

基于 U 系统的数字图象水印技术

丁 玮¹⁾ 闫伟齐²⁾ 齐东旭^{2),3),4)}

¹⁾(联想电脑公司战略发展研究部, 北京 100085)

²⁾(中国科学院计算技术研究所 CAD 开放研究实验室, 北京 100080)

³⁾(北方工业大学 CAD 研究中心, 北京 100041) ⁴⁾(澳门科技大学信息学院, 澳门)

摘 要 在研究 U 系统的基础上, 提出了一种在图象中植入数字水印的简便易行的方法, 介绍了分段线性 U 系统及其性质, 并将其扩展为分段 k 次 U 系统; 在讨论如何使用分段线性 U 系统对数字图象进行分解的基础上, 提出了基于 U 系统的数字图象水印方法, 并给出了相应的实验结果, 实验表明这种算法是可行的。

关键词 U 系统 数字图象水印 图象信息隐藏

中图法分类号: TP391.41 **文献标识码:** A **文章编号:** 1006-8961(2001)06-0552-06

Digital Image Watermarking Based on U-System

DING Wei¹⁾, YAN Wei-qi²⁾, QI Dong-xu^{2),3),4)}

¹⁾(Department of Strategic Development, Legend Group, Beijing 100085)

²⁾(CAD Laboratory, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080)

³⁾(CAD Research Center, North China University of Technology, Beijing 100041)

⁴⁾(Macao University of Science and Technology, Macao)

Abstract This paper present a novel easy and effective algorithm to plant digital watermark into digital images, this algorithm is different to general watermarking methods based on spread spectrum, because a new orthogonal base based on piecewise polynomial is constructed. The watermark based on this algorithm can resist energy loss caused by lose compression of digital image. In the first part of this pper, piecewise linear U-system and its properties will be introduced respectively, corresponding graphs are shown, too. Following this part, how to generalize this algorithm to piecewise k-degree U-system is discussed; In the third part fo this paper, based on decompose digital image by piecewise linear U-system, a kind of digital image watermarking scheme will be provided, the process of this algorithm is introduced step by step. By the end of this paper, some corresponding experimental results based on U-system will be listed. The experimental results demonstrate the algorithm is reliable.

Keywords U-System, Digital image watermarking, Image information hiding

0 引 言

随着互联网的迅速发展和媒体的进步, 数据隐藏(Data Hiding)^[1]问题越来越引起人们的兴趣和关注. 如针对图象信息而言, 人们已经开始研究种种“所见非所得”的技术. 从原则上讲, 经典的加密方

法虽然都可以用于图象的信息隐藏, 但却不见得适用, 因为图象数据量庞大, 并且具有自相关性, 而经典的加密方法对此往往不予考虑, 可是事实上, 这些图象本身的特性不容忽视, 并且是可以利用的. 此外, 图象作为一种直观的信息表达方式, 还具有可以利用的“迷惑性”, 即如果能够在图象中隐藏某些重要信息(声音, 图象, 文字等), 而又对图象本身损失

很小,那么攻击者就有可能被图象表面所迷惑,即使他知道图象中藏有某些重要信息,不知道提取算法也无可奈何。

近年兴起的数字水印技术就是这样一种图象信息隐藏技术。它主要应用于电子出版物的版权保护领域^[2]。著作权拥有人如果把代表自己身份的特征图象植入电子出版物的某些关键图象中,那么,就可以在适当的时候从中提取特征图象来证明自己对作品的拥有权,这个特征图象就是我们所说的数字水印。一般地,对数字水印的要求主要有以下两点:

(1) 隐藏性,这是对数字水印的基本要求,即数字水印植入图象后,人眼无法把它直接地从图象中识别出来;

(2) 鲁棒性,即水印的抗攻击能力,要求水印在经过通用的变换、滤波等图象处理操作之后仍然可以被提取;

