一种双帧数字图像的双盲水印技术

王道顺，戴一奇，梁敬弘
（清华大学计算机科学与技术系，北京 100084）

摘 要： 本文提出一种新的安全水印嵌入技术：同时对两帧数字图像嵌入两种不同水印，对任意提取一幅图像的水印，无法恢复两个水印的任何信息．在获得双密钥情况下，方可恢复两幅图像的水印．从数学上证明了我们提出的新技术的有效性，并对算法安全性给予了分析．在变换域上给出了实现了双盲水印的算法，采用 StirMark 水印测试软件进行了一系列攻击性试验，其测试结果表明此技术提供了一种新的数字版权保护的方法．

关键词： 双盲数字水印；编码；安全性；StriMark 攻击

中图分类号： TP309 **文献标识码：** A **文章编号：** 0372-2112 (2002) 12A-1982-04

A Novel Technology of Two Blind Watermarks for Two Images

WANG Dao-shun, DAI Yi-qi, LIANG Jing-hong
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: A novel and secure watermark embedding technology is given, which embeds two different watermarks into two digital images. Any information of the two watermarks from any one of the two images can not be obtained. Any information of two watermarks can not be recovered without any one of the two keys or one extracted information of two Stego-images. The validity of the technology is proved with mathematical theory, and the security of the algorithm is also discussed in the paper. The embedding algorithm of two blind watermarks is given based on transformation domain. Then a series of attacking tests are performed with StirMark software. The test results verify that the validity of the technology. Therefore, the technology provides a new method of copyright protection.

Key words: two blind digital watermark; encode; security; StirMark attack

1 引言

近年来，随着国际互联网的快捷发展，在网上传输数字化媒体已经变得愈来愈普遍．因媒体易于复制，从而可能会导致大规模非法拷贝，而这极可能损害媒体业的发展．为了防止合法所有者的信息被他人有意或无意地使用，信息保护是不可缺少的．如何保护媒体所有权问题，成为近年来研究的热点，一种普遍的方法是在原始信息中嵌入版权标志，从而可以正确地判定所有权的归属，这就是所谓的水印技术．一个有效的水印系统需满足一系列要求如透明性，鲁棒性等[5,6]．

关于水印的研究现状和进展，见文[1～6]．对图像水印嵌入技术研究，已提出了许多方案[5,6]，这些研究集中在空间域和变换域上寻求各种嵌入算法．因空间域在鲁棒性等方面的局限性，对变换域水印系统的研究是发展的主流．在变换域中，DCT 域的嵌入方法因其计算简单，且与国际数据压缩标准如 JPEG、MPEG、H.261/263 等兼容，便于在压缩域中实现，目前用得最多．而 DWT 域和 DFT 域等，对水印嵌入技术在原理上是相同，方法上是相似的[5,6]，为方便，本文算法验证在 DCT 域上实现，其他域可以类推．

在 DCT 域中有两种比较典型算法，Koch 和 Zhao 通过对 DCT 域的三个中频系数进行微小的修改以嵌入一个二进制序列水印[8]．这样做的原因是：低频分量在视觉上很重要，若对它修改容易被感知；而高频分量又容易被篡改．Cox 等提倡用一种整体的 DCT 扩频来隐藏水印[6,7]．它基于这样事实，如果一个窄带信号在一个带宽大得多的信号之中传输，在任何频率中的信号能量都是不可检测的．在宽带上传输窄带信号，可导致水印在所有频率上分布，使得它在任何单一频率上的能量很小，因此不可检测．Cox 等嵌入固定长度的水印，并且使它满足(0,1)高斯分布．这样，可均匀地把水印分配给 1000 个最大的 AC 系数，以相似度作为评价原始水印和被提取出的水印的客观度量．Cox 等提出的扩频水印技术已经被很多研究者使用[2,6,7]，成为一种典型的模式．

目前公开发表的文献中，主要讨论单帧图像的水印技术[1～6]，但在实际应用中，需要研究帧与帧之间的水印技术，如：Video 和 Audio 等方面，目的是通过对帧与帧之间嵌入水印关联的研究，可用于连续帧水印之间的掉帧（数据丢包）检验和完整性校验，从而给出一种新的解决方法．然而，对双帧实

收稿日期：2002-06-06；修回日期：2002-09-29
基金项目：国家 973 计划（No.G1998030420）

现双水印研究,已有研究对此还没有涉及.

