。

5 实验结果

实验中采用了 256×256 的"Lena"图像作为原始载体图像 $\boldsymbol{I}$,用 32×32 大小的二值图像"湖南师大"作为含有版权信息的水印 $\boldsymbol{W}$,并使用 Matlab 来做仿真实验。提取出的水印图像 $\boldsymbol{W}^*$ 和原始水印图像 $\boldsymbol{W}$ 之间的相似性,使用专门针对二值图像水印的相似性测量标准[4],用 NC 值来表示,它的值越大表示两个图像 $\boldsymbol{W}$ 和 $\boldsymbol{W}^*$ 越相象。NC 定义如下:

$$NC = \sum_{m,n} (\boldsymbol{W}_{m,n}^* \oplus \widetilde{W}_{m,n})/(m \times n) \quad (8)$$

式中,⊕表示异或运算,~表示逻辑非运算。

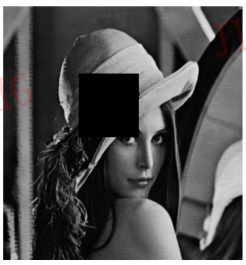
图 1(a)为原始图像 Lena,图 1(b)为采用本文算法嵌入两种水印后的图像。图 1(c)为原始鲁棒水印图像,图 1(d)为对鲁棒水印进行混沌置乱后的效果。图 1(e)为对含水印图像进行 64×64 的剪切攻击后的图像,图 1(h)和图 1(j)分别为受剪切攻击后检测出的篡改位置图和提取出的鲁棒水印,提取的鲁棒水印与原始鲁棒水印的相似度为 NC = 0.966 8。图 1(f)为含水印图像经过随意涂改后的效果,其篡改位置可以精确的定位,如图 1(i)所示,提取出来的鲁棒水印如图 1(k)所示,NC = 0.974 6。图 1(g)是含水印图像在受到 0.02 的椒盐噪声的影响后的图像,图 1(r)和图 1(s)分别为受椒盐噪声攻击后检测出的篡改位置图和提取出的鲁棒水印,提取的鲁棒水印与原始鲁棒水印的相似度为 NC = 0.886 7。图 1(l)至图 1(n)分别为受到质量因子等于 90、70、50 的 JPEG 攻击后检测到的篡改位置图。当压缩量增大时,检测到的篡改点明显增多,可以定义一个阈值 T 用来区分非恶意篡改和恶意篡改。当篡改点数多于阈值 T 时,则为恶意篡改;当篡改点数少于阈值 T 时,则为非恶意篡改。图 1(o)至图 1(q)分别为质量因子 Q = 90、70、50 时,提取出来的鲁棒水印,相似度 NC 值分别为 0.985 4、0.881 8、0.774 4。


(a) Lena 原图


(b) 嵌入两种水印后


(c) 原始水印


(d) 混沌置乱后的鲁棒水印


(e) 64×64 的剪切攻击


(f) 任意涂改攻击


(g)0.02 的椒盐噪声攻击


(h) 由图(e)检测出的篡改


(i) 由图(f)检测出的篡改


(j) 图(e)中提取出的鲁棒水印 $NC=0.9668$


(k) 图(f)中提取的鲁棒水印 $NC=0.9746$


(l) JPEG($Q=90$)篡改检测


(m) JPEG($Q=70$)篡改检测


(n) JPEG($Q=50$)篡改检测


(o) JPEG($Q=90$) $NC=0.9854$


(p) JPEG($Q=70$) $NC=0.8818$


(q) JPEG($Q=50$) $NC=0.7744$


(r) 由图(g)检测出的篡改


(s)由图(g)提取出的鲁棒水印，$NC=0.8867$

图 1 仿真实验结果

Fig. 1 Simulation results

6 结 论

该文提出了一种新颖的复合型图像水印技术，在图像作品里同时嵌入了鲁棒水印和脆弱水印。鲁棒水印采用分块奇异值分解技术嵌入，不仅使计算速度大大增快，而且非常鲁棒。脆弱水印则是基于图像本身内容生成的，能够精确地定位图像被篡改的位置。两种水印的提取和检测工作都不需要原始图像就可以完成，是一种盲水印算法。仿真实验结果表明，该算法比较有效，很好地满足了数字水印的透明性，同时实现了版权保护和内容认证两大功能，因此具有较好的应用前景。

参考文献(References)

1 Liu Rui-zhen, Tan Tie-niu. SVD based digital watermarking method [J]. Chinese Journal of Electronics, 2001, **29**(2): 168 ~ 171. [刘瑞祯，谭铁牛. 基于奇异值分解的数字图像水印方法[J]. 电子学报，2001，**29**(2)：168 ~ 171.]

2 Hu Jun-quan, Huang Ji-wu, Huang Da-ren. An algorithm for fragile watermarking based on HVS[J]. Chinese Journal of Electronics, 2003, **31**(7): 1057 ~ 1061. [胡军全，黄继武，黄达人. 一种基于HVS的图像易碎水印[J]. 电子学报，2003，**31**(7)：1057 ~ 1061.]

3 Sun Sheng-he, Lu Zhe-ming, Niu Xia-mu. The Technology and Application of Digital Watermarking [M]. Beijing: Science Press, 2004: 510 ~ 512. [孙圣和，陆哲明，牛夏牧. 数字水印技术及应用[M]. 北京：科学出版社，2004：510 ~ 512.]

4 Yang Hen-fu, Chen Xiao-wei. A robust image-adaptive public watermarking technique in wavelet domain[J]. Journal of Software, 2003, **14**(9): 1652 ~ 1660. [杨恒伏，陈孝威. 小波域鲁棒自适应公开水印技术[J]. 软件学报，2003，**14**(9)：1652 ~ 1660.]