

一种安全多功能图像水印系统模型与算法

朱从旭 陈志刚

(中南大学信息科学与工程学院 长沙 410083)

摘要 为提出一种安全多功能的图像水印系统,首先利用3维统一混沌系统的混沌序列 Y 、 Z 生成可见水印的嵌入系数,同时在图像的空域嵌入可见水印,以实现版权通知功能;然后在含有可见水印的图像中加入第1种不可见水印,以实现版权保护功能;最后再在消除可见水印的图像中加入第2种不可见水印,以实现非授权拷贝跟踪。两种不可见水印的嵌入位置都由统一混沌系统的混沌序列 X 、 Y 随机选择,并基于一种新的双参数量化技术在选择的图像子块小波域低频系数中嵌入水印,并能进行盲提取。实验结果表明,可见水印能被授权用户完全消除,但很难被非授权用户消除;而不可见水印对图像的质量影响很小,并对常规图像处理操作具有良好的鲁棒性。

关键词 水印模型 提升小波变换 统一混沌系统 可见水印 不可见水印

中图法分类号:TP391.9 文献标识码:A 文章编号:1006-8961(2008)05-0894-06

A Security Multipurpose Image Watermarking System Model and Algorithm

ZHU Cong-xu, CHEN Zhi-gang

(School of Information Science and Engineering, Central South University, Changsha 410083)

Abstract To develop a security multipurpose image watermarking system, we use the 3D unified chaotic system sequences Y and Z to generate embedding coefficients of visible watermarks, and embed the visible watermarks in the image spatial domain to achieve the goal of copyright notification. Then we embed the first invisible watermarks in the image with embedded visible watermarks to obtain the aim of copyright protection. After removing the visible watermarks, the second invisible watermarks are embedded in the image to obtain the aim of unauthorized copy tracing. Two kinds of invisible watermarks' embedding positions are selected randomly by unified chaotic system sequences X and Y , based on a novel dual parameters quantization technique. Both watermarks that can be blindly extracted are embedded in the lifting wavelet transform (LWT) domain of those selected blocks. Simulation results show that the visible watermarks can be removed entirely by authorized users and can hardly be removed by unauthorized users. The impact of the invisible watermarks on the image quality is slight, and the invisible watermarks are robust to common image processing operations.

Keywords watermarking model, lifting wavelet, unified chaotic system, visible watermark, invisible watermark

1 引言

随着网络通信技术的飞速发展,互联网已成为发布信息的重要途径,如今各种形式的多媒体数字作品已开始通过网络对外发布,电子商务也日益普及,随之而来的数字媒体版权保护和防止非授权滥

用问题已成为一个迫切需要解决的课题。为了避免版权所有者和合法用户蒙受经济损失,近年迅速发展起来的数字水印技术为解决该问题提供了一种新的有效方法。但目前大多数研究者提出的图像数字水印一般为单一的不可见水印,而关于可见水印^[1-4]的文献报道却很少。由于可见水印可以用于明确的版权通知和产品广告宣传,比如,媒体制作者

基金项目:国家自然科学基金项目(60573127);教育部博士点专项科研基金资助项目(20040533036)

收稿日期:2006-08-28; **改回日期:**2006-12-08

第一作者简介:朱从旭(1963~),男。1992年7月获湖南师范大学物理系硕士学位,2006年11月获中南大学信息科学与工程学院博士学位,副教授。主要研究领域为图像处理、多媒体信息安全等。已发表重要论文40余篇。E-mail:zhucong xu@126.com

可以将含有可见水印的作品放到网页上做宣传,并表明版权,因此用户可以公开下载含可见水印的作品样品,感兴趣的用户还可以通过信用卡购买消除可见水印的作品。罗永等最近提出的一种可见数字水印^[3],不但具有公开表明图像版权的作用,同时可消除可见水印所需要的信息隐藏在图像的小波变换域,这样合法用户可首先通过密钥提取消除可见水印所需的信息,然后实现可见水印的消除,恢复出不含可见水印的图像。但文献[3]算法,其消除可见水印后的图像质量指标——峰值信噪比(PSNR)值偏低,且单纯依靠半透明水印来表明版权是不够的,因为它不能充分保护图像的版权。文献[4]基于离散余弦变换(DCT)提出了一种同时拥有图像版权通知和版权保护双重功能的水印算法,但文献[4]的方案仍然存在下列问题:对于授权用户在得到不含可见水印的作品后再进行非法复制转售的行为无法跟踪,因为无法找到那个将作品非法再传播的人。一旦授权用户得到不含可见水印的作品,那么他就能由不含可见水印的图像推导出可见水印的嵌入系数,也就能够提取图像中的可见水印,并盗取该可见水印的版权作为它用。