水印技术具有隐蔽通信等特点,其安全性主要集中在抗检测,抗攻击等方面,但密钥在水印技术中占有重要的地位.能否借鉴密码学方面知识,研究帧与帧间水印安全性问题?本文第 2 节给出了回答.

本文重点介绍我们提出新技术理论基础,并以此给出在变换域(DCT)实现的相关技术.2 节给出双帧图像实现双盲水印的理论基础,包括编码和解码;并分析了实现水印算法的有效性.3 节在 DCT 域上给出了实现水印嵌入策略,嵌入算法,使用 StirMark 攻击软件,对我们的水印方案进行不同种类的攻击,并给出了相应的实验结果.

2　双幅图像双变换编码

2.1　预处理

为了讨论方便,我们首先对图像及所用的符号进行一些规范化处理.在本文中,总视给定的两幅被嵌入图像(以下简称编码图像)具有相同大小的象素数.因为若它们不相同,可采用以下方式把它们变为相同大小的图像:对较小的图像用扩展其背景色,使其与另一幅较大的图像具有相同尺寸;或同时对两幅图像进行扩展,使它们具有相同的尺寸.若有必要,再对图像进行归一化处理.以下我们给出三个基本假设:

假设 1　对原数字图像 $\boldsymbol{P},\boldsymbol{Q}$,将与其对应的象素矩阵等同.

假设 2　两幅数字图像 $\boldsymbol{P},\boldsymbol{Q}$,具有相同的大小,不妨设为 $m\times n$ 矩阵.

设 $\boldsymbol{A}$ 是一个矩阵:$\boldsymbol{A}=[a_{ij}]_{m\times n}$.如果在 A 中去掉 k 行和 l 列,则称留下的矩阵为 A 的一个 $(m-k)\times(n-l)$ 子矩阵.如果在 $\boldsymbol{A}$ 中去掉的是相邻的 k 行和相邻的 l 列,则称留下的子矩阵为 A 的一个 $(m-k)\times(n-l)$ 主子矩阵.

以下令 $\boldsymbol{P}=[p_{ij}]_{m\times n}$,$\boldsymbol{Q}=[q_{ij}]_{m\times n}$,其中 $p_{ij},q_{ij}\in\{1,2,\cdots,\}$ 表示图像的数字象素值,根据主子矩阵规定可知,$\boldsymbol{P}$ 和 $\boldsymbol{Q}$ 的 $(m-k)\times(n-l)$ 主子矩阵 $\boldsymbol{P}^*=[p_{ij}]_{(m-k)\times(n-l)}$,$\boldsymbol{Q}^*=[q_{ij}]_{(m-k)\times(n-l)}$ 的组合只有以下 16 种情况:

(1)在 $\boldsymbol{P}$ 中去掉后 k 行和左 l 列;在 $\boldsymbol{Q}$ 中去掉前 k 行和左 l 列;
(2)在 $\boldsymbol{P}$ 中去掉后 k 行和左 l 列;在 $\boldsymbol{Q}$ 中去掉前 k 行和右 l 列;
(3)在 $\boldsymbol{P}$ 中去掉后 k 行和左 l 列;在 $\boldsymbol{Q}$ 中去掉后 k 行和左 l 列;
(4)在 $\boldsymbol{P}$ 中去掉后 k 行和左 l 列;在 $\boldsymbol{Q}$ 中去掉后 k 行和右 l 列;
(5)在 $\boldsymbol{P}$ 中去掉后 k 行和右 l 列;在 $\boldsymbol{Q}$ 中去掉前 k 行和左 l 列;
(6)在 $\boldsymbol{P}$ 中去掉后 k 行和右 l 列;在 $\boldsymbol{Q}$ 中去掉前 k 行和右 l 列;
(7)在 $\boldsymbol{P}$ 中去掉后 k 行和右 l 列;在 $\boldsymbol{Q}$ 中去掉后 k 行和左 l 列;
(8)在 $\boldsymbol{P}$ 中去掉后 k 行和右 l 列;在 $\boldsymbol{Q}$ 中去掉后 k 行和右 l 列;
(9)在 $\boldsymbol{P}$ 中去掉前 k 行和左 l 列;在 $\boldsymbol{Q}$ 中去掉前 k 行和左 l 列;
(10)在 $\boldsymbol{P}$ 中去掉前 k 行和左 l 列;在 $\boldsymbol{Q}$ 中去掉前 k 行和右 l 列;
(11)在 $\boldsymbol{P}$ 中去掉前 k 行和左 l 列;在 $\boldsymbol{Q}$ 中去掉后 k 行和左 l 列;
(12)在 $\boldsymbol{P}$ 中去掉前 k 行和左 l 列;在 $\boldsymbol{Q}$ 中去掉后 k 行和右 l 列;
(13)在 $\boldsymbol{P}$ 中去掉前 k 行和右 l 列;在 $\boldsymbol{Q}$ 中去掉前 k 行和左 l 列;
(14)在 $\boldsymbol{P}$ 中去掉前 k 行和右 l 列;在 $\boldsymbol{Q}$ 中去掉前 k 行和右 l 列;
(15)在 $\boldsymbol{P}$ 中去掉前 k 行和右 l 列;在 $\boldsymbol{Q}$ 中去掉后 k 行和左 l 列;
(16)在 $\boldsymbol{P}$ 中去掉前 k 行和右 l 列;在 $\boldsymbol{Q}$ 中去掉后 k 行和右 l 列.

为方便起见,在本文中我们只讨论矩阵 $\boldsymbol{P},\boldsymbol{Q}$ 的主子矩阵的情形.其它情形可以看成是主矩阵的变形.在实际应用中,采用其变形方式并不增加太多工作量,但可大大增强编码的复杂度,增大破译的难度,有利于信息的安全.由于基本原理基于主子矩阵方式,因此不失一般性,后面的讨论以两个矩阵组合的第 1 种情况讨论.

定义 1　对两幅数字图像 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 进行一定数学变换,我们称所得到的两个变换后的图像 $\boldsymbol{C}$ 和 $\boldsymbol{D}$ 为原始图像 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 的双变换,如果它们具有以下性质:

(1)单独从从图像 $\boldsymbol{C}$ 和 $\boldsymbol{D}$ 中得不到图像 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 的信息;

(2)对图像 $\boldsymbol{C}$ 和 $\boldsymbol{D}$ 进行一定运算,可正确恢复图像 $\boldsymbol{A}$;

(3)图像 $\boldsymbol{C}$ 和 $\boldsymbol{D}$ 按一定方式错位后再执行一个运算,可正确恢复图像 $\boldsymbol{B}$.

定义 2　如果矩阵 $\boldsymbol{T}_s,\boldsymbol{R}_s$ 满足以下性质,则称 $\boldsymbol{T}_s,\boldsymbol{R}_s$ 为编码变换矩阵:

(1)矩阵 $\boldsymbol{P},\boldsymbol{Q}$ 经过一定运算后得到的矩阵 $\boldsymbol{T}_s,\boldsymbol{R}_s$ 与原矩阵,相比增加了 k 行和 l 列;

(2)从矩阵 $\boldsymbol{T}_s,\boldsymbol{R}_s$ 中任意一个矩阵无从得知原矩阵 $\boldsymbol{P},\boldsymbol{Q}$ 的信息;

(3)只要从矩阵 $\boldsymbol{T}_s,\boldsymbol{R}_s$ 中选定相应的子矩阵经过一定的运算(异或),就能还原成 $\boldsymbol{P},\boldsymbol{Q}$.

