基于 Walsh 变换的数字水印算法 *

袁占亭[1], 王立鹏[1], 金渊智[2]
(1. 兰州理工大学 电气工程与信息工程学院, 兰州 730050; 2. 重庆大学 信息安全与计算智能研究所, 重庆 400030)

摘 要: 经对目前数字水印变换域算法的研究,发现常用的变换大多都是正交变换(如 DCT 和 DWT 等)。通过对 Walsh 正交函数系的研究,获得了与之对应的性能优良的正交变换,提出一种新颖的、鲁棒的 Walsh 域盲水印算法。实验表明,该算法计算简单,且具有良好的不可见性,并且在抵抗噪声和 JPEG 压缩攻击等方面具有较强的鲁棒性。

关键词: 数字水印; Walsh 变换
中图分类号: TP309.7 **文献标志码**: A **文章编号**: 1001-3695(2010)07-2654-03
doi:10.3969/j.issn.1001-3695.2010.07.072

Watermarking algorithm based on Walsh transform

YUAN Zhan-ting[1], WANG Li-peng[1], JIN Yuan-zhi[2]
(1. *College of Electrical & Information Engineering, Lanzhou University of Technology, Lanzhou* 730050, *China*; 2. *Institute of Computational Intelligence & Information Security, Chongqing University, Chongqing* 400030, *China*)

Abstract: Of all popular algorithms of transform domain, found most transformations to be orthogonal transformations (such as DCT and DWT). Selected Walsh transformation with excellent performance by studying Walsh function system. Finally, proposed a digital watermarking algorithm based on Walsh transformation. Experimental results show that the simple algorithm is good at perceptual transparency as well as robustness against noise and JPEG compression.

Key words: digital watermarking; Walsh transformation

0 引言

长期以来,正余弦函数系作为完备正交函数系在数字信号处理领域中占据统治地位。随着集成电路技术和数字计算机的快速发展,数字化通信系统为以 Walsh 函数为代表的非正弦正交函数的研究开拓了新的道路。本文通过对 Walsh 正交函数系的研究,从连续的 Walsh 函数中经过采样得出了离散的 Walsh 矩阵,接着通过一系列的理论证明得出了 Walsh 矩阵可用做数字水印技术中的变换矩阵。由于 DCT 域水印方案,本身计算量较小,且与国际数据压缩标准(如 JPEG、MPEG)兼容,最后结合 HVS 模型和 DCT 域的经典算法,提出了一种基于 Walsh 变换的盲水印算法。该算法在水印检测时无须某些假设或处理,同时通过对水印信息进行置乱加密及随机产生嵌入位置来保证水印的安全性,使嵌入的水印从根本上不可逆。最后的实验部分将该算法与 DCT 域的算法在同等条件下作了对比。实验结果表明,基于 Walsh 变换的水印算法与基于 DCT 变换的算法一样具有较强的使用价值。

1 Walsh 变换矩阵的生成过程

Walsh 函数系是美国数学家 Walsh[1] 于 1923 年提出的,他将不完备的雷德麦彻(Rademacher)函数加以完备化,形成了一组完备的、正交的矩型函数系,现在被称为沃尔什函数系。Walsh 函数系一般可以分为三类,即 Walsh 序的 Walsh 函数系、Paley 序的 Walsh 函数系和 Hadamard 序的 Walsh 函数系。这三类函数的区别在于它们各个函数出现的编号不同。这三种序的本质是一样的,它们之间可以通过变换矩阵相互转换[2]。如不特别声明,本文所讨论的函数系均为 Walsh 序的函数系。

定义 Walsh 函数的方法有多种,如利用 Haar 函数、递推公式、Hadamard 矩阵以及对称方程等。在此仅给出 Walsh 序的 Walsh 函数。所谓 Walsh 函数系是指下列函数系:

$$w(k,t)=\prod_{j=0}^{m-1}\operatorname{sgn}(\cos k_j 2^j \pi t);0\leqslant t<1,k=0,1,2,\cdots$$