此外,还要求数字水印植入后对原始图象影响不能太大。

目前,水印植入方法主要是从原始图象的位置空间、色彩空间、频率空间出发,寻求水印植入位置和表示方法。

本文基于U系统,提出了一种的简便易行的在图象中植入数字水印的方法。

1 分段线性U系统

对于给定的平方可积函数,可以将之展开为相应的级数

$$f(x) \sim \sum_{j=0}^{\infty} a_j \varphi_j(x), a_j = \langle f, \varphi_j \rangle = \int_0^1 f(x) \varphi_j(x) dx \quad (1)$$

其中, $\{\varphi_j(x)\}$ 是 $[0, 1]$ 上的正交函数系(如 Fourier 三角函数系、Haar 函数系、Walsh 函数系等)中的一种。显然,在实际计算中,因为对于用任意有限项级数表示的 $f(x)$ 都可能导致不理想的结果,所以应该根据函数 $f(x)$ 的性质来选择选取光滑性或间断性的函数做有限逼近,但在实际问题中,由于信号往往既包含渐变(光滑)的部分,又包含突变(间断)的部分,因此如果能够找出一类自适应的正交函数系来兼顾光滑与间断,就能很好地逼近信号。

U系统是80年代初期提出的一类分段线性正交函数系,后来被推广到分段 k 次多项式的一般情形^[3~5],其中分段线性U系统定义如下

$$U_0(x) = 1, U_1(x) = \sqrt{3}(1 - 2x),$$

$$0 \leq x \leq 1$$

$$U_2^1(x) = \begin{cases} \sqrt{3}(1 - 4x) & 0 \leq x < \frac{1}{2} \\ \sqrt{3}(4x - 3) & \frac{1}{2} < x \leq 1 \end{cases}$$

$$U_2^2(x) = \begin{cases} (1 - 6x) & 0 \leq x < \frac{1}{2} \\ (5 - 6x) & \frac{1}{2} < x \leq 1 \end{cases} \quad (2)$$

$$U_{n+1}^{(2k-1)}(x) = \begin{cases} U_n^{(k)}(2x) & 0 \leq x < \frac{1}{2} \\ U_n^{(k)}(2 - 2x) & \frac{1}{2} < x \leq 1 \end{cases}$$

$$U_{n+1}^{(2k)}(x) = \begin{cases} U_n^{(k)}(2x) & 0 \leq x < \frac{1}{2} \\ -U_n^{(k)}(2 - 2x) & \frac{1}{2} < x \leq 1 \end{cases}$$

$$k = 1, 2, 3, \dots, 2^{n-1}, n = 2, 3, \dots$$

其中,在间断点处,函数取两侧的极限平均值。如此定义的分段线性U系统前8个函数的图象如图1所示。

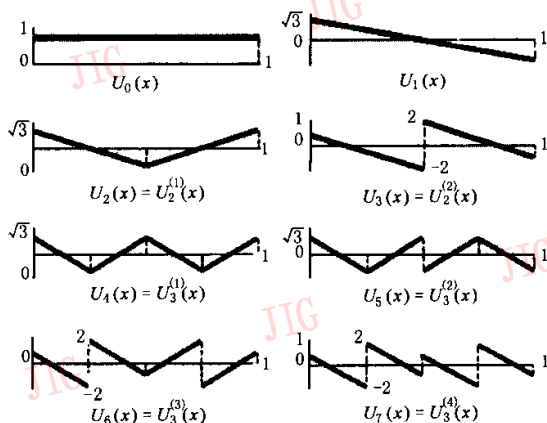


图1 分段线性U系统前8个函数图象

上述的分段线性U系统具有如下性质:

(1) 标准正交性

$$\langle U_m^{(i)}, U_n^{(j)} \rangle = \int_0^1 U_m^{(i)}(x) U_n^{(j)}(x) dx = \delta_{m,n} \delta_{i,j}$$

其中, $m, n = 0, 1, 2, \dots, i = 1, 2, 3, \dots, 2^{m-1}$

$$j = 1, 2, 3, \dots, 2^{n-1}, \delta_{k,l} = \begin{cases} 1 & k=l \\ 0 & k \neq l \end{cases} \quad (3)$$

