充分利用视觉冗余的图像不同域信息掩密术

周琳娜[1,2], 郭云彪[2], 杨义先[1]
(1. 北京邮电大学信息安全中心, 北京 100876; 2. 北京电子技术应用研究所, 北京 100091)

摘 要: 充分利用人类视觉冗余实现安全地秘密信息嵌入是信息隐藏技术追求的目标. 现有图像信息掩密技术很多是在图像数据相同域实现的. 本文将信号量化压缩编码的理论和方法应用于信息掩密, 提出了一种充分利用人类视觉冗余的图像不同域信息掩密新方法并设计了三种纠错方法保证了密文信息的准确盲提取和复原. 实验表明, 该算法对空域图像数据的统计特性改变较少, 具有更高的隐藏容量和安全性.

关键词: 信息掩密; 视觉冗余; 隐藏容量; 空间域; 频域
中图分类号: TP391 文献标识码: A 文章编号: 0372-2112 (2006) 12A-2429-05

High Capcity Image Steganography Based on Transform Domain

ZHOU Lin-na[1,2], GUO Yun-biao[2], YANG Yi-xian[1]
(1. *Beijing University of Posts and Telecommunications, Beijing* 100876, *China*;
2. *Beijing Application Institute of Electronic Technology, Beijing* 100091, *China*)

Abstract: A new image steganography mothod simulating quantization processing in image Joint Photographic Experts Group compression is presented. Three kinds of error correctiong coding is applied to assure that hidden information can be retrieved accurately. Experimental results demonstrate that the proposed method has high capacity good vision performance.

Key words: steganography; vision redundance; hidden capacity; space domain; frequency domain

1 引言

信息隐藏是利用人类感觉器官的不敏感, 以及数字信号本身存在的感觉冗余, 将信息隐藏于一个宿主信号中, 不被觉察到或不易被注意到, 而且不影响宿主信号的知觉效果和使用价值[1]. 因此, 充分利用人类视觉冗余实现安全地秘密信息嵌入是信息隐藏技术追求的目标. 信息隐藏技术有三个属性: 不可感知性、鲁棒性和隐藏容量[2]. 旨在隐蔽通信的信息掩密术(stegonagraphy)强调的是不可感知性和隐藏容量. 而用于版权保护的数字水印技术, 其强调的则是不可感知性和鲁棒性. 不同的应用目的、不同的强调属性造就了信息隐藏技术具体实现的多样性和复杂性.

很多信息隐藏算法是在相同域实现的, 有些信息隐藏算法是在不同域实现的. 典型的不同域信隐藏算法大都应用于数字水印, 它可以充分利用人的视觉冗余来增强水印的鲁棒性. Cox 等人利用扩展频谱的方法在空域图像的 Discrete Cosine Transform 域(以下简称 DCT 域)低频系数中嵌入水印信息[3], 由于 DCT 域低频系数是人类视觉感知的最重要部分, 如果以期对这些感知重要区域进行篡改攻击来消除水印, 将不可避免地影响图像的主观质量, 因此, Cox 水印具有较强的鲁棒性. 沿用 Cox 算法将信息嵌入到图像中视觉感知最重要部分的鲁棒性水印思路, 涌现了多种改良的变换域鲁棒水印算法, 如根据频率系数的刚可察觉失真度(just noticeable difference, JND)决定水印嵌入强度的图像自适应数字水印算法[4], 基于视觉对比度掩盖模型的水印算法[5], 根据图像熵掩盖模型设计的自适应嵌入水印算法[6]和将人眼多种视觉特性融合在一起的小波域图像水印[7]等. 这些算法将视觉感知模型引入到扩频水印算法中对水印信息的嵌入强度进行控制, 以保证其嵌入水印信息的不易察觉性, 并将水印信息嵌入到图像的重要感知区域, 增强了水印的鲁棒性.

不同域信息隐藏技术具有充分利用视觉冗余、提高嵌入强度等优点, 但应用于掩密术的不同域信息隐藏算法却并不多见. 典型的不同域数字水印算法不能简单照搬应用到掩密术中, 它有以下局限性: (1)这类应用于版权保护的水印技术

收稿日期: 2006-05-08; 修回日期: 2006-11-20
基金项目: 国家863基金(No. 2005AA145010); 国家242基金(No. 2005C43)

追求的是强鲁棒性,往往嵌入的水印信息容量较小,有时甚至只有1比特水印信息;(2)有些水印算法在检测时都需要原始图像的参与,不能进行盲检测;(3)这些算法将少量的水印信息反复嵌入多次,最后靠提取出水印信息的平均值和原始图像的比较来确定是否含有水印,而不能保证嵌入的秘密信息能够百分百完全复原.