其中:sgn 为符号函数,对于 sgn[x],当 $x>0$ 时,值为 +1,而当 $x<0$ 时,值为 -1, k、j 取值 0 或 1 是由序数 k 的二进制码来决定,即

$$k=\sum_{j=0}^{m-1}k_j 2^j$$

显然,Walsh 函数系的所有函数的周期都是 1,并且函数的取值在单位区间 [0, 1) 上均非零,因此称 Walsh 函数系为全局函数。由上述定义可以得出 Walsh 函数图形,此处给出了前八个 Walsh 函数的图形,如图 1 所示。

离散 Walsh 变换是指由 Walsh 矩阵所确定的正交变换。Walsh 矩阵可以从图 1 所示的函数系的每个图形采样得到。现以 8×8 阶 Walsh 矩阵为例来说明采样的具体过程,其他阶的 Walsh 矩阵依此类推。对每个方波进行 8 等分采样,得到 8

收稿日期: 2009-10-20; **修回日期**: 2009-11-27 **基金项目**: 国家"十一五"科技支撑计划项目(2006BAF01A21);甘肃省自然科学基金资助项目(3ZS062-B25-037)

作者简介:袁占亭(1961-),男,教授,博导,主要研究方向为自动化控制等;王立鹏(1979-),男,博士研究生,主要研究方向为生物算法(wlp_cn@hotmail.com);金渊智(1984-),男,河南洛阳人,硕士研究生,主要研究方向为信息安全.

个离散的值,将这些数值组合起来即是 8×8 阶 Walsh 矩阵:

$$W^*(3)=\begin{bmatrix} w(0,t)\\ w(1,t)\\ w(2,t)\\ w(3,t)\\ w(4,t)\\ w(5,t)\\ w(6,t)\\ w(7,t)\end{bmatrix}=\begin{bmatrix} 1&1&1&1&1&1&1&1\\ 1&1&1&1&-1&-1&-1&-1\\ 1&1&-1&-1&-1&-1&1&1\\ 1&1&-1&-1&1&1&-1&-1\\ 1&-1&-1&1&1&-1&-1&1\\ 1&-1&-1&1&-1&1&1&-1\\ 1&-1&1&-1&-1&1&-1&1\\ 1&-1&1&-1&1&-1&1&-1\end{bmatrix}$$

Walsh 矩阵的最大特点是取值简单,仅取 +1 和 −1 两个值,在计算机中可以方便地用高/低电平来模拟。从而可以方便地用于信号的数字化处理,并适合并行计算。

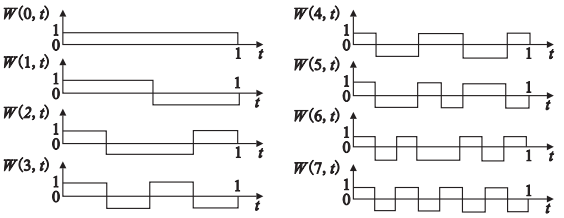

图1　前八个Walsh函数的图形

2　可用于数字水印技术的 *Walsh* 变换

2.1　离散 *Walsh* 变换

根据 Walsh 函数的正交性,可得

$$W^*(x)[W^*(x)]^{\mathrm{T}}=2^xE_2^x$$

对于 2^x 维数据矢量 $\{f(x)\}$,矢量:

$$\{F(x)\}=1/2^xW^*(x)\{f(x)\}$$

叫做数据矢量 $\{f(x)\}$ 的离散 Walsh 变换。其中,$W^*(x)$ 和 $\{f(x)\}$ 的阶数相同,逆变换式为 $\{f(x)\}=[W^*(x)]^{\mathrm{T}}\{F(x)\}$。

可见,$W^*(x)$ 不是归一化的正交矩阵,需要在其前面乘上一个系数,即:$1/\sqrt{2^x}W^*(x)$ 才是归一化的正交矩阵。也就是说,若 $W=1/\sqrt{2^x}W^*(x)$,则 $WW^{\mathrm{T}}=E$。