由定义 1 和定义 2 可知:$\boldsymbol{T}_s$ 和 $\boldsymbol{R}_s$ 所对应的图像是 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$ 所对应图像的双变换.同时定义 2 也表明:矩阵 $\boldsymbol{T}_s,\boldsymbol{R}_s$ 是由 $\boldsymbol{P},\boldsymbol{Q}$ 经过一个特定的运算得到的,它们增加的行列数根据 $k,l(k\geqslant 1,l\geqslant 1)$ 的值而定,并且经过变换的矩阵满足安全性,其解码运算是一定方式下进行变换.由此可以得出:我们之所以称定义 2 的矩阵 $\boldsymbol{T}_s,\boldsymbol{R}_s$ 为编码变换矩阵,是因为它们具有编码和解码的性质,即经过相关运算可还原出原矩阵.

2.2　编码变换矩阵的构造模式

随机矩阵 $\boldsymbol{F}_s,\boldsymbol{G}_s$ 的构造

设 $f_0(i,j)(i=1,2,\cdots,m+k;j=1,2,\cdots,n+l)$ 是一个随机函数,$F_A(i,j)$ 和 $F_B(i,j)(i=1,2,\cdots,m;j=1,2,\cdots,n)$ 均为常函数.我们下面给出两个均只由 $f_0(i,j)$,$F_A(i,j)$ 和 $F_B(i,j)$ 生成的集合 Φ 和 Γ,其中每个元素是由随机函数 $f_0(i,j)$ 与常函数 $F_A(i,j)$,$F_B(i,j)$ 的变换构成的.具体地说,Φ 和 Γ 的定义如下:

$$\begin{aligned}\Phi=\{&F_s(i,j):F_0(i,j)=f_0(i,j),F_1(i,j)\\&=f_0(i,j)\wedge F_B(i-k,j-l)\},F_{s+2}(i,j)\\&=F_s(i,j)\wedge F_A(i,j)\wedge F_B(i-k,j-l),s=0,1,2,\cdots\},\\ \Gamma=\{&G_s(i,j):G_0(i,j)=f_0(i,j),G_1(i,j)\\&=f_0(i,j),G_1(i,j)=f_0(i,j)\wedge F_A(i,j),G_{s+2}(i,j)\\&=G_s(i,j)\wedge F_B(i-k,j-l)\wedge F_A(i,j),s=0,1,2,\cdots\},\end{aligned}$$

下面我们来讨论集合 Φ 和 Γ 中元素 $F_s(i,j)$ 和 $G_s(i,j)$ 的性质.

性质 1　二元函数 $F_s(i,j)$(或 $G_s(i,j)$)是一个随机函数,$\boldsymbol{F}_s$(或 $\boldsymbol{G}_s$)是一个随机矩阵,其中 $\boldsymbol{F}_s=[F_s(i,j)]$,$\boldsymbol{G}_s(i,j)(i=1,\cdots,m;j=1,\cdots,n),s=0,1,2,\cdots$.

性质 1 的证明是很显然的.根据集合 Φ 和 Γ 的构造,用归纳法可以证明:

性质 2 $F_s(i,j) \wedge G_{s-1}(i,j) = F_A(i,j)$,

$$i = 1,\cdots,m; j = 1,\cdots,n$$

$$G_s(i+k,j+l) \wedge F_{s-1}(i,j) = F_B(i,j),$$

$$i = k,k+1,\cdots,m+k; k = l,l+1,\cdots n+l; s = 0,1,2,\cdots.$$

上面的性质表明集合 Φ 和 Γ 中的元素均满足定义 2 的条件.

