一种基于离散小波域的隐蔽通信中的混合型信息隐藏技术

孙启禄，殷肖川，王　宾
（空军工程大学 电讯工程学院，陕西 西安　710077）

摘　要：提出了一种应用于隐蔽通信的基于离散小波(DWT)域的混合型信息隐藏技术，详细阐述了算法流程，分析了其技术特点，给出了实验结果和结论。结果和分析都表明，将信息隐藏技术应用于隐蔽通信，具有较好的效果。

关键词：信息隐藏；离散小波变换；量化；扩频；置乱
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-3516(2004)06-0063-05

信息隐藏的基本原理是利用人体感觉器官对数字媒体的感觉冗余，将被隐藏的数据嵌入在某种覆盖媒体中(如图像、声音、视频、文本等)，很难被观察者和监视系统发现。信息隐藏因为隐蔽了信息的真实存在形式，从而具有不会引起猜疑的优点[1]。信息隐藏的目的是在通信双方之间建立一种隐蔽通信的方式，因而在保密通信领域，其应用价值更为明显。

根据秘密数据的嵌入位置来分，信息隐藏的方法可以分为基于空间域的隐藏和基于变换域的隐藏。与基于空间域的算法相比而言，基于变换域的信息隐藏算法具有较强的鲁棒性和较高的安全性。在该类算法中，常用的变换有离散余弦变换(DCT)和离散小波变换(DWT)。与其它变换(例如DCT)相比，离散小波变换具有下列可用于信息隐藏的特性：空间——频率局部化特性；多分辨率表示特性；与HVS模型吻合特性；更高的安全性。因而，基于DWT的算法一直是稳健型图像信息隐藏的研究热点。

基于上述情况，本文提出一种应用于隐蔽通信的基于图像DWT域的混合型信息隐藏盲提取算法，即在载体图像DWT域的不同层级，分别采用基于量化和基于扩频的不同嵌入方式，实现隐秘信息和数字标识码的同步嵌入以及隐秘信息的安全提取，并通过数字标识码的检测实现信息的真实性验证。最后对其进行了实验验证。

1　基于量化和扩频的信息隐藏算法比较

1.1　基于扩频的信息隐藏算法

该类算法是通过将一个低能量的伪随机高斯白噪声序列加入到宿主信号中达到嵌入隐藏信息的目的。在检测时，首先计算原始序列与待测信号的相关值，然后将该相关值与门限值进行比较以判定待测信号中是否含有隐藏信息。

不失一般性[2]，我们设信息嵌入在图像的变换域中，$X=[x_1,\cdots,x_N]$表示用于嵌入变换域中的N个系数，$W=[w_1,\cdots,x_N]$表示隐藏信息比特流，要求其为满足高斯分布的2值序列，其中，$w_i\in\{-1,1\}$。信号W按下式嵌入系数X中，

$$x_i^w=x_i+\alpha_i w_i \qquad 1\leqslant i\leqslant N \tag{1}$$

式中，x_i^w表示嵌入后的第i个系数，α_i表示信息序列第i项的嵌入强度。对图像进行检测时，首先提取

收稿日期：2004-05-31
基金项目：空军科研基金资助项目
作者简介：孙启禄(1977-)，男，山东泰安人，硕士生，主要从事信息安全技术研究.

待测系数向量 $X^E=[x_1^E,\cdots,x_N^E]$,然后计算 X^E 与原始信息序列的相关值,相关值和阈值 T 进行比较,判定图像是否含有原始信号。检测器是一个相关检测器,该检测器输出的检验统计量 q 为

$$q=\frac{\sum_{i=1}^{n}y_i}{V_y\sqrt{N}}=\frac{M_y\sqrt{N}}{V_y} \tag{2}$$

式中,y_i 表示待检测图像系数的第 i 个系数 x_i^E 与原始序列第 i 项的乘积,M_y 表示 y_i 采样均值,V_y^2 表示 y_i 采样方差,根据应用需求设定阈值 T,判断 q 与 T 的大小关系,按照下述假设检验得到检测结果。