离散 Walsh 变换[3] 和快速 Walsh 变换(FWT)[4~8] 仅涉及数值的加减运算,而不含乘除运算,它比离散余弦变换(DCT)、快速傅里叶变换(FFT)和小波变换(DWT)更为迅捷。因此 FWT 更适用于二维矩阵的处理和实时数据的处理。

2.2　图像矩阵正交变换的能量无损证明

这里利用矩阵理论的知识来证明:数字图像矩阵经过正交变换后的能量保持不变。从而说明了图像在经过某个正交变换后再进行逆变换可以还原为原始图像。当然这里所说的还原只是在理论上是一样的,实际上,这里的还原仅仅是得到了原始图像在能量损失最小的情况下的图像的近似表示。

定义 1　*F*-范数。

设 $A=(a_{ij})_{n\times n}\in V_{n\times n}$,令

$$\|A\|_F=\Big(\sum_{i,j=1}^{n}|a_{ij}|^2\Big)^{1/2}=\sqrt{tr(A^*A)}\tag{1}$$

其中:A^* 为 A 的共轭转置,若只考虑实正交矩阵的话 $A^*=A^{\mathrm{T}}$。则 $\|\cdot\|_F$ 是一种范数,称为 $V_{n\times n}$ 上的 Frobenius 范数,简称 *F*-范数[9]。

现在假设 A 为 $n\times n$ 阶图像矩阵,则 A 经过正交变换 $T^{\mathrm{T}}S$ 后的变换矩阵:

$$B=T^{\mathrm{T}}AS\tag{2}$$

其中:S 和 T 为归一化正交矩阵,式(2)也可以表示为

$$A=TBS^{\mathrm{T}}\tag{3}$$

将 S 和 T 分别写成向量的形式,即

$$S=[s_1,s_2,s_3,\cdots,s_n],T=[t_1,t_2,t_3,\cdots,t_n]$$

式(3)可以写成:

$$A=[t_1,t_2,t_3,\cdots,t_n]B\begin{bmatrix}s_1^{\mathrm{T}}\\ s_2^{\mathrm{T}}\\ \acute{u}\\ s_n^{\mathrm{T}}\end{bmatrix}\tag{4}$$

根据正交矩阵的性质,有

$$s_i^{\mathrm{T}}s_j=\delta_{ij}=\begin{cases}1 & \text{当 } i=j\\ 0 & \text{当 } i\neq j\end{cases};t_i^{\mathrm{T}}t_j=\delta_{ij}=\begin{cases}1 & \text{当 } i=j\\ 0 & \text{当 } i\neq j\end{cases}$$

矩阵 B 可以写成 n^2 个 $n\times n$ 阶矩阵之和,每一个矩阵只有一个非零元素,如下式所示:

$$B=\begin{bmatrix}b_{11}&0&\cdots&0\\0&0&\cdots&0\\\acute{u}&\acute{u}&&\acute{u}\\0&0&\cdots&0\end{bmatrix}+\begin{bmatrix}0&b_{12}&\cdots&0\\0&0&\cdots&0\\\acute{u}&\acute{u}&&\acute{u}\\0&0&\cdots&0\end{bmatrix}+\cdots+\begin{bmatrix}0&0&\cdots&0\\0&0&\cdots&0\\\acute{u}&\acute{u}&&\acute{u}\\0&0&\cdots&b_{nn}\end{bmatrix}$$

那么式(4)可以表示为一个和式:

$$A=\sum_{i,j=1}^{n}b_{ij}t_is_j^{\mathrm{T}}\tag{5}$$

式(5)就称为图像矩阵 A 向量外积的展开形式。由式(5)可得

$$A^{\mathrm{T}}A=\sum_{i,j=1}^{n}b_{ij}s_jt_i^{\mathrm{T}}\sum_{k,l=1}^{n}b_{kl}t_ks_l^{\mathrm{T}}=\sum_{i,j=1}^{n}\sum_{k,l=1}^{n}b_{ij}b_{kl}s_j(t_i^{\mathrm{T}}t_k)s_l^{\mathrm{T}}=\sum_{j=1}^{n}\sum_{k,l=1}^{n}b_{kj}b_{kl}s_js_l^{\mathrm{T}}\tag{6}$$