本文提出了一种安全多功能水印系统模型,其不仅可实现图像的版权通知、版权保护和非授权拷贝跟踪三重功能,且算法具有密码学意义的安全性。

2 相关多功能水印算法的安全性分析

在文献[4]提出的双重水印算法中,可见水印所采用的嵌入公式为

$$\hat{A}_{i,j} = \alpha_{k,l} \times A_{i,j} + (1 - \alpha_{k,l}) \times \frac{V_{i,j}}{255} A_{i,j} \quad (1)$$

其中, $A_{i,j}$ 、 $V_{i,j}$ 和 $\hat{A}_{i,j}$ 分别为原始灰度图像、可见水印图像和含可见水印的灰度图像中位置 (i,j) 处的像素值, $\alpha_{k,l}$ 为原始灰度图像中第 (k,l) 个 8×8 子块的归一化方差,该方差作为嵌入系数。设嵌入双水印后的最终图像为 \hat{A} , \hat{A} 是公开可得的。下面将分析指出,这种可见水印不能抵御某些攻击。

假设某用户以合法方式得到不含可见水印的图像 B ,则对比 B 和 \hat{A} 的每个 8×8 子块,就很容易判断 \hat{A} 中那些与图像 B 中像素值有差异的子块就是嵌入了可见水印的子块;接着就可以由消除了可见水印的图像 B 计算出这些曾经嵌入了可见水印的子块的方差

$\sigma_{k,l}$;而 σ_{\min} 就是这些 $\sigma_{k,l}$ 中的最小值。虽然方差值最大的子块是在那些嵌入了不可见水印的子块中,这将导致不能直接求出 σ_{\max} ,但却不难通过穷举法推导,同时还可以求得可见水印。推导算法步骤如下:

(1)在嵌入可见水印的子块中先任取一个 8×8 子块,然后从选取的子块中取第1个像素点;

(2)因为该点的像素值 $\hat{A}_{i,j}$ 和 $A_{i,j}$ 已经知道,而可见水印像素的取值 $V_{i,j}$ 则有限: $0 \leq V_{i,j} < V_{\max} = 255$, $V_{i,j}$ 的可能取值共256种,所以穷举256个值,就可计算得到该子块的256种归一化方差的可能值 $\alpha_1(n)$;

(3)对该子块的所有点重复步骤(2),并由各点求出子块归一化方差的可能值,共将得到64组解: $\alpha_1(n), \alpha_2(n), \dots, \alpha_{64}(n), n = 1, 2, \dots, 256$;

(4)这64组解中必然存在一个以上有意义的公共解,设有 p 个公共解($p \geq 1$),这些公共解 $\alpha(m)$ 都有可能是该子块的归一化方差, $m = 1, 2, \dots, p$;

(5)由该子块归一化方差的可能值 $\alpha(m)$ 分别结合图像的子块方差最小值 σ_{\min} (已知)和该子块的绝对方差 $\sigma_{k,l}$,通过式(1)计算即可得到图像子块方差最大值的可能取值 $\sigma_{\max}(m), m = 1, 2, \dots, p$ 。

(6)得到 $\sigma_{\max}(m)$ 、 σ_{\min} 及每个子块的绝对方差 $\sigma_{k,l}$ 后,即可得到那些嵌入了可见水印的所有子块的归一化方差 $\alpha_{k,l}(m)$ 共有 p 个版本($m = 1, 2, \dots, p$)。

(7)由各子块 p 个版本的归一化方差 $\alpha_{k,l}(m)$ 值,通过式(1)即可得到 p 个版本的可见水印值序列 $\{V_{i,j}(m), m = 1, 2, \dots, p\}$ 。