(2) Fourier-U级数收敛性

若给定函数 F 的 Fourier-U 级数为

$$F = \sum_{i=0}^{\infty} a_i U_i \quad (4)$$

其中, U_i 是将式(2)中定义的函数依次排序,即 $U_i =$

$U_n^{(k)}, n = [\log_2 i] + 1, k = i - 2^{n-1} + 1$. 记

$$a_i = \langle F, U_i \rangle = \int_0^1 F(x) U_i(x) dx \quad (5)$$

及

$$p_{n+1} F = \sum_{i=0}^n a_i U_i \quad (6)$$

则

$$\lim_{n \rightarrow \infty} \|F - p_n F\|_2 = 0, F \in L_2[0, 1] \quad (7)$$

$$\lim_{n \rightarrow \infty} \|F - p_{2^n} F\|_\infty = 0, F \in C[0, 1] \quad (8)$$

式(2)表明 Fourier-U 级数的 L_2 收敛性及完备性; 式(7)表明 Fourier-U 级数的“分组”一致收敛性. 此外, 需要说明的是: 一定存在这样的连续函数, 且它的 Fourier-U 级数不一致收敛到自身.

(1) Fourier-U 级数的再生性

若函数 F 为分段线性函数, 且其间断点仅出现

在 $x = \frac{q}{2^r}$ 处, 其中 q 和 r 为整数, 那么 F 可以用有限项 Fourier-U 级数来精确表达.

(2) 变号数递增性

函数 F 在区间 $[0, 1]$ 上随 x 从 0 到 1 的连续变化而出现的符号变化的次数, 叫做 F 在 $[0, 1]$ 上的变号数, 记为 $S^-(F)$. 由分段线性 U 系统的定义可知

$$S^-(U_0) = 0, S^-(U_1) = 1$$

$$S^-(U_2^{(1)}) = 2, S^-(U_2^{(2)}) = 3$$

一般有

$$S^-(U_n^{(k)}) = 2^{n-1} + k - 1 \quad (9)$$

$$n = 0, 1, \dots, k = 1, 2, \dots, 2^{N-1}$$

2 分段 k 次 U 系统

将分段线性 U 系统推广到任意 k 次分段多项式.

在区间 $[0, 1]$ 上有限个函数的集合 $\{f_i(x), i = 1, 2, \dots, m\}$, 若满足如下性质:

(1) $f_i(x)$ 是以 $x = \frac{1}{2}$ 为结点的分段 k 次多项式, 且此时有 $m = k + 1$;

(2) $\langle f_i(x), f_j(x) \rangle = \delta_{ij}, i, j \in \{1, 2, \dots, m\}$;

(3) $\langle f_i(x), x^j \rangle = 0, i \in \{1, 2, \dots, m\}, j \in \{1, 2, \dots, k\}$

则称 $\{f_i(x), i = 1, 2, \dots, m\}$ 为函数生成元.

这种分段 k 次 U 系统的构造步骤为

(1) 取区间 $[0, 1]$ 上的前 $k+1$ 个 Legendre 多项式, 作为 k 次 U 系统的前 $k+1$ 个函数, 记为

$$U_0(x), U_1(x), \dots, U_k(x)$$

(2) 构造 $k+1$ 函数生成元

$$\{f_i(x), i = 1, 2, \dots, k+1\}$$

它应该满足前面函数生成元的, (1)~(3) 条即

$\{f_i(x)\}$ 中的函数彼此正交, 且与 $U_0(x), U_1(x), \dots, U_k(x)$ 皆正交. 若将 $f_i(x)$ 依次排在 $\{U_j(x), j = 0, \dots, k\}$ 之后, 得到

$$U_0(x), U_1(x), \dots, U_k(x), f_1(x), f_2(x), \dots, f_{k+1}(x)$$

(3) 压缩复制生成后续序列: 从 $f_1(x)$ 开始, 每个函数都复制出另外两个新函数, 一个是压缩偶对称复制, 另一个是压缩奇对称复制, 即

$$f_{i,1} = \begin{cases} f_i(2x) & 0 \leq x < \frac{1}{2} \\ f_i(2-2x) & \frac{1}{2} < x \leq 1 \end{cases} \quad (10)$$

$$f_{i,2} = \begin{cases} f_i(2x) & 0 \leq x < \frac{1}{2} \\ -f_i(2-2x) & \frac{1}{2} < x \leq 1 \end{cases} \quad (11)$$

这个过程无限地进行下去, 即可得到所需要的正交函数系

$$U_0(x), U_1(x), U_k(x), f_1(x), f_2(x), \dots,$$

$$f_{k+1}(x), f_{11}(x), f_{12}(x), f_{21}(x), f_{22}(x), \dots$$

这里仅给出分段 k 次 U 系统的形式定义, 具体的构造例子参见文献[5].