将式(1)两端平方,并将式(6)代入得

$$\|A\|^2=tr(A^{\mathrm{T}}A)=\sum_{j=1}^{n}\sum_{k,l=1}^{n}b_{kj}b_{kl}tr(s_js_l^{\mathrm{T}})=\sum_{j=1}^{n}\sum_{k,l=1}^{n}b_{kj}b_{kl}tr(s_l^{\mathrm{T}}s_j)=\sum_{k,l=1}^{n}b_{kl}^2=\|B\|^2\tag{7}$$

式(7)说明,图像矩阵 A 经过正交变换后的范数没有改变。换句话说,也就是在经过正交变换后图像的能量保持不变。因此,从理论上讲可以选择任意的正交变换将图像变换到相应的变换域,然后利用数字水印算法,将水印信息嵌入图像的变换域,最后再执行正交变换的反变换得到带有水印信息的原始图像。

根据 2.1 节的介绍可知,离散 Walsh 变换是正交变换,下一节将利用离散 Walsh 变换来做数字水印。

3　水印的嵌入和提取

3.1　水印预处理

水印图像置乱是一种常见的水印加密方法,它使得合法使用者可以自由控制算法的选择、参数的选择以及使用随机数技术,这就加大了攻击者非法破译的难度。由于 Arnold 算法易于实现,其置乱次数可以为隐藏系统提供密钥(key),从而增强了系统的安全性和保密性,同时该算法实现的置乱克服了随机置乱的不可恢复性。本文采用 Arnold 变换对水印信息进行置乱。对 $M\times M$ 的水印图像按照式(8)进行 Arnold 变换,

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\left[\begin{bmatrix}1&1\\1&2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}\right]\bmod M,(x,y)\in\{0,1,\cdots,M-1\}\tag{8}$$

再将得到的矩阵按列优先转换为一维二进制序列 m,即下

面要嵌入的信息序列 m。

3.2 嵌入块的选择

设原始载体图像 I 为 $N\times N$ 阶的灰度图像,水印图像 W 为 $M\times M$ 阶的二值图像。先将 I 分成 8×8 的子块 I_{st},$s,t\in\{1,2,\cdots,N/8-1\}$,然后按照列优先的顺序从左到右将所有的子块转变成一维的数据集合 I_l,$l\in\{1,2,\cdots,(N/8)^2\}$,则有

$$I=\bigcup_{l=1}^{\max(l)} I_l\ (I_{l_1}\cap I_{l_2}=\Phi)$$

其中:$\max(l)=(N/8)^2$,即每个子块之间互不重叠,若 N 不是 8 的倍数则右边和下边多余出来的部分不嵌入水印信息。

现将欲嵌入的信息序列 m:

$$\{m\mid m=m_1,m_2,\cdots,m_k\ m_i\in\{0,1\},k\leqslant(N/M)^2\}$$

其中:$k=M\times M$,按照如下方法选取嵌入位置,嵌入到子块 I_l 中,每个子块嵌入 1 bit。引入 Logistic 映射函数,即式(9)

$$X_{i+1}=\mu\times X_i\cdot(1-X_i)\quad \mu\in[0,4]\ X\in[0,1] \tag{9}$$

固定 $\mu=4$,存在一个整数集合 P,选取 X 的初始值 X_0 作为一个私密密钥,进行迭代,将每次迭代的结果变换到区间$[1,(N/8)^2]$上并取整得到一个整数 a,若 $a\notin P$ 则将 a 放入集合 P 中。当 P 中整数个数为 k 时,停止迭代。最后将 P 中的整数按从小到大排序,得到一个有序的序列集合,仅在子块 I_u,$u\in P$ 中嵌入水印信息。这样做也起到了加密的目的。即使攻击者知道了该水印的嵌入和提取方法,而不知道具体是哪些块嵌入了水印,也无法正确地提取出水印信息。

3.3 嵌入方法

为了兼顾不可见性和鲁棒性,将水印嵌入到中高频区比较合适。直接修改选中子块 I_u,$u\in P$ 中的中高频系数即可表达水印 0、1 信息。本文使用(3,3)与(4,2)这一对系数,通过调整它们的大小关系来表示水印信息,具体做法如下:

当 $m_i=0$ 时,调整 $I_u(4,2)$ 和 $I_u(3,3)$ 的大小关系,使之满足:$I_u(4,2)>I_u(3,3)$,为了具有更好的鲁棒性,还需 $|I_u(4,2)-I_u(3,3)|>d$。其中:d 是水印嵌入强度;为了同时兼顾不可见性和鲁棒性,实验表明将 d 的值设置在[20, 40]上比较合适。

当 $m_i=1$ 时,同样调整 $I_u(4,2)$ 和 $I_u(3,3)$ 的大小关系,使之满足:$I_u(4,2)<I_u(3,3)$;为了具有更好的鲁棒性,还需 $|I_u(4,2)-I_u(3,3)|>d$。其中,d 是水印嵌入强度。

按照上述方法对 Walsh 系数矩阵修改过后,再用逆变换将 Walsh 系数矩阵还原为携带水印信息的图像。

3.4 提取方法

水印的提取过程是嵌入的逆过程,即对含有水印的图像进行 Walsh 变换,根据密钥 X_0 按照式(9)进行迭代,选出水印嵌入位置 $I_u(u=1,2,\cdots,k)$

$$\text{if } I_u(4,2)>I_u(3,3)\Rightarrow m_i'=0$$

$$\text{else } m_i'=1$$

恢复出序列 m' 并重构二值图像,最后用 Arnold 置乱算法对其进行恢复,得到水印图像。

4 实验及结果分析

本文所有的实验均在 MATLAB 7.0 上完成,处理器 Intel Celeron 1.8 GHz,内存 1 GB,操作系统为 Windows XP。在实验中选用的载体图像是 256×256 的 Lena 图像,水印信息为有意义的 32×32 的二值图像。根据前面论述可知,这样做已经达到了水印信息的最大嵌入量,即 256×256 的 Lena 图像最多可以嵌入 1 024 bit 的信息,这样更能说明该水印算法具有较好的不可见性及较好的鲁棒性。

下面给出四大类常见攻击的实验结果,这四大类攻击分别是噪声攻击、JPEG 压缩、滤波攻击和剪切攻击(嵌入强度 $d=30$)。这里仅给出有代表性的实验结果,更为详细的实验数据将汇总后给出。

4.1 无攻击下的实验结果

含水印的图像和提取结果如图 2 所示。

4.2 噪声攻击实验

将嵌入水印的 Lena 图像加入均值为 0、方差为 0.003 的高斯噪声对其进行攻击,然后再从加噪后的图像中提取水印,实验结果如图 3 所示。

4.3 JPEG 压缩实验

将嵌入水印的 Lena 图像进行不同程度的 JPEG 压缩,然后再从压缩过的图像中提取水印。实验结果如图 4 所示。

图2 含水印的图像和提取结果

图3 高斯噪声攻击和提取结果

图4 JPEG压缩攻击和提取结果

4.4 滤波攻击的实验结果

将嵌入水印的 Lena 图像进行高斯低通滤波攻击,然后再从滤波后的图像中提取水印,其中标准偏差 sigma = 0.5。实验结果如图 5 所示。

4.5 剪切攻击实验

4.6 实验数据汇总

各种实验结果对比如表 1 所示。

表 1 实验结果对比

攻击类型	参数	Walsh	DCT	攻击类型	参数	Walsh	DCT
无攻击	–	1	1	无攻击	90	1	1
高斯噪声(μ,δ^2)	(0,0.001)	0.9755	0.9677	JPEG压缩/率	80	1	1
	(0,0.003)	0.8398	0.8232		50	0.9798	1
	(0,0.005)	0.7065	0.7014		36	0.8411	1
盐椒噪声(d)	0.008	0.8194	0.8550	高斯低通滤波(4×4)	0.5	0.8098	0.8950
	0.01	0.7993	0.7992		0.8	0.7275	0.8626
	0.04	0.5738	0.5729		1.2	0.6228	0.8239
随机噪声(λ)	5	1	1	均值滤波(窗口大小)	2×2	0.8122	0.8982
	10	0.9420	0.9414		3×3	0.7693	0.9461
	18	0.6878	0.6859				
乘性噪声(n)	0.005	0.9492	0.9420	剪切(比例)	1/16	0.8234	0.8234
	0.01	0.8772	0.8610		1/4	0.5872	0.5872
	0.02	0.7240	0.7136		1/2	0.4568	0.4568