最后,对所得的 p 个版本可见水印值序列进行判断,删除那些包含无意义值($V_{i,j}(m) < 0$ 或 $V_{i,j}(m) > 255$)的版本,即可得到真正的可见水印序列,该序列构成一幅可见水印图像的一部分;组成可见水印图像的另一部分像素的位置由原始图像和嵌入可见水印后图像的像素值完全相同的子块位置确定。在这些位置中,要么是 $V_{i,j} = 255$,要么是 $\alpha_{k,l} = 1$ 。考虑到原始图像中同时具有最大方差值($\alpha_{k,l} = 1$)的子块数不会很多,因此完全可以认为可见水印图像另一部分像素的值都是255,这样处理最多可能导致对个别子块像素值估计错误,但不影响整个可见水印图像。

分析以上穷举算法的时间开销,主要是推算图像子块最大方差值的时间,设原始图像大小为 $N \times N$,若分成 $N \times N / (8 \times 8)$ 个子块,按原算法的要求,则嵌入可见水印的图像中至多只能有 $3/4$ 的块(亦即 $3/4$ 的像素)发生变化,因此算法的时间复杂度

为 $O(3/4 \times N \times N \times 256)$, 即 $O(N \times N)$ 。对于一般图像来说, $N \leq 512$, 这个时间开销并不大。

3 提出的多功能水印系统模型和算法

3.1 系统模型框架

为了解决合法用户在得到不含可见水印图像后可能非法复制的问题, 本文方案要求用户在购买图像产品时, 要提供一个有效的用户注册号, 并进行注册登记。注册成功后将自动消除图像的可见水印, 并将同时用户的注册号以二值图像形式作为另一个不可见水印嵌入载体图像, 这样不同用户得到的图像中就加入了不同的用户水印, 如果作品被滥用(非授权拷贝), 则版权所有者就可以找出那个应负责任的用户。本文提出的多功能水印系统模型如图 1 所示。

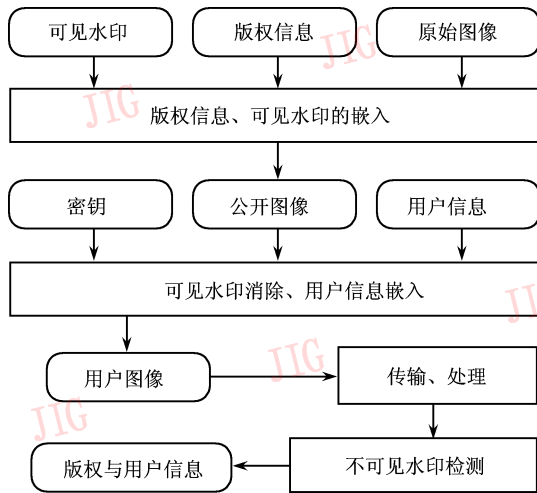


图 1 本文提出的多功能水印系统模型

Fig. 1 The proposed multipurpose watermarking system model

3.2 统一混沌系统和提升小波变换

混沌是一种貌似无规则的运动, 它是在确定性非线性系统中, 不需附加任何随机因素也可出现的一种类似随机性行为(内在随机性)。由于混沌序列具有对初始条件的敏感性、伪随机性和无周期性, 并可使其与密码学中的扩散、混合和随机等要求相吻合, 因此混沌系统在信息加密、置乱的应用中有很好的应用前景。目前文献中用于信息加密的混沌系统多为 1 维系统, 例如广为使用的 Logistic 系统, 但由于 1 维系统存在密钥空间小、安全性差的缺点, 因此为了加强 1 维混沌密码系统的安全性, 一般应对 1 维系统进行处理, 或者使用高维混沌系统。2002 年, 吕金虎、陈关荣等人提出了一个新的 3 维混沌系

统^[5], 该系统将 Lorenz 系统和 Chen 系统连接起来, 而 Liu 系统只是它的一个特例, 故称其为统一混沌系统, 其数学模型为^[5]

$$\begin{cases} \dot{x} = (25\alpha + 10)(y - x) \\ \dot{y} = (28 - 35\alpha)x - xz + (29\alpha - 1)y \\ \dot{z} = xy - (8 + \alpha)z/3 \end{cases} \quad (2)$$

其中, 系统参数 $\alpha \in [0, 1]$, 在此范围内系统(2)具有全域性混沌特性。本文将采用系统(2)获得 3 个离散混沌序列 X, Y, Z 来加强水印系统的安全性。