2.3 编码变换矩阵的构成

假设矩阵

$$\boldsymbol{P} = [\boldsymbol{P}_1,\boldsymbol{P}_2,\cdots,\boldsymbol{P}_n], \boldsymbol{Q} = [\boldsymbol{Q}_1,\boldsymbol{Q}_2,\cdots,\boldsymbol{Q}_n]$$

其中

$$\boldsymbol{P}_k = (p_{1k},p_{2k},\cdots,p_{m-1k},p_{mk})^{\mathrm{T}},$$

$$\boldsymbol{Q}_k = (q_{1k},q_{2k},\cdots,q_{m-1k},q_{mk})^{\mathrm{T}}, \quad k = 1,2,\cdots,n.$$

下面给出上述编码变换矩阵的生成. 由随机函数 $F_s(i,j)$ 和 $G_A(i,j)$ 的构造,作一映射 g,使它满足以下要求:

$$F_s(i,j) = g(P(i,j)), F_B(i,j) = g(Q(i,j))$$

$$\boldsymbol{T}_s := [T_s(i,j)] = [g(F_s(i,j))] = [t_{ij}]$$

$$\boldsymbol{R}_s := [R_s(i,j)] = [g(G_s(i,j))] = [r_{ij}],$$

$$i = 1,\cdots,m+k; j = 1,\cdots,n+l$$

这样便生成了编码变换矩阵 $\boldsymbol{T}_s,\boldsymbol{R}_s$. 为了使编码变换矩阵 $\boldsymbol{T}_s$, $\boldsymbol{R}_s$ 更加安全,可以给出一定变换序列,按其进行变换. 我们不难证明 $\boldsymbol{T}_s,\boldsymbol{R}_s$ 满足定义 2 的性质 1,在构造模式中,$\boldsymbol{T}_s,\boldsymbol{R}_s$ 增加的行列数为 k 和 l. 矩阵 $\boldsymbol{T}_s,\boldsymbol{R}_s$ 生成过程,由随机函数决定且与原矩阵 $\boldsymbol{P},\boldsymbol{Q}$ 从得到的结果没有直接联系. 单独从矩阵 $\boldsymbol{T}_s,\boldsymbol{R}_s$ 得不到矩阵 $\boldsymbol{P},\boldsymbol{Q}$ 的任何信息. 它满足定义 2 中的性质 2.

由上面性质直接得出:

定理 由编码变换矩阵 $\boldsymbol{T}_s,\boldsymbol{R}_s$ 可唯一地还原矩阵 $\boldsymbol{T}_s$, $\boldsymbol{Q}_s$.

定理实质上给出了一个解码过程. 见性质 2. 由上构造算法可以知 k,l 是恢复编码信息的的密钥.

为了满足安全性水印嵌入,我们必须对上述得到的编码变换矩阵 $\boldsymbol{T}_s,\boldsymbol{R}_s$ 进一步处理.

设由两个指定种子 $s1$ 和 $s2$ 生成两个伪随机矩阵 $\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$

$$\boldsymbol{T}_s = \boldsymbol{T}_s \wedge \boldsymbol{T}_1; \boldsymbol{T}_s = \boldsymbol{T}_s \wedge \boldsymbol{T}_2 \tag{1}$$

2.4 算法安全性讨论

从上可知,从式(1)若还原矩阵 $\boldsymbol{P},\boldsymbol{Q}$. 必须具备以下两个条件:(1)两个种子 s_1 和 s_2 和编码矩阵解密密钥 k,l;(2)同时得到两个编码矩阵.

因此,算法的安全性取决于密钥的安全性. 若编码算法公开,其安全性依赖于两个伪随机数种子和恢复解密的两个密钥 k,l,而伪随机数两个种子的选取可以利用大素数分解定理.

在水印技术中,抗检测性比密钥和算法复杂度更为重要. 对需要嵌入水印的覆盖图像(cover-image)进行统计分析,找出服从的分布函数,由此选择两个种子 s_1 和 s_2,使其生成的伪随机矩阵 $\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$ 尽可能与覆盖图像 $\boldsymbol{P},\boldsymbol{Q}$ 矩阵具有相似的统计分布特性,其目的是抗水印检测. 实际应用中,通常对二值水印设计,使其满足正态高斯分布[6].

3 基于 DCT 变换的双盲水印

3.1 水印嵌入策略

DCT 域水印嵌入研究,已有成熟的技术和方法,我们借鉴已有研究结果,见文献[1~6]. 下面我们给出水印的嵌入和提取的算法流程图.