假设检验:

$$H_0:q<T$$

$$H_1:q\geqslant T$$

H_0 表示待测图像不含对应原始信号,H_1 表示包含原始信号。

1.2 基于量化的信息隐藏算法

在基于量化的信息隐藏算法中,原始信息(通常是一个 2 值序列)是通过一种称之为量化 - 替代的方法嵌入宿主数据中的。所谓量化—替代就是先对宿主数据进行量化,然后根据要嵌入的原始信号用相应的另一个量化值来替代宿主信号当前的量化值。这一类水印算法的最大优点是不受宿主信号的干扰。

这里先定义一个量化函数,该量化函数 Q_Δ 首先将实数 x 除以量化步长 Δ,将结果用四舍五入法取整,然后根据取整后结果的奇偶性,将实数 x 映射到集合 $\{-1,1\}$ 上,然后通过式(3)将原始信息比特 $w_i\in\{-1,1\}$ 嵌入到变换系数 x_i 中,嵌入后的系数 x_i^w 为

$$x_i^w=\begin{cases}[x_i]_\Delta & Q_\Delta(x_i)=w_i\\ [x_i]_\Delta+\Delta & Q_\Delta(x_i)\neq w_i\&x_i\geqslant[x_i]_\Delta,1\leqslant i\leqslant N\\ [x_i]_\Delta-\Delta & Q_\Delta(x_i)\neq w_i\&x_i<[x_i]_\Delta\end{cases} \tag{3}$$

式中,N 表示原始信息的长度;$[x_i]_\Delta$ 表示对 x_i 的量化,它的计算公式为

$$[x_i]_\Delta=\mathrm{round}\left(\frac{x_i}{\Delta}\right)\Delta$$

上式中,round 为取整函数。按如下的规则恢复嵌入的信息比特 $\hat{w}_i$

$$\hat{w}_i=Q_\Delta(x_i^E) \tag{4}$$

上式中,x_i^E 表示待测图像的变换系数。

1.3 算法比较分析

在图像 DWT 域中,子带的频率越高,它的系数个数就越多,系数的幅值也越小;子带的频率越低,它的系数个数就越少,系数的幅值也越大。分析式(1)和式(3),可以发现,扩频技术与系数幅值密切相关,频率越高的子带越适合使用扩频技术;而基于量化的算法的稳健性只与量化的步长 Δ 有关,与系数的幅值大小无关,因而,在较高频和较低频的小波子带中分别用基于扩频和基于量化的技术嵌入数字标识码和隐秘信息,都能保证较好的的稳健性。

2 混合型信息隐藏算法

2.1 预处理

为确保信息隐藏的隐蔽性,有必要对图形化的隐秘信息进行置乱处理。这里选用技术成熟的 Arnold 变换作为置乱工具[3],n 维 Arnold 变换,关系如式(5)所示(N 为阶数)

$$\begin{pmatrix}x'_1\\ \vdots\\ x'_n\end{pmatrix}=\begin{pmatrix}1&1&1&\cdots&1&1\\ 1&2&2&\cdots&2&2\\ 1&2&3&\cdots&3&3\\ &\vdots&&&&\vdots\\ 1&2&3&\cdots&n-1&n-1\\ 1&2&3&\cdots&n-1&n\end{pmatrix}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\ (\mathrm{mod}N) \tag{5}$$

Arnold 变换具有周期性,即经过一定步骤的迭代之后,图像将恢复原样。考虑到算法复杂性,这里取 $n=3$,其周期 m_N 与 N 的对应关系如表 1 所示。

表 1　Arnold 变换周期

N	2	3	4	5	6	7	8	9	01	11	12	25	50	60	100	120	125	128	256	480	512
m_N	7	13	7	31	91	21	14	39	217	133	91	155	1 085	2 812	1 085	5 642	755	224	448	22 568	896