基于提升(lifting)结构的快速小波变换^[6]克服了传统小波变换的一些缺点, 被称为第 2 代小波变换。这种提升小波变换算法的基本思想是将传统小波变换 Mallat 算法中的每一级滤波运算分解为分裂(split)、预测(predict)和更新(update)3 个过程。实践表明, 提升小波变换在提高运算速度和保证图像无损变换方面具有明显优越性。

3.3 版权通知和保护水印的嵌入

本文用于版权通知的可见水印是一幅与宿主图像等大的灰度图像, 可采用如式(3)所示的加权融合方式将可见水印嵌入到宿主图像空域。

$$\hat{A}_{i,j} = (\alpha_{i,j} + \beta_{i,j}^2 - \alpha_{i,j}\beta_{i,j}^2)A_{i,j} \quad (3)$$

其中, $A_{i,j}, \hat{A}_{i,j}$ 分别为宿主图像中点 (i, j) 处嵌入可见水印前后的像素灰度值; $\alpha_{i,j}$ 为位置 (i, j) 处的嵌入权重系数; 可见水印图像中点 (i, j) 处的像素值与其最大像素值之比为 $\beta_{i,j} = V_{i,j}/V_{\max}$ 。由式(3)可知, 由于对应于可见水印取最大像素值点的 $\beta_{i,j} = 1$, 因而载体图像的像素值不变($\hat{A}_{i,j} = A_{i,j}$), 因此, 可以利用这些点嵌入另一种版权保护水印。本文的嵌入权重系数 $\alpha_{i,j}$ 由统一混沌系统的混沌序列 Y, Z 控制产生, $\alpha_{i,j}$ 的取值数目为无穷, 但只要要求以下一个范围: $r_1 \leq \alpha_{i,j} \leq r_2$, 其中 r_1 和 r_2 是两个预定常数。可见水印嵌入算法步骤如下:

(1) 初始化参数 N (宿主图像大小为 $N \times N$), 混沌系统初值 (x_0, y_0, z_0) 、系统演化起止时刻 t_s 和 t_e (长度与 N 有关); 嵌入权重系数范围 $[r_1, r_2]$ 。

(2) 利用变步长 4 阶 5 级 Runge-Kutta-Fehlberg 算法来求解给定初值的混沌系统微分方程组, 即可得到以下 3 个长度为 N 的混沌序列: $X = \{x(i)\}$, $Y = \{y(i)\}$, $Z = \{z(i)\}$, $i = 1, 2, \dots, N$ 。

(3) 对嵌入点 (i, j) , 计算嵌入权重系数 $\alpha_{i,j}$:

$$\text{temp} = \lfloor (|x(i) \times y(j)| - |x(i) \times y(j)|) \times 10^3 \rfloor \quad (4)$$

$$\alpha_{i,j} = (r_2 - r_1) \times temp/999 + r_1 \quad (5)$$

并计算 $\beta_{i,j} = V_{i,j} / V_{max}$ 。

(4) 利用式(3)将点 (i,j) 处的水印像素嵌入到

载体图像的点 (i,j) 处来得到载体图像像素值 $\hat{A}_{i,j}$ 。

(5) 重复步骤(3)~步骤(4),对其他水印像素进行嵌入,直到全部可见水印嵌入完毕。

本文用于版权保护的鲁棒水印为一幅二值文字图像 $W_R = \{w_r(i,j), 1 \leq i \leq L_1, 1 \leq j \leq L_2\}$ (下角 R 代表 robust)。对每个不可见鲁棒水印像素 $w_r(i,j)$, 首先要在载体图像中随机选择一个未嵌入可见水印的 8×8 子块(称可嵌块), 原始图像的可嵌块位置由可见水印中像素均值为 V_{max} 的子块确定。而随机选择可嵌块的方式则由统一混沌系统的序列 X 和 Y 来控制, 并运用 2 维混沌序列排序实现地址置乱。若将载体图像的一个 8×8 子块看成一个点, 则可以用 $b(i,j)$ 表示第 (i,j) 个子块。从混沌序列 X 和 Y 中分别取以下两个长度为 $N/8$ 的子序列: $X_0 = \{x(i)\}, i = 1, 2, \dots, N/8; Y_0 = \{y(j)\}, j = 1, 2, \dots, N/8$; 并分别对两子序列进行排序, 若 X_0 中的第 i 个值在其有序序列中的位置序号为 $p_x(i)$, Y_0 中的第 j 个值在其有序序列中的位置序号为 $p_y(j)$, 则由于实值混沌序列的无周期性, 因此 i 与 $p_x(i)$ j 与 $p_y(j)$ 之间有一一对应关系。根据如下思路随机选择可嵌子块: 在版权水印图像中位置 (i,j) 处取一像素点, 首先将其行、列下标分别映射到与混沌序列 X_0 和 Y_0 对应的位置序号对 $(p_x(i), p_y(j))$; 然后将由坐标位置 $(p_x(i), p_y(j))$ 决定的子块 $b(p_x(i), p_y(j))$ 作为水印嵌入候选子块。如果该子块 $b(p_x(i), p_y(j))$ 为不可嵌子块, 则按一定顺序考察下一组位置坐标 $(p_x(\hat{i}), p_y(\hat{j}))$, 如此反复, 直至找到的子块 $b(p_x(\hat{i}), p_y(\hat{j}))$ 为可嵌子块, 再将鲁棒水印嵌入至该子块的小波低频系数。具体的嵌入方法则采用一种新的双参数量化嵌入算法(如图 2 所示)。