到目前为止,信息掩密术已在图像数据的相同域中实现了多种成熟的掩蔽算法[8~10].文献[11]中虽然在小波域中实现了抵抗JPEG压缩的信息掩密术,但该技术仍是以增强嵌入信息的鲁棒性为目的,且隐藏容量较小,小于0.002bpp.本文在充分研究人类视觉感知模型的基础上,将秘密信息的嵌入与JPEG压缩编码理论紧密结合,利用量化有损编码压缩失真来度量空域图像冗余信息,充分利用人类视觉冗余,提出了一种在空域图像的频域变换数据中实现秘密信息的自适应嵌入方案,并设计特定的纠错方法解决了不同域隐藏信息准确复原的难题,实现了具有更好不可感知性、高安全性、大隐藏容量的图像不同域自适应信息掩密技术.

2 用JPEG量化压缩失真度量空域图像视觉冗余

人的视觉特性是指人眼视觉对于视觉信号变化的响应情况.人的视觉系统是一个复杂非线性系统,正是由于人类视觉的非线性才给我们图像信息掩密留下了较大的回旋余地,我们可以对表征图像的数据做某些修改而不影响人们的视觉感受,这就是所谓的视觉冗余.

JPEG是一种有损压缩图像处理标准,图像处理前后存在失真,由于图像的JPEG压缩处理充分地利用了人类的视觉冗余,所以这种量化处理具有较高的压缩比,并且失真是肉眼所无法辨识的,这些在JPEG压缩过程中可以被量化压缩掉的图像冗余信息也可以用来于信息掩密.图1以一个8*8图像数据块为例说明了JPEG压缩前后图像的变化情况[12]:

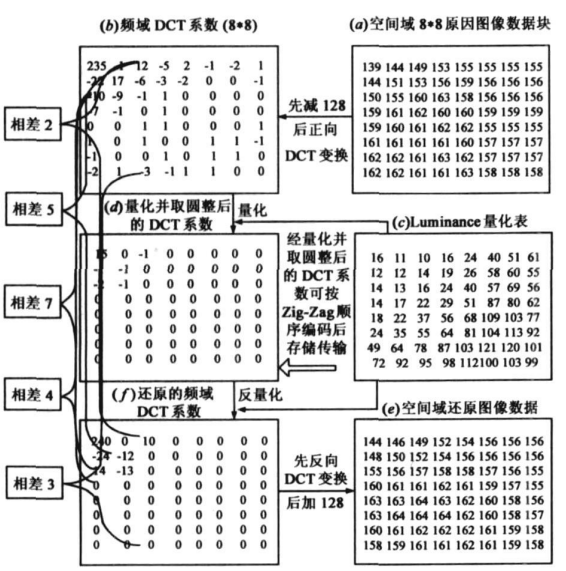


图1 频域DCT系数量化压缩冗余

我们将图1中的量化前频域DCT系数记为一个二维数组Org_DCT[x][y](其中,x取0~7,y取0~7),反量化后恢复出的空间域还原图像数据单元中的数据也记为一个二维数组Rev_DCT[u][v](其中,u取0~7,v取0~7),由图1可以看出,Org_DCT[x][y]并不完全等于Rev_DCT[u][v],这是因为对频域DCT系数进行量化压缩后,需要对量化后的DCT系数取圆整后再进行存储和传输,因此,再反量化恢复出的频域DCT系数并不等于原始频域DCT系数.JPEG图像标准的成功普及说明,这种对频域DCT系数量化压缩失真是人类视觉所感觉不到的,在某种程度上可以说,JPEG有损压缩去掉的是图像中的冗余信息部分.可以用压缩前后的图像数据的差异来度量图像的视觉冗余.

2000年6月,张春田教授提出了信息隐藏和信号编码共同分享视觉冗余同一块蛋糕的观点[13],认为编码压缩的冗余空间可以用来容纳隐藏信息.本文借鉴和发展了这个观点,提出了用信号量化压缩编码方法来度量可用于隐藏信息冗余空间的方法,充分利用人类视觉冗余,实现了基于信号频域量化压缩特性的图像不同域信息掩密技术.