3 基于 U 系统的数字水印隐藏

下面以分段线性 U 系统为例, 提出一种基于 U 系统的数字水印隐藏方法, 它可以很容易地推广到分段 k 次 U 系统上.

首先, 将区间 $[0, 1]$ 划分为以下 8 个子区间:

$$\left[0, \frac{1}{8}\right], \left(\frac{1}{8}, \frac{1}{4}\right], \left(\frac{1}{4}, \frac{3}{8}\right], \left(\frac{3}{8}, \frac{1}{2}\right],$$

$$\left(\frac{1}{2}, \frac{5}{8}\right], \left(\frac{5}{8}, \frac{3}{4}\right], \left(\frac{3}{4}, \frac{7}{8}\right], \left(\frac{7}{8}, 1\right]$$

由此, 将分段线性 U 系统形式地表达为如下形式

$$\begin{aligned}
U_0(x) &= (1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1) \\
U_1(x) &= \sqrt{3} (1-2x_0 \quad 1-2x_1 \quad 1-2x_2 \quad 1-2x_3 \quad 1-2x_4 \quad 1-2x_5 \quad 1-2x_6 \quad 1-2x_7) \\
U_2(x) &= \sqrt{3} (1-4x_0 \quad 1-4x_1 \quad 1-4x_2 \quad 1-4x_3 \quad 4x_4-3 \quad 4x_5-3 \quad 4x_6-3 \quad 4x_7-3) \\
U_3(x) &= (1-6x_0 \quad 1-6x_1 \quad 1-6x_2 \quad 1-6x_3 \quad 5-6x_4 \quad 5-6x_5 \quad 5-6x_6 \quad 5-6x_7) \\
U_4(x) &= \sqrt{3} (1-8x_0 \quad 1-8x_1 \quad 8x_2-3 \quad 8x_3-3 \quad 5-8x_4 \quad 5-8x_5 \quad 8x_6-7 \quad 8x_7-7) \\
U_5(x) &= \sqrt{3} (1-8x_0 \quad 1-8x_1 \quad 8x_2-3 \quad 8x_3-3 \quad 8x_4-5 \quad 8x_5-5 \quad 7-8x_6 \quad 7-8x_7) \\
U_6(x) &= (1-12x_0 \quad 1-12x_1 \quad 5-12x_2 \quad 5-12x_3 \quad 12x_4-7 \quad 12x_5-7 \quad 12x_6-11 \quad 12x_7-7) \\
U_7(x) &= (1-12x_0 \quad 1-12x_1 \quad 5-12x_2 \quad 5-12x_3 \quad 7-12x_4 \quad 7-12x_5 \quad 11-12x_6 \quad 11-12x_7)
\end{aligned} \quad (12)$$

其中

$$\begin{aligned}
x_0 &\in \left[0, \frac{1}{8}\right], x_1 \in \left(\frac{1}{8}, \frac{1}{4}\right], \\
x_2 &\in \left(\frac{1}{4}, \frac{3}{8}\right], x_3 \in \left(\frac{3}{8}, \frac{1}{2}\right], \\
x_4 &\in \left(\frac{1}{2}, \frac{5}{8}\right], x_5 \in \left(\frac{5}{8}, \frac{3}{4}\right], \\
x_6 &\in \left(\frac{3}{4}, \frac{7}{8}\right], x_7 \in \left(\frac{7}{8}, 1\right]
\end{aligned}$$

然后,将之离散化、正交单位化,得到 8×8 的变换矩阵 T .