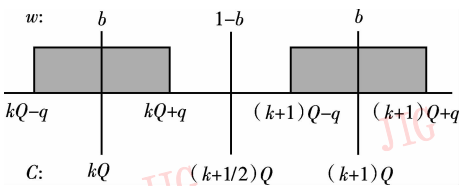


图 2 双参数量化水印嵌入

Fig. 2 Watermark embedding with dual quantization parameters

该量化方法考虑了有意义二值水印图像中常常

存在的 0、1 比特数量不均的特性, 将水印图像中数目占多数的比特定义为优值比特, 用 b 表示, 而将占少数的比特定义为劣值比特, 用 $(1-b)$ 表示, (Q, q) 为双量化参数。若嵌入的水印 w 为优值比特 b , 则修改宿主图像的对应系数 C 到一个最近的区间 $[kQ - q, kQ + q]$ 范围内; 若嵌入的水印 w 为劣值比特 $(1-b)$, 则修改宿主图像的对应系数 C 到一个最近的数值 $(k+1/2)Q$, 其中 k 为整数。可证明: ①对优值比特和劣值比特宿主图像系数的最大修改度分别为 $(Q/2 - q)$ 和 $Q/2$; ②对优值比特而言, 在降低对宿主图像系数修改幅度的同时, 还降低了系数被修改的概率; ③在嵌入强度一定的条件下, 双参数量化嵌入算法可以整体降低对宿主图像的修改程度和提高宿主图像的视觉质量。

3.4 可见水印的消除与用户水印的嵌入

可先利用相同的混沌初值来产生相同的混沌序列 Y, Z , 由序列 Y, Z 生成参数 $\alpha_{i,j}$; 然后根据式(3), 即可计算出不含可见水印的宿主图像的像素值 $A_{i,j}$; 最后求出所有位置的像素值 $A_{i,j}$ 后, 即可得到消除可见水印的图像。非法用户由于不掌握混沌系统初始状态参数, 因此不能生成相同的混沌序列, 于是不能每次得到正确的参数 $\alpha_{i,j}$, 也就不能正确消除可见水印。

用户水印是标识购买者身份的另一种不可见水印, 它可实现对用户非授权传播数字产品的行为进行跟踪, 也是一种鲁棒水印。这里嵌入用户标识水印的方法与前面嵌入版权水印的方法相同, 只是在确定嵌入子块的时候, 应该找那些曾经包含可见水印的子块。当可见水印被消除后, 再将购买者的标识嵌入这些子块位置, 使得最后发放到购买用户手中的产品同时包含版权信息和用户信息两种不可见水印, 两者的嵌入位置互不相同。

3.5 不可见水印的提取

提取不可见水印的过程是嵌入信息的逆过程, 即先用与嵌入时相同的密钥生成混沌序列, 找到两种不可见水印的嵌入子块位置; 然后将该子块做三级提升小波变换; 最后再运用双参数反量化操作从含有水印的小波低频系数 \hat{C}_w 中提取水印 \hat{w} , 这里提取水印不需要参考原始图像, 属盲提取。双参数反量化提取水印算法的具体实现规则如式(6)和式(7)描述。

$$\hat{r} = |\hat{C}_w| - \lfloor |\hat{C}_w| / Q \rfloor \times Q \quad (6)$$

$$\hat{w} = \begin{cases} b & \text{如果 } \hat{r} - Q/2 > (Q/2 - q)/2 \\ 1 - b & \text{其他} \end{cases} \quad (7)$$