JPEG量化压缩失真是为人类视觉所无法感知的,JPEG压缩处理是一种人们常用的图像处理方式,可以模拟JPEG量化压缩的图像处理方式设计出充分利用人类视觉冗余的图像不同域信息掩密算法,该算法先将空间域图像转化到频域,再对频域DCT系数进行修改来嵌入秘密信息,其嵌入深度由JPEG量化压缩失真来控制.

3 秘密信息自适应嵌入算法

3.1 利用量化压缩失真控制嵌入深度

利用量化压缩失真对嵌入深度尺度的控制主要取决于两个因素:图像DCT系数的绝对值和图像JPEG量化容许误差.若$L_{i,j}$为该图像量化表中第i行、j列个量化系数,那么图像JPEG量化后系数将会向上或向下取圆整,其量化容许误差应为$L_{i,j}/2$,设$Y_{i,j}$为某个DCT系数块的第i行、j列量化前的DCT系数,将$\mathrm{Scale}_{i,j}$定义为DCT系数$Y_{i,j}$可以修改的尺度,则对$\mathrm{Scale}_{i,j}$的限定如下:

$$\mathrm{Scale}_{i,j}=\min\{\lfloor L_{i,j}/2\rfloor,\lfloor \mathrm{abs}(Y_{i,j})\rfloor\} \quad (1)$$

则DCT系数$Y_{i,j}$可嵌入秘密信息的位数$D_{i,j}$为:

$$D_{i,j}=\log_2\mathrm{Scale}_{i,j}-n,\ \text{其中}\ n\in[1,2,\cdots,\log_2\mathrm{Scale}_{i,j}] \quad (2)$$

具体嵌入时用$\mathrm{Scale}_{i,j}$对$Y_{i,j}$进行操作,设$Y'_{i,j}$为$Y_{i,j}$嵌入了秘密信息后的DCT系数,$S_m(m=1,2,3,\cdots)$是秘密信息序列,则可按式(3)进行秘密信息的自适应嵌入操作:

$$Y'_{i,j}=\begin{cases} Y_{i,j}, & \mathrm{Scale}_{i,j}=0 \\ Y_{i,j}-\mathrm{LSB}_{D_{i,j}}(Y_{i,j})+\mathrm{LSB}_{D_{i,j}}(S_m), & \text{其他} \end{cases} \quad (3)$$

在式(1)~(3)中,abs(X)为X取绝对值运算,LSBk(X)表示对X取k位最低有效位,式(2)中n为对嵌入深度的控制,n越大,嵌入深度越浅,隐藏容量越小,同时秘密信息嵌入对携密图影响的不可感知性越好.

提取为嵌入的逆过程,得到携带有秘密信息的$Y'_{i,j}$后,先根据量化系数$L_{i,j}$和$Y'_{i,j}$求出该DCT系数嵌入秘密信息位

数 $D_{i,j}$.

$$D_{i,j}=\min\{\lfloor[\log_2(L_{i,j}/2)]-n\rfloor,\lfloor\log_2 Y_{i,j}-n\rfloor\} \quad (4)$$

式(4)中 n 为与嵌入方约定好的对嵌入深度的控制. 根据求出的 $D_{i,j}$即可由式(5)从 $Y'_{i,j}$ 提取出密文信息 S'_m

$$S'_m=\begin{cases}\mathrm{LSB}_{D_{i,j}}(Y_{i,j}), & D_{i,j}\neq 0\\ \Phi(\text{空集, 不提取}), & D_{i,j}=0\end{cases} \quad (5)$$

上述利用量化压缩失真控制秘密信息自适应嵌入的操作是在图像的 DCT 域进行的, 具体实现时先将空间域图像数据经正向 DCT(Forward DCT) 变换到频域, 利用量化压缩失真控制对频域 DCT 系数进行秘密信息自适应嵌入, 再将携带有秘密信息的频域图像数据逆向 DCT(Inverse DCT) 变回到空间域. 由上述过程可以看出, 图像不同域信息掩密术的秘密信息嵌入、携密空间域图像传输和秘密信息提取过程需要对图像数据进行多次域变换. 而图像域变换的计算舍入误差, 使得经过域变换的图像数据存在一定的失真, 如果不经任何处理而只是简单地将秘密信息嵌入, 所提取出的信息将会有较原始秘密信息有较多误码. 因此, 在不同域信息掩密技术中必须设计合理的差错控制技术来保证密文的百分百准确可靠复原. 根据分析研究和实验结果, 我们综合运用下列几种纠错方式, 保证了秘密信息嵌入与脱密处理的准确可靠性.