对于原始图象, $I(i, j) \in \{0, 1, \dots, 255\}$, $i=0, 1, \dots, M-1$, $j=0, 1, \dots, N-1$, 以及原始水印图象 $I_w(i, j) \in \{0, 1\}$, $i=0, 1, \dots, M_w-1$, $j=0, 1, \dots, N_w-1$, 如果满足 $M \geq 2M_w$, $N \geq 2N_w$, 那么也可将图象 $I(i, j)$ 分割为 8×8 的小块 I_{ij} , $i=0, 1, \dots, \frac{M}{8}-1$, $j=0, 1, \dots, \frac{N}{8}-1$, 然后,对每个小块,做如下变换

$$F'_{ij} = T F_{ij} T' \quad (13)$$

式中, F'_{ij} 为与 F_{ij} 对应的 U 系统变换系数矩阵,其低频部分集中在左上角位置,而右下角为高频部分. 接着在此 8×8 系数块中抽取 $\frac{256 \times M_w \times N_w}{M \times N}$ 个中频系数,构成一个 4 倍于水印图象的系数矩阵,其元素记为 $C(i, j)$, $i=0, 1, 2, \dots, 2M_w-1$, $j=0, 1, 2, \dots, 2N_w-1$. 并记所有 U 系统变换系数为 $F'(i, j)$.

对水印图象 $I_w(i, j)$ 做置乱变换^[6]得到置乱的水印图象 $I'_w(i, j)$, 这样做的目的是避免在植入水印后的图象中产生人眼可以分辨的放大的水印暗纹. 然后再根据 $I'_w(i, j)$ 对 $C(i, j)$ 做如下调整.

(1) 若 $F'_w(i, j)=0$, 则

$$\begin{aligned}
\tilde{C}(i, j) &= \tilde{C}(i + M_w, j + N_w) \\
&= (C(i, j) + C(i + M_w, j + N_w))/2 \\
\tilde{C}(i + M_w, j) &= \tilde{C}(i, j + N_w) \\
&= (C(i + M_w, j) + C(i, j + N_w))/2
\end{aligned}$$

(2) 若 $F'_w(i, j)=1$, 则

当 $C(i, j)=C(i + M_w, j + N_w)$ 时

$$\begin{aligned}
\tilde{C}(i, j) &= (C(i, j) + C(i + M_w, j + N_w))/2 + \Delta \\
\tilde{C}(i + M_w, j + N_w) &= (C(i, j) + C(i + M_w, j + N_w))/2 - \Delta \\
\text{当 } C(i + M_w, j) &= C(i, j + N_w) \text{ 时} \\
\tilde{C}(i + M_w, j) &= (C(i + M_w, j) + C(i, j + N_w))/2 - \Delta' \\
\tilde{C}(i, j + N_w) &= (C(i + M_w, j) + C(i, j + N_w))/2 + \Delta' \\
i &= 0, 1, \dots, M_w-1, j = 0, 1, \dots, N_w-1
\end{aligned}$$

其中 Δ, Δ' 是充分小的量,并满足

$$\begin{aligned}
\tilde{C}(i, j) &\neq \tilde{C}(i + M_w, j + N_w) \\
\tilde{C}(i + M_w, j) &\neq \tilde{C}(i, j + N_w)
\end{aligned}$$

将调整后的系数矩阵 $\tilde{C}(i, j)$ 放回原位置,得到新的 U 系统变换系数矩阵 $F''(i, j)_{M \times N}$, 对每个 8×8 系数块做如下变换

$$F'''_{ij} = T' F''_{ij} T$$

得到植入了两份数字水印的图象 $I'''(i, j)$. 根据上面的数字水印植入方法,不难得出提取数字水印的算法. 但是需要注意的是,在提取水印时,由于计算机表示位数有限,可能引起误差,所以在判断相邻系数的关系时,要给出一个阈值 ϵ , 如果满足

$$|F'(x, y) - F'(x + 1, y)| \leq \epsilon$$

就认为这两个系数是相同的. 最后,根据植入水印时使用的置乱变换做相应的逆变换,得到恢复后的水印图象 I''_w .

下面是一个基于分段线性 U 系统的数字水印隐藏的例子(见图 2).