4 实验结果与分析

实验采用 Matlab7 仿真平台。原始载体图像和可见水印均为 512×512 pixels 的 8bits 灰度图像;作为版权保护的鲁棒水印为 32×32 pixels 的“印”字二值图像;作为客户标识的鲁棒水印为 12×85 pixels 的数字二值图像,分别如图 3(a)~(d)所示。



图 3 原始宿主图像和 3 种水印

Fig. 3 The original cover image and three watermark images

4.1 可见水印的能消除性与安全性

对于 Goldhill 载体图像,选取如下参数: $r_1 = 0.25, r_2 = 0.50, Q = 120, q = 12$;每一点产生一个不同的嵌入系数,其所得到的嵌入可见水印和版权标识水印后的图像如图 4(a)所示。实验得到的正确消除了可见水印后的图像与仅含版权水印的图像具有相同的 PSNR 值(41.954 9dB)。在消除可见水印的图像中再嵌入用户标识水印后的图像如图 4(b)所示(PSNR 值为 39.333 3dB)。采用其他经典图像实验,得到的发行图像 PSNR 值如表 1 所示;表 1 同时也列出了文献[3]发行图像最佳的 PSNR 值。注意,本文的发行图像含有两种不可见水印,水印容量为 204 4bits;而文献[3]的发行图像则含有 30bits 的二值序列加上 33bits 的纠错码,水印容量仅为 63bits。在不可见水印容量远大于文献[3]水印容量的情况下,本文算法的发行图像质量指标比文献[3]发行图像的质量还要好。其原因在于文献[3]的双重水印,其嵌入位置重叠,水印互相影响,即使拥有正确密钥也不可能完全消除原可见水印。而本文的可见水印则可以被完全消除;此外,本文的不可见水印采用了双参数(Q, q)量化嵌入算法,起到了优化载体图像视觉质量的作用。若采用通常量化嵌入算法,则上述发行图像的 PSNR 值只有 37.821 4dB。



(a) 含原始双水印的图像 (b) 正确消除了可见水印后的图像

图 4 可见水印消除前后的图像

Fig. 4 The image before and after removing visible watermark

表 1 合法消除可见水印后图像质量的比较

Tab. 1 Compare of image quality after removing visible watermarks legally

图像	PSNR 值(dB)	PSNR 值 ^[3] ($t = 1.230\ 174$) (dB)
Lena	39.781 7	36.137
Barb	39.702 8	36.513
Boat	39.395 0	36.726
Goldhill	39.333 3	36.162
Mandrill	39.124 9	36.522

图 5 所示为在消除可见水印时所用的参数仅只有混沌系统状态参量 $x(0)$ 与正确值相差 10^{-12} 的结果,图 5(a)是消除可见水印的宿主图像(PSNR 值仅为 30.274 7dB),图 5(b)是非法提取的版权水印。由图(5)可见,非法消除可见水印的图像质量很差,而且非法用户不能提取正确的版权水印。这对非法用户都是不利的。



(a) 非法消除可见水印的图像 (b) 非法提取的版权水印

图 5 $x(0)$ 相差 10^{-12} 时水印的消除和提取结果

Fig. 5 The result of removing or extracting watermarks with $x(0)$ has a discrepancy of 10^{-12}