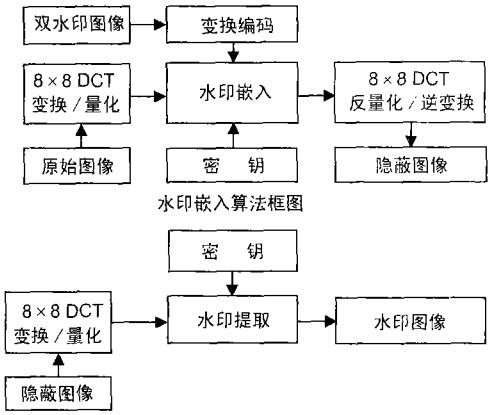

图 1 水印提取算法框图

3.2 水印嵌入与提取算法

$D_k = [d_{kij}]_{Mn\times Mn}, i,j = 1,\cdots,Mn; k = 1,2$ 是提取变换的两个系数矩阵,对 d'_{kij} 按其值大小作一个相应的排序,得到 $D'_k = [d'_{kij}]_{Mn\times Mn}, i,j = 1,\cdots,Mn; k = 1,2$. 设对水印图像 $H_{wk}(x,y)$,根据 $H_k(x,y)$ 对做如下调整.

若 $H_w(i,j) = 0$,则:

$$d'_k(x+1,y) = (d'_k(x+1,y) + d'_k(x,y))/2 - \Delta_1;$$

$$d'_k(x,y) = (d'_k(x+1,y) + d'_k(x,y))/2 - \Delta_2$$

或

$$d'_k(x,y+1) = (d'_k(x,y+1) + d'_k(x,y))/2 - \Delta_1;$$

$$d'_k(x,y) = (d'_k(x,y+1) + d'_k(x,y))/2 - \Delta_2;$$

若 $H_{wk}(i,j) = 1$,则:

$$d'_k(x+1,y) = d'_k(x+1,y) + \Delta_1;$$

$$d'_k(x,y) = d'_k(x,y) - \Delta_2$$

或

$$d'_k(x,y+1) = d'_k(x,y+1) + \Delta_1$$

$$d'_k(x,y) = d'_k(x,y) - \Delta_2$$

其中 Δ_1,Δ_2 是充分小的量满足 $d'_k(x+1,y) \neq d'_k(x,y)$(或 $d'(x,y+1) \neq d'(x,y)$)且保持原有相应的排序. 将调整后的系数矩阵 $d'_k(x,y)$ 放回原位置,得到新的两个 DCT 变换系数矩阵,经过逆变换得到嵌入了数字水印的图像.

根据上面的数字水印嵌入算法,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,因计算机表示位数有限,可能引起误差,在判断相邻系数的关系时,要给出二个阈值 ε_1 和 ε_2,若满足 $|d'_k(x,y) - d'_k(x+1,y)| \leqslant \varepsilon_1$ 或 $|d'_k(x,y) - d'_k(x,y+1)| \leqslant \varepsilon_1$,认为此两个系数是相同的. 若满足 $|d'_k(x,y) - d'_k(x+1,y)| \geqslant \varepsilon_2$ 或 $|d'_k(x,y) - d'_k(x,y+1)| \geqslant \varepsilon_2$,以此判断这两个系数是不相同的. 最后,根据嵌入水印时使用的变换做相应的逆变换,得到恢复后的水印图像.

下面给出在 DCT 域上实现双盲水印的实例

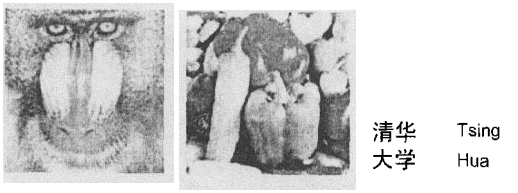

图 2　掩饰图与水印

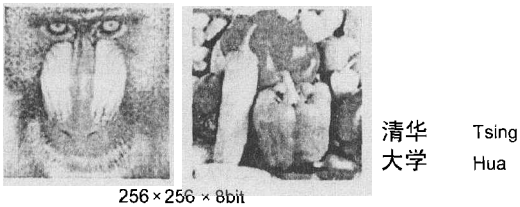

图 3　隐秘图与提取的水印

对隐蔽图分别单帧提出水印(算法公开的话)，见下图

若要恢复双水印图像，必须借助密钥完成.