3.2　保证密文可靠复原的三种纠错方式

3.2.1　二维奇偶校验码纠错

采用二维奇偶校验码纠错的方式可进行检错和纠错, 该纠错方法在 64 位中能可靠地纠正一位错误. 具体方法为: 在秘密信息嵌入端将要嵌入的密文数据每 64 位排列为 8× 8 的二维阵列, 每行和每列都用模 2 和算出一个校验位, 将算出的 16 位校验位和 64 位密文数据一起组成新的一维 80 位密文数据进行嵌入; 在秘密信息提取端就可用提取的 16 位校验位对 64 位密文数据进行检错和纠错. 二维奇偶校验码纠错的 64 位校验图如图 2 所示.

	密文数据	校验位
密文数据	× × × × × × × ×	×
	× × × × × × × ×	×
	× × × × × × × ×	×
	× × × × × × × ×	×
	× × × × × × × ×	×
	× × × × × × × ×	×
	× × × × × × × ×	×
	× × × × × × × ×	×
校验位	× × × × × × × ×	

图 2　64 位二维奇偶校验码纠错

3.2.2　负反馈纠错方法

由于图像域变换的计算舍入误差将会导致不同域信息掩密技术的掩密过程嵌入密文和脱密过程脱出密文会有较多的误码, 而这些误码很难单纯用网状奇偶纠错方法完全保证纠正修改过来. 因此, 我们设计了第二钟纠错方法: 负反馈纠错. 根据控制学负反馈理论, 我们根据输出与输入之间的偏差来调节修正输入, 使输出严格地跟随输入. 具体的做法是: 在秘密信息嵌入端增加一个负反馈调节过程, 将携密的空间域图像数据再经过 IDCT 变换得到携密频域图像数据, 根据掩密过程原始生成的携密频域图像数据与经过 FDCT、IDCT 两次域变换生成的携密频域图像数据的差值来调节秘密信息的嵌入过程. 这样经过多次秘密信息的嵌入提取修正过程可以使得输入与输出偏差最小. 负反馈纠错调节过程的示意图如图 3 所示, 这个不断微调的负反馈调节过程将最终得到一个合适的携密空间域图像使得掩密端携密频域数据和脱密端携密频域数据趋于一致, 从而使由于域变换引起的秘密信息提取误码概率降到最低.

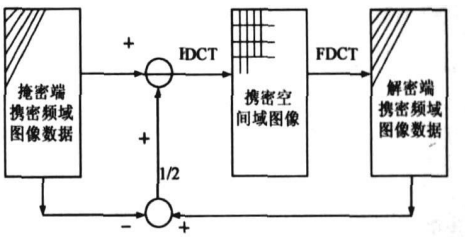


图 3　负反馈纠错调节过程示意图

3.2.3　ECM 纠错方式

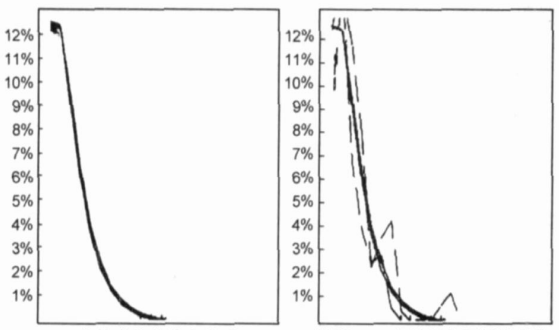
由于图像不同域信息掩密的秘密信息嵌入、提取过程经过了 FDCT、IDCT、FDCT 共 3 次域变换, 利用上述两种纠错方法只能降低错误几率, 并不能完全保证秘密信息能够百分百准确复原. 因此, 为了保证秘密信息能够百分百准确复原, 我们又设计了第 3 种纠错思路: ECM 纠错, 将出错块的密文重新反馈后再嵌入. ECM 纠错是在前两种纠错基础上进行的, 在前两种纠错机制下完成一个 DCT 系数块秘密信息嵌入操作, 再在秘密信息嵌入端对该携密 DCT 系数块进行脱密, 将脱密出的密文与原始密文进行比较, 若此时在拥有前两种纠错机制前提下还存在误码, 则启动 ECM 纠错方式. ECM 纠错将该 DCT 系数块置上标志, 并将该 DCT 系数块所嵌入的秘密信息反馈后再嵌入. ECM 纠错在前两种纠错的基础上进行, 它从根本上保证了密文的准确复原, 当然错误码反馈和再嵌入降低了信息隐藏容量.