上述所有实验的 PSNR 值均在 10~30,不再详细给出。由于 Walsh 矩阵中值的分布比较均匀,改变一个变换后的系数就要对载体变换前的更多系数同时进行少量改变,即载体变换前的更多系数去分担这一少量改变,这样有利于增强水印的不可见性。同时,Walsh 系数矩阵中值的分布也比较均匀,不像 DCT 系数矩阵一样除了左上角其他部分几乎全是零,这样有利于增强水印的鲁棒性。总体来说,在抵抗噪声方面,基于 Walsh 变换的算法要略好于传统的 DCT 算法;在抵抗 JPEG 压缩及滤波攻击时,传统的 DCT 算法要略好于基于 Walsh 变换的算法;在抵抗剪切方面,由于采用的水印置乱方法相同,两种算法的提取效率一样。

(下转第 2660 页)

数运算所需的时间，T_{mul}表示模乘运算所需时间，T_{inv}表示模逆运算所需时间，模加运算的复杂度相当小，可以忽略。由于在初始段增加了对密钥影子的验证，在部分签名生成与验证阶段增加了对成员身份的验证和消息的盲性，与文献[8]方案比较，由此增加了计算量。但是因为没有可信中心，计算量比文献[6]方案减小。具体计算量见表1。从表1给出的结果可以看出，本方案在保证安全性的前提下，比文献[6]方案计算量减少，并且没有可信中心，因为可信中心很难保证方案的安全，所以本文方案安全性有所提高。虽然比文献[8]方案计算量有所增加，但安全性明显提高。因此本方案在保证安全性的前提下，具有很高的效率。

表1　本文方案与其他门限签名方案计算量和性能的比较

计算量	文献[8]方案	文献[6]方案	本文方案
初始化阶段	是否有可信中心：无 $3T_{exp}+(2t^2-2t+n+1)T_{mul}+(t^2-t)T_{inv}$ 对密钥影子的验证：无	是否有可信中心：有 $(5tn+2t+2)T_{exp}+(tn+4t)T_{mul}$ 对密钥影子的验证：有	是否有可信中心：无 $(3tn-3t+2)T_{exp}+(tn-t)T_{mul}$ 对密钥影子的验证：有
部分签名生成与验证阶段	$5T_{exp}+(5t+1)T_{mul}+(2t-1)T_{inv}$ 消息是否具有盲性：无	$17T_{exp}+(9t-1)T_{mul}+(2t+1)T_{inv}+T_h$ 消息是否具有盲性：有	$12T_{exp}+8tT_{mul}+(2t+1)T_{inv}+T_h$ 消息是否具有盲性：有
门限群签名生成与验证阶段	$3T_{exp}+2T_{mul}+T_{inv}+T_h$ 是否能防范伪造签名攻击：否 是否能防范合谋攻击：否	$4T_{exp}+3T_{mul}+T_{inv}+T_h$ 是否能防范伪造签名攻击：是 是否能防范合谋攻击：是	$4T_{exp}+3T_{mul}+T_{inv}+T_h$ 是否能防范伪造签名攻击：是 是否能防范合谋攻击：是

6　结束语

本文提出以 Shamir 门限方案为基础，克服了传统的只由可信中心参与的签名，可能导致整个系统瘫痪的缺点，并且在传统的(t,n)门限签名方案的基础上，应用可信成员的签名私钥以及增加了消息的盲性，能根本上抵抗伪造签名的攻击。同时，本文的方案也具有较高的效率。

参考文献：

[1] CHAUM D. Blind signatures for untraceable payments[C]//Proc of Crypto: Lecture Notes in Computer Science. 1982:199-203.