用文献[4]算法嵌入的可见水印是不能盲消除的,因为消除可见水印需要知道原始图像的每个子块归一化方差,而本文算法在消除可见水印时则不需要

原始图像,而且可以从理论和实验证明,对于相同的嵌入系数误差,采用本文方法消除可见水印的效果比使用文献[4]方法的效果更差,这对非法者更不利。

安全性分析:要想完全去除可见水印,则必须准确知道图像每个像素点的嵌入权重系数。根据本文算法产生权重系数的公式(式(5)),对于图像的每一个像素点,若取混沌序列值小数点后 m 位数字来随机产生权重系数,则每点产生的权重系数可能值有 10^m 种;这样整个图像像素嵌入权重系数的组合数则有 $10^{m \times (N \times N)}$ 种。本文载体图像的 N 值为512, $m=3$,该组合数为 $10^{3 \times (512 \times 512)}$ 种。对比文献[3]的系数分配组合数目 $h^{(N \times N)}$,其中 h 为一个确定系数序列的长度, h 一般很小,如文献[3]的 h 值只取2;可见本文的嵌入权重系数组合数远大于文献[3]的系数分配组合数目,且本文的嵌入权重系数组合数随 m 的增长率为指数函数增长率,即 $d(10^{m \times N \times N})/dm = N^2 \times 10^{m \times N \times N} \times \ln 10$;而文献[3]的嵌入权重系数组合数随 h 的增长率则是按幂函数的速度增长率,即 $d(h^{N \times N})/dh = N^2 \times h^{N \times N - 1}$;可见本文的嵌入权重系数组合数随 m 的增长速度更快。而作为密钥的混沌系统初值是3个实数,由于密钥空间巨大,足以抵抗现有硬件条件下的强力攻击,所以,本文算法具有密码学意义的安全性。

4.2 不可见水印的鲁棒性

发行图像在使用传播过程中,可能遭遇各种图像处理 and 信道噪声的攻击,本文通过实验模拟这些攻击,然后从受到攻击的载体图像中提取两种不可见水印,提取的结果如图6所示。同时分别计算了提取的水印与原始水印之间的归一化相似度系数 NC_1 、 NC_2 。



图6 两种不可见水印的鲁棒性提取结果

Fig. 6 The robustness of two invisible watermarks

以上实验表明,不可见水印对常规图像处理具有鲁棒性。特别是抵抗JPEG压缩的鲁棒性相当强,当JPEG压缩质量参数在24以上时,实验提取的两种不可见水印均可以达到100%的准确度。

5 结论

本文提出了一种基于统一混沌系统和提升小波变换的安全多功能图像水印系统模型及算法。该算法具有如下特点:(1)突破了现有多功能水印系统只有双重功能的局限性,实现了图像的版权通知、版权保护和非授权拷贝跟踪三重功能。(2)本文水印算法采用了高维非线性混沌系统进行处理,具有密码学意义的安全性,其既可使非授权用户很难消除可见水印,也不能提取不可见水印;(3)由于不可见水印的嵌入采用了一种新的基于水印比特0、1分布特性的双参数量化算法,从而使水印在保持相同鲁棒性的前提下,提高了载体图像的视觉质量;(4)采用了提升小波变换,使算法具有运算速度快、存储开销小的优越性。本文算法也很容易推广应用于彩色图像。这些特点大大提高了该多功能水印系统的实用性。

参考文献 (References)

- Jiang Shou-da, Lu Zhe-ming, Wu Hao-tian. DCT based multipurpose watermarking technique for image copyright notification and protection [J]. Journal of Harbin Institute of Technology (New Series), 2004, 11(3): 237 ~ 239.
- Lu Zhe-ming, Wu Hao-tian, Xu Dian-Guo, et al. A multipurpose image watermarking method for copyright notification and protection [J]. IEICE Transactions on Information and Systems, 2003, E86-D(9): 1931 ~ 1933.
- Luo Yong, Cheng Li-zhi, Wu Yi, et al. Translucent digital watermark based on wavelets and error-correct code [J]. Chinese Journal of Computers, 2004, 27(11): 1533 ~ 1539. [罗永, 成礼智, 吴翊等. 小波变换结合纠错编码的半透明数字水印[J]. 计算机学报, 2004, 27(11): 1533 ~ 1539.]
- Lu Zhe-ming, Wu Hao-tian, Liu Zhong-ren, et al. A multipurpose color image watermarking algorithm for copyright notification and protection [J]. Acta Electronica Sinica, 2004, 32(5): 778 ~ 781. [陆哲明, 吴昊天, 刘忠仁等. 一种用于版权通知和保护的多功能彩色图像水印算法[J]. 电子学报, 2004, 32(5): 778 ~ 781.]
- Lu Jin-hu, Chen Guan-rong, Zhang Suo-chun. The compound structure of a new chaotic attractor [J]. Chaos, Solitons and Fractals, 2002, 14(5): 669 ~ 672.
- Daubechies I, Sweldens W. Factoring wavelet transforms into lifting steps [J]. Journal of Fourier Analysis and Applications, 1998, 4(3): 247 ~ 269.