取图形化的隐藏信息为 256×256 大小的 256 色灰度图像,其变换周期为 448,实验发现 272 步变换后的图像更加近似于白噪声,因而选定 272 步作为置乱次数,176 步作为置乱恢复次数。

在信息嵌入和提取的过程中,有可能产生低概率随机性的错误;在数据传输的过程中,也可能会引入噪声。为了检查或者纠正被更改的数据,可以对置乱后的图像数据进行差错控制编码。在此,这里选用 8 bit 比特网格编码[4]进行差错控制。

对于数字标识码,采用 m 序列扩频进行预处理,即将数字标识码进行比特重复(过采样),然后使用 m 序列对过采样后的序列进行调制,得到类似白噪声的待嵌入序列。

2.2　嵌入流程

图 1 是嵌入操作的基本流程,其具体步骤如下:

步骤 1:将待嵌入的隐秘信息和数字标识码预处理后,生成与其相对应的两个二进制序列 $W^1=(w_0^1,\cdots,w_{L-1}^1)$ 与 $W^2=(w_0^2,\cdots,w_{M-1}^2)$,其中 L、M 分别为两个序列的长度,$w_i^1\in\{-1,1\}$,$w_i^2\in\{-1,1\}$。

步骤 2:对原始图像进行 L 级尺度的离散小波变换(在此选用 Haar 小波)[5~7],产生 $3L+1$ 个子带图像参数矩阵,即在每一个层次都有水平(如图 2 中 $f_{h,1}$ 所示),垂直(如图 2 中 $f_{v,1}$ 所示)和斜线(如图 2 中 $f_{d,1}$ 所示)3 个方向的小波系数矩阵。在最低分辨率上还有一个低频分量矩阵(如图 2 中 $f_{a,3}$ 所示)。分解级数 L 由嵌入信息量选择,为保证较大嵌入量,一般选择 4 级以上。

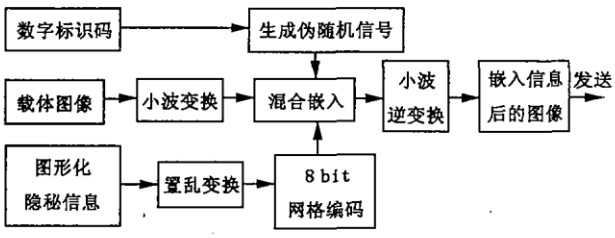


图 1　嵌入流程

(a)　原始图像　　(b)　3 层小波分解后的各子带信息　　(c)　3 层小波变换的结构图

图 2　3 层小波的图像分解

步骤 3:在小波分解的第二层,用基于扩频技术的方法嵌入信号 W^1:

$$f_{0,2}^w(m,n)=f_{0,2}(m,n)+\alpha\times\theta_{0,2}(m,n)\times w^1(m,n),0\in\{h,v,d\} \tag{6}$$

式中,$f_{0,2}^w$表示嵌入水印后的第二层小波系数;α 是水印嵌入总能量的控制参数;$\theta(m,n)$表示水印嵌入局部能量的控制参数,该参数可通过 HVS 模型计算得到[8~9]。

步骤 4:在小波分解的较高层,用基于量化技术的方法嵌入信号 W^2:

$$f_{o,p}^w(m,n)=\begin{cases}[f_{o,p}(m,n)]_\Delta & Q_\Delta(f_{o,p}(m,n))=w^2(m,n)\\ [f_{o,p}(m,n)]_\Delta+\Delta & Q_\Delta(f_{o,p}(m,n))\neq w^2(m,n)\,\&\,f_{o,p}(m,n)\geqslant[f_{o,p}(m,n)]_\Delta\\ [f_{o,p}(m,n)]_\Delta-\Delta & Q_\Delta(f_{o,p}(m,n))\neq w^2(m,n)\,\&\,f_{o,p}(m,n)<[f_{o,p}(m,n)]_\Delta\end{cases} \tag{7}$$