[2] OKAMOTO T. Provably secure and practical identification schemes and corresponding signature schemes[C]//Proc of Crypto: Lecture Notes in Computer Science. 1992:31-53.

[3] FAN C I, LEI C L. Efficient blind signature scheme based on quadratic residues[J]. IEEE Electronics Letters, 1996,32(9):811-813.

[4] HARN L. Group-oriented (t, n) threshold digital signature scheme and digital multisignature[J]. IEEE Proceedings of Computers and Digital Techniques, 1994,141(5):307-313.

[5] KONG Jie-jun, ZERFOS P, LUO Hai-yun, *et al*. Providing robust and ubiquitous security support for MANET[C]//Proc of the 9th International Conference on Network Protocols. [S.l.]: IEEE Computer Society,2001:251-260.

[6] JUANG W S, LEI C L, LIAW H T. Fair blind threshold signatures based on discrete logarithm[C]//Proc of National Computer Symposium. [S.l.]: IEEE Computer Society, 2001:371-379.

[7] DONG Y, GO H W, SUI A F, *et al*. Providing distributed certificate authority service in mobile Ad hoc networks[C]//Proc of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks. 2007: 149-156.

[8] 王斌，李建华. 无可信中心的(t,n)门限签名方案[J]. 计算机学报，2003,26(11):1581-1584.

[9] 张文芳，王小敏，何大可. 一个无可信中心的(t,n)门限签名方案的安全缺陷及其改进[J]. 铁道学报，2008，30(3):40-45.

(上接第2656页)

由于本文采用的是有意义的水印信息，即便是当 *NC* 的值小于0.5时，也能通过主观判断来获得正确的水印信息，如剪切比例为0.5时，水印的 *NC* =0.456 8，通过主观判断也可以很明显地识别出水印信息，如图6所示；而 *NC* 的值越接近1，则表明该水印算法的效果越好。

图5　高斯低通滤波攻击和提取结果

图6　1/2剪切和提取结果

本文通过大量的仿真实现验证了该算法，从结果可以看出，水印信息在嵌入后具有良好的不可见性、提取的稳健性和较强的鲁棒性等特性。

5　结束语

本文通过大量的理论证明和实验数据，成功将 Walsh 正交函数系理论应用于数字水印技术中。这为寻找性能更为优良的变换矩阵提供了一个参考。本文提出的基于 Walsh 变换的数字水印算法总结起来有三个优点：a)盲水印，提取水印时不需要原始图像；b)在中高频嵌入水印，具有较强的鲁棒性；c)利用了人眼视觉敏感特性，具有较好的视觉透明性。这给数字图像的版权认证提供便利，因此具有一定的实际应用价值。

参考文献：

[1] WALSH J L. A closed set of normal orthogonal functions[J]. American Journal of Mathmatics, 1923,45(5):5-24.

[2] 叶瑞松，廖海泳. Walsh 变换核矩阵的简单生成及其应用[J]. 通讯和计算机，2005,2(10):21-25.

[3] 胡辉，叶鑫华. 离散 Walsh 变换并行性分析与实现[J]. 计算机工程与应用，2009，45(2):82-84.

[4] 曾凡智，胡学进，王能超. 关于逆 Walsh 序的快速 Walsh 变换算法研究[J]. 计算机工程，2004,30(16)：23-25.

[5] 郭卫斌，王能超，施保昌. M 序 Walsh 变换的快速算法设计[J]. 小型微型计算机系统，2003,24(2)：295-298.

[6] 鲁晓磊，王能超，鲁建华. Walsh 函数的一种新定义及快速算法设计[J]. 应用数学，2004 ,17(增):160-164.

[7] 朱敏莉，王能超. 二维 Walsh 变换的快速算法设计[J]. 武汉交通科技大学学报，2002 ,24(1):5-8.

[8] 李青，王能超. 快速 Walsh 变换的二分算法[J]. 中山大学学报论丛，1996,5(1):12-15.

[9] 苏育才，姜翠波，张跃辉. 矩阵理论[M]. 北京：科学出版社，2006.