这三种纠错方式在图像不同域信息掩密技术中是相互结合、相互补充而应用的: 首先采用负反馈纠错方法将由于图像域转换计算舍入误差引起的误码降低到最低限度, 再用网状奇偶纠错方法进行检错纠错, 对网状奇偶纠错方法无法纠正的错误, 最后再采用 ECM 纠错进行反馈再嵌入处理. 这三种纠错方法在图像不同域信息掩密技术中的结合应用, 既保证了秘密信息的可靠复原, 又保证该技术有较大的隐藏容量.

4　实验与性能分析

4.1　抗检测能力(不可感知性)

我们采用了图像数据统计规律(图 4) 和图像不同位平面抽取[14](图 5) 两个流行的图像信息掩密技术检测方法对图像不同域信息掩密技术和同域 LSB 信息掩密技术进行了对比测试实验, 实验结果充分地验证了本技术的安全性和抗检测能力.



注:两个实验均采用同一幅标准测试图像 LENA.BMP,嵌入的密文为同一文本文件.图中实线为原始图像的统计特性曲线,虚线为嵌入后图像的统计特性曲线.

图 4 图像特性分析检测方法

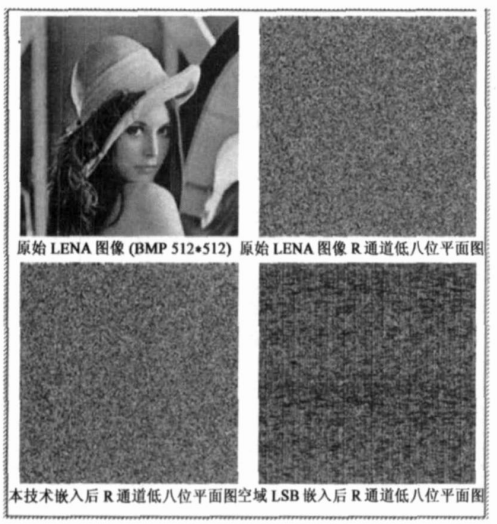


图 5 图像不同位平面抽取检测方法

图像不同域信息掩密技术是将空间域图像变换到频域内再进行秘密信息嵌入处理,其存储和传输的是空间域携密图像数据,而进行秘密信息嵌入修改的是频域图像数据.图像的多次域变换运算在带来大量"麻烦"的误码同时也使得对频域图像数据嵌入修改"痕迹"被均匀地扩散在携密空间域图像数据中.图像不同域信息掩密技术较好地保留了原始空间域图像的数据特性,对携密空间域图像数据的检测分析难以检出异常,更难以在嵌入修改"痕迹"被均匀扩散的携密空间域图像数据中提取出与密文有关的信息.因此,图像不同域信息掩密技术具有较相同域信息掩密技术更高的抗检测、破解能力.

4.2 隐藏容量

本算法以 JPEG 量化压缩的图像信息冗余作为秘密信息嵌入的安全度量,在图像的不同于综合运用了三种纠错方式保证了秘密信息的百分百准确提取,实现了在图像不同域秘密信息安全、可靠的嵌入与提取,并且由于只是进行了图像的域变换而没有量化的过程,部分图像的高频分量不为零,可以最大量地利用 JPEG 图像的中频、高频 DCT 系数携带秘密信息,与文献[11]中小波域信息掩密术相比,在几乎相同峰值信噪比的条件下,该技术具有更大的隐藏容量.