式中:$o\in\{h,v,d\}$,$p\in\{3,\cdots,L\}$。

步骤 5:对嵌入后的小波系数进行小波逆变换(IDWT),得到嵌入水印后的图像。

2.3 提取检测流程

图 3 给出了提取检测的基本流程,其具体步骤如下:

步骤 1:接收方将原始数字标识码采用与发送方相同的方式产生与其相对应的二进制序列 $W^2=(w_0^2,\cdots,w_{M-1}^2)$,其中 M 分别为序列的长度,$w_i^2\in\{-1,1\}$。

步骤 2:将待测图像进行 L 级离散 Haar 小波变换。假设变换后得到的各层的系数为 $f_{o,l}^D(m,n)$。下标 l 表示小波变换的层,$l\in\{1,\cdots,L\}$;$o\in\{h,v,d\}$ 表示水平,垂直和倾斜 3 个子带。

步骤 3:在第二层的小波子带中用式(2)计算检验统计量 q,并与阈值 T(选定 $T=6$)比较判定隐秘信息来源的真实性。

步骤 4:在第三层及以上的小波子带中用式(4)恢复信号,得到恢复后的信号 $\hat{W}^2$,对 $\hat{W}^2$ 进行重组,解码,进行 176 步三维 Arnold 变换,恢复原始图形化隐秘信息。

3 试验结果及结论

我们采用 256×256 大小的 256 色灰度 Lenar 图像作为测试图像,在 1024×768 的 256 色 BMP 图像中进行了实验,结果如图 4 所示其中,sim 为提取图像与原始图像的相似度。

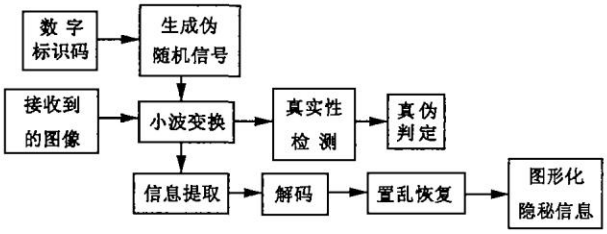
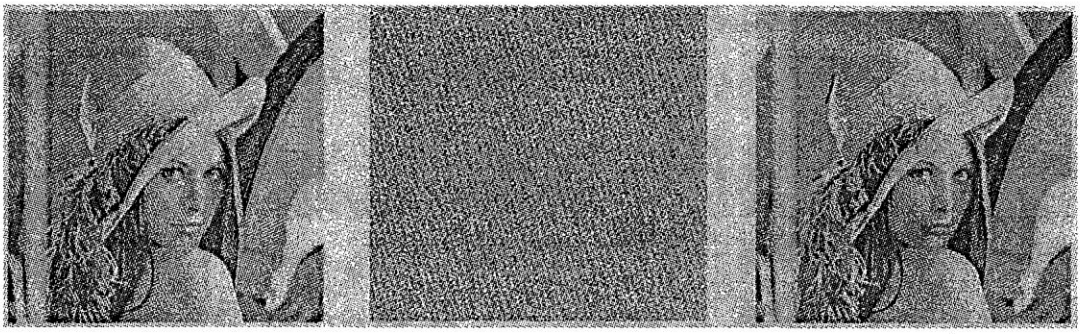


图 3 提取检测流程

分别对载体图像进行、中度高斯模糊、30% JPG 压缩的情况下,数字标识码仍能正确检测,表明该算法具有较高的稳健性,对于信息的真伪度具有很强的鉴别能力。

综上所述,该算法具有较好的稳健型,具有下述优点:①安全性高;②容忍度强;③检测能力强。能够抵抗各种常规的攻击方式,非常适合应用于高敏感度保密通信。



(a)原始隐秘信息图像 (b)272 步 Arnold 变换后的图像 (c)正常提取的图像(sim=95.7%)

(d)30% JPEG 压缩(sim=89%) (e)中度高斯模糊(sim=74.3%) (f)50%加性噪声(sim=52%)

图 4 实验结果

参考文献:

[1] Cox I J, Miller M L. The First 50 Years of Electronic Watermarking[J]. Journal of Applied Signal Processing, 2002, (2):126-132.