图 4　随机图

3.3　算法攻击检验

StirMark 是剑桥大学计算机实验室编写的一个用于测试图像水印技术鲁棒性的免费软件[9]，它是比较理想的测试平台.我们使用 StirMark3.1 对嵌入后生成的水印进行测试，测试结果如图所示：

图 5　Stirmark 测试结果 1

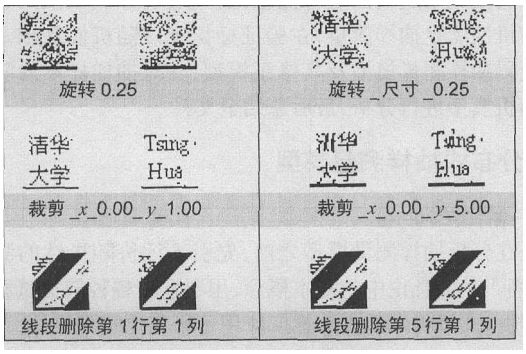

图 6　Stirmark 测试结果 2

从攻击实验结果可以看出，本文提出的数字水印算法对常见的信号处理操作具有较强的鲁棒性.但其对修剪(Cropping)和旋转攻击抵抗较差.以上实验结果表明了我们提出的实现双幅图像的双盲水印算法具有较好的透明性、鲁棒性，安全性等特点.

4　结束语

本文理论上给出了实现双盲水印的算法，并讨论了其安全性问题.在 DCT 域实现了双盲水印，从 StirMark 对水印测试的结果显示，此新技术在解决数字版权保护，提供了一种新的水印嵌入方法，在多帧媒体实现水印方面具有安全有效等特点，可用于 Video 和 Audio 水印技术.

参考文献：

[1] Ross Anderson. Information Hiding: First International Workshop, Lecture Notes In Computer Science(in brief, LNCS)[C]. Berlin: Spinger-Verlag, 1996.1174.

[2] David Aucsmith. Information Hiding: 2nd International Workshop, LNCS [C]. Berlin: Spinger-Verlag, 1998.1525.

[3] Andreas Pfitzmann. Information Hiding: Third International Workshop on Information Hiding [C]. Hotel Elbflorenz, Dresden, Germany, LNCS: Spinger-Verlag, 1999.1768.

[4] Ira S Moskowitz. Information Hiding: 4th International Workshop on Information Hiding [C]. Hotel Elbflorenz, Dresden, Germany, LNCS: Spinger-Verlag, 2001.2137.

[5] S Katzenbeisser, F A P Petitcolas. 信息隐藏技术-密写术与数字水印[M]. 吴秋新，钮心忻，杨义先，等，译. 北京：人民邮电出版社，2001，9.

[6] Imgemar J Cox, Matthew L Miller, Jeffrey A Bloom. Digital Watermarking [M]. Mogran Kaufemann Publishers, 2002.

[7] I J Cox, J Kilian, F T Leighton, T Shamoon. Secure spread spectrum watermarking for multimedia [J]. IEEE Trans Image Processing, 1997, 6:1673 – 1687.

[8] E Koch, J Zhao. Towards robust and hidden image copyright labeling [A]. Proc 1995 IEEE Workshop on Nonlinear Signal and Image Processing [C]. Neos Marmaras, Greece: IEEE, Jun 1995.452 – 455.

[9] Stirmarking [CP/OL]. http://www.cl.cam.ac.uk/~fapp2/watermarking/benchmark/.

作者简介：

王道顺　男，1964 年出生于四川苍溪，博士，副教授，研究方向为：图像加密、数字水印和密码算法.

戴一奇　男，1946 年出生于浙江省，教授，博导，研究方向为信息安全.