表 1 小波域信息掩密术和本技术隐藏容量对比

技术 / Image	小波域信息掩密术[11]		本技术	
	PSNR	Hidden capacity	PSNR	Hidden capacity
Boat	39.13	0.0020	39.11	0.152
Lena	39.15	0.0017	39.13	0.161
Mandrill	39.15	0.0020	39.11	0.155
Peppers	39.13	0.0017	39.13	0.153

5 结论

本文以图像 JPEG 量化压缩机理作为秘密信息嵌入深度的度量,充分利用了空间域图像中冗余信息的设计并实现了一种空域图像在 DCT 域的信息掩密技术.以 JPEG 量化压缩机理为嵌入深度的安全度量和图像不同域转换之间存在的随机计算误差使得该技术没有直接的嵌入修改痕迹,该技术携密空间域图像和直接将原始空间域图像进行 JPEG 压缩后再解压缩生成空间域图像的视觉效果和数据统计特性难以区分.负反馈纠错、网状奇偶纠错和 ECM 纠错三种纠错方法在该技术中的结合应用,保证了秘密信息的可靠复原,更保证该技术具有较大的隐藏容量.实验证明,该技术具有较高的不可感知性和隐藏容量.

本文较好地在空域图像的 DCT 变换域中实现了具有较高的不可感知性和隐藏容量的信息掩密技术,在信息掩密技术的不可感知性和隐藏容量两个基本属性的探索和提高上作了研究.该方向的未来研究应进一步研究更高效的纠错码以进一步提高隐藏容量和将图像不同域掩密思路推广到视频和音频掩密术中应用.

参考文献:

[1] 尤新刚,周琳娜,等.信息隐藏学科的主要分支及术语[A].夏大平.信息隐藏第三届全国学术研讨会论文集[C].西安:西安电子科技大学出版社,2001.43-50.

[2] 郭云彪.信息隐藏的安全性研究[D].天津:天津大学,2005.

[3] Ingemar J Cox. A secure robust watermark for multimedia[A]. 1st Workshop on Information Hiding[C]. UK: University of Cambridge, 1996. 143-156.

[4] Podilchuk C I, Zeng W J. Image-adaptive watermarking using visual models[J]. IEEE Journal on Selected Areas in Communications, 1998, 16(4): 525-539.

[5] Swanson M D, Zhu B, et al. Transparent robust image watermarking[A]. Proc IEEE Int Conf Image Processing[C]. Switzerland: Lausanne Press, 1996. 211-214.

[6] Suthaharan S. Perceptually tuned robust watermarking scheme for digital images[J]. Pattern Recognition Letters, 2000, 21(2): 145-149.

[7] Barni M, Bartolini F, et al. Improved wavelet-based watermarking through pixel-wise masking[J]. IEEE Transactions on Im-

age Processing, 2001, 10(5): 783- 791.
[8] Steganography Software for Windows[DB/OL]. http://members.tripod.com/steganography/stego/software.html, 1996-04-16/1996-08-05.
[9] Westfeld, Pfitzmann. High capacity despite better steganalysis [A]. Moskowitz. Information Hiding 4th International Workshop[C]. Berlin: Springer-Verlag Press, 2001. 289- 302.
[10] Provos. Defending against statistical steganalysis[A]. 10th USENIX Security Symposium[C]. New York: Academic Press, 2001. 189- 195.
[11] Jianyun Xu, Andrew H, et al. JPEG compression immune steganography using wavelet transform [A]. International Conference on Information Technology[C]. Berlin: Springer-Verlag Press, 2004. 205- 211.
[12] CCITT Recommendation T.81, Digital Compression and Coding of Continuous-tone Still Images[S].
[13] 张春田. 关于信息隐藏信道模型的讨论[A]. 夏大平. 信息隐藏第二届全国学术研讨会论文集[C]. 西安: 西安电子科技大学出版社, 2000. 306- 311.
[14] 金淮斌. 基于数学形态学的图像信息隐藏检测研究[A]. 夏大平. 信息隐藏第二届全国学术研讨会论文集[C]. 西安: 西安电子科技大学出版社, 2000. 215- 220.
[15] 王新梅, 肖国镇. 纠错码 ——原理与方法[M]. 西安: 西安电子科技大学出版社, 1991. 38- 56.

作者简介:

周琳娜　女, 1972 年 4 月出生于湖南省邵阳市, 1993 年毕业于解放军信息工程大学通信工程系, 现为北京电子技术应用研究所副研究员, 主要研究方向为图像分析与处理、信息隐藏、多媒体信息安全.
E-mail: wdmzln@263.net

郭云彪　男, 1969 年 8 月出生于河北省赵县, 博士, 北京电子技术应用研究所副所长, 副研究员, 中国电子学会高级会员, 中国计算机学会高级会员, 主要研究领域为: 信号处理、多媒体信息安全.
E-mail: gybgnx@hotmail.com