[2] Cox I J, Kilian J, Leighton T, et at. Secure Spread Spectrum Watermarking for Multimedia[A]. Proceedings of The IEEE International Conference on Image Processing ICIP97[C]. USA October: Santa Barbara, California, 1997, 1673 - 1687.
[3] 孙　伟. 关于 Arnold 变换的周期性[J]. 北方工业大学学报, 1999, 11: 33 - 35.
[4] Cox J, Miller L, Bloom A. 数字水印[M]. 王　颖. 北京:电子工业出版社, 2003.
[5] Kundur D, Hatzinakos D. A Robust Digital Image Watermarking Method Using Wavelet - Based Fusion[A]. Proc. 4th IEEE Int. Conf. Image Processing97[C]. CA: Santa Barbara, 1997. 544 - 547.
[6] Hongmei Liu, Jiufen Liu, Jiwu Huang, et al. A Robust DWT - Based Blind Data Hiding Algorithm[J]. IEEE International Symposium on Circuits and Systems, 2002, (2): 672 - 675.
[7] 李晓春. 一种基于小波变换的图像融合新方法[J]. 空军工程大学学报(自然科学版), 2003, 4(6): 55 - 57.
[8] 刘　挺. 一种基于 DWT 和 HVS 的彩色图像混合型数字水印技术[A]. CCICS2003[C]. 北京:科学出版社, 2003, 319 - 326.
[9] 吴崇明, 王晓丹. 数字水印系统的鲁棒性和常见的攻击[J]. 空军工程大学学报(自然科学版), 2002, 3(1): 90 - 93.

(编辑:门向生)

A Confidential - Communication - oriented and DWT - Based Hybrid Information Hiding Technology

SUN Qi - lu, YIN Xiao - chuan, WANG Bin
(The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China)

Abstract: A DWT based on hybrid information hiding technology oriented to confidential communication for images is presented, based on this, the flowcharts are described in detail and their technological characteristics are analyzed. Then, the results of the experiments are shown and the conclusion is made. Both the results and the analysis indicate that the algorithm is good in performance in the application of information hiding technology to confidential communication.

Key words: information hiding; DWT; quantization; spread spectrum; scrambling

(上接第 52 页)

参考文献:

[1] 常　硕, 陈忠辉, 张智军. 超宽带信号在波导中传播的 FDTD 分析[J]. 空军工程大学学报(自然科学版), 2003, 4(5): 53 - 55.
[2] 葛德彪, 闫玉波. 电磁波时域有限差分法[M]. 西安:西安电子科技大学出版社, 2003.
[3] 王小平, 曹立明. 遗传算法 - 理论、应用与软件实现[M]. 西安:西安交通大学出版社, 2003.
[4] Aaron Kerkhoff, Robert Rogers, Hao Ling. The Use of The Genetic Algorithm Approach in The Design of Ultra - Wideband Antennas [J]. IEEE Trans, 2001, (7): 189 - 194.

(编辑:门向生)

A Novel UWB Abnormal Monopole Antenna

XIAO Zhi - wen, LU Wan - zheng, MA Jia - jun
(The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China)

Abstract: This paper presents a novel abnormal monopole antenna by means of optimization with FDTD method genetic algorithm. The relative bandwidth of the antenna with input voltage standing wave ratio less than 2.5 exceeds 100%. This antenna can be used in ultra - wideband communication systems.

Key words: ultra - wideband antenna; finite difference time domain; genetic algorithm