这里,用峰值信噪比(Peak Signal-to-Noise Ratio)来衡量原始图象与植入水印图象之间的数值差别,用噪音比(Noise Ratio)来衡量原始水印图象与恢复水印图象之间的噪音比率

$$NR = \frac{\sum_{i=0}^{M_w-1} \sum_{j=0}^{N_w-1} P_{ij}}{M_w \times N_w} \times 100\%$$

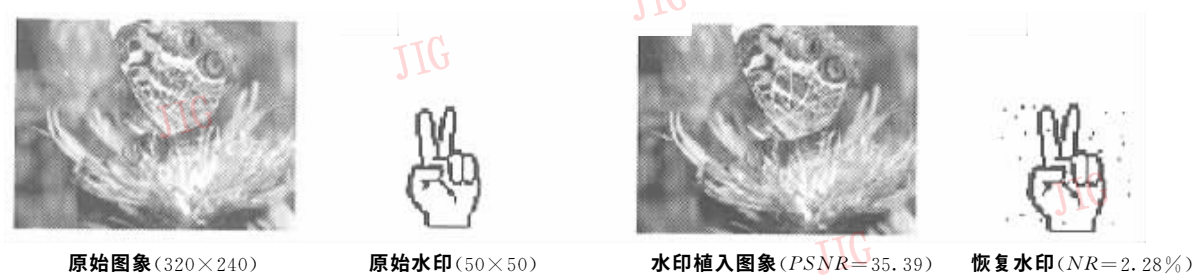


图 2 基于分段线性 U 系统的数字水印隐藏

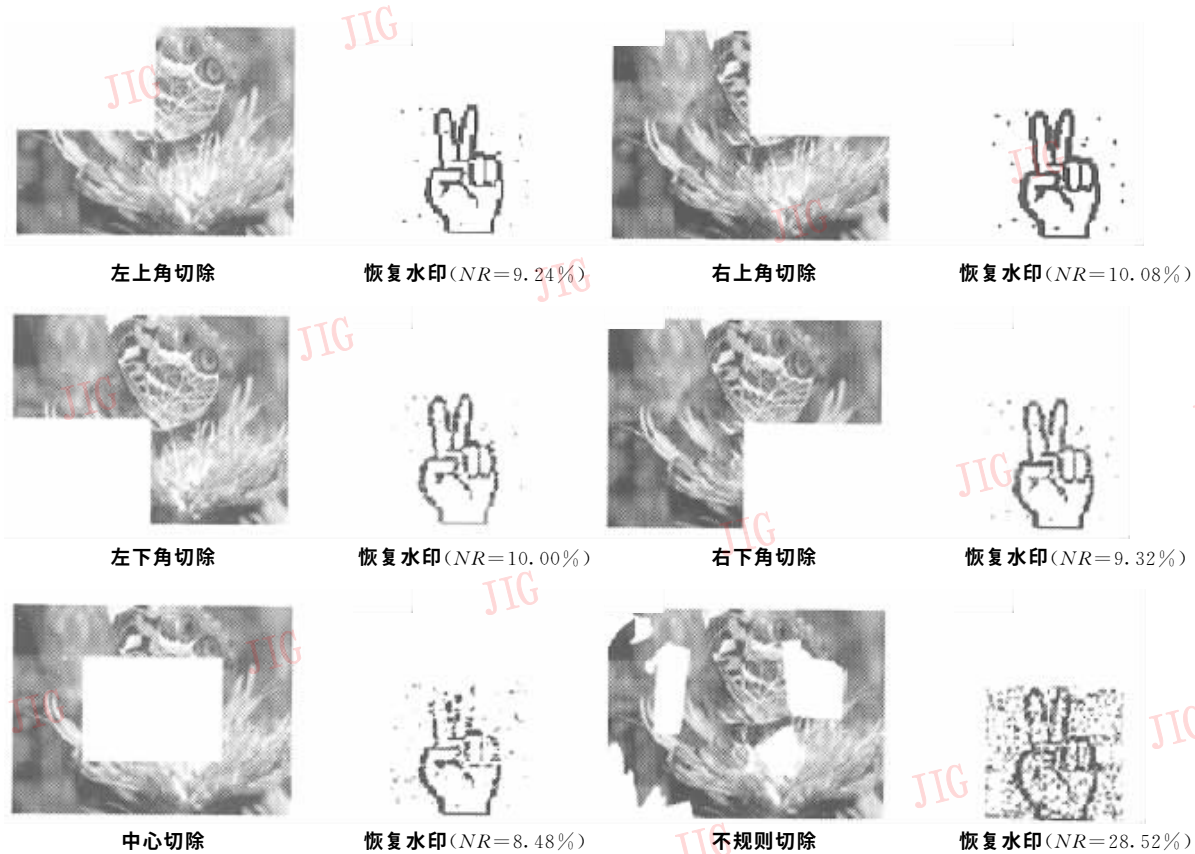


图 3 部分切除水印植入图象所恢复的水印

$$P_{ij} = \begin{cases} 0 & \text{如果 } F_w(i, j) = F''_w(i, j) \\ 1 & \text{如果 } F_w(i, j) \neq F''_w(i, j) \end{cases} \quad (19)$$

由图 2 可见,从视觉上无法区分植入水印前后两幅图象的区别,图 3 给出一些对植入水印图象进行切除后恢复水印的例子以说明本文水印技术的效果.

4 结 论

与以往所做的图象信息隐藏工作不同,数字水印对鲁棒性的要求很高. 为了保证植入水印后的图象在最大程度上抵挡攻击,必须想方设法减少水印信息可能的损失. 目前最好的方法是在不影响图象

质量的前提下,尽可能在图象中植入多个水印备份. 当然基于 U 系统的数字水印植入方法对图象的切除是有效的,但并不能保证针对其他的一些问题时一样有效. 事实上,这种方法仅仅是在频率空间上植入水印.

今后的研究工作中,我们将继续寻求在图象的位置空间、色彩空间以及频率空间上的水印植入方法.

参 考 文 献

1 Bender W, Gruhl D, Morimoto N *et al.* Techniques for data hiding, IBM System Journal, 1996,35(3&4):313~335.
2 Sapwater E, Wood K. Electronic copyright protection, Photo-Electronic Imaging, 1994,37(6):16~21.

3 齐东旭,冯玉瑜. 关于 Fourier-U 级数的收敛性. 中国科技大学学报,数学专辑,1983.

4 齐东旭,冯玉瑜. 关于一类正交分段多项式快速变换的注记. 中国科技大学学报(增刊 83003),1983.

5 齐东旭. 分形及其计算机生成. 北京:科学出版社,1994.

6 丁玮,齐东旭. 数字图象变换及信息隐藏与伪装技术. 计算机学报,1998,21(9):838~843.

7 Qi D X, Ding W, Li H S. A new image transformation scheme and digital approximation between different pictures. Advances in Computational Mathematics, Lecture Notes in Pure and Applied Mathematics, Marcel Dekker Inc. 1999:465~469.

8 Qi D X, Ding W, Li H S. Tangram algorithm; image transformation for storing and transmitting visual secrets. Proc. of 5th International Conference on Computer-Aided Design & Computer Graphics, International Academic Publishers. 1997, 1:135~139.

9 丁玮,齐东旭. 信息伪装中一种新的数字图象变换. 中国科协第三届青年学术年会论文集(信息科学与电子技术),北京:中国科学技术出版社,1998:309~311.

丁 玮 1971 年生,2000 年获中国科学院计算技术研究所计算机应用专业工学博士学位,现为联想集团发展战略研究部高级研究员. 研究兴趣为数字图象压缩和数字图象信息的隐藏等. 已发表论文近 30 篇.

闫伟齐 1968 年生,1996 年获西北大学数学系理学硕士学位,现为中国科学院计算技术研究所博士研究生. 研究方向为计算机图形学和数字图象的安全处理.

齐东旭 教授、博士生导师,现为北方工业大学 CAD 研究中心主任. 主要研究领域为数值分析、计算机辅助几何设计、计算机图形学、计算机动画、数字图象压缩和数字图象的安全处理等. 已发表论文 130 余篇,出版专著 5 部.