

一种大容量的 DCT 域信息隐藏算法

谢建全^{1,2)} 阳春华¹⁾ 黄大足^{1,2)} 谢多思³⁾

¹⁾(中南大学信息科学与工程学院,长沙 410083) ²⁾(湖南财经高等专科学校信息管理系,长沙 410205)

³⁾(南京理工大学自动化学院,南京 210094)

摘要 基于 DCT(离散余弦变换)域的信息隐藏算法是目前应用最广的变换域算法,此类算法的最大不足是嵌入信息量小。通过分析 DCT 域隐藏算法隐藏容量少的原因,提出了一种大容量的 DCT 域信息隐藏算法。算法首先对载体图像进行频谱均匀化处理,然后对图像进行全局 DCT 变换,并将隐藏信息嵌入到载体图像的低频 DCT 系数上,信息嵌入采用分段量化的方法实现,提取隐藏信息时不需要原始载体图像。实验结果表明,该算法的嵌入容量大,不可感知性好。

关键词 信息隐藏 离散余弦变换 频谱均匀化 量化 盲提取

中图法分类号:TP309.2 文献标识码:A 文章编号:1006-8961(2009)08-1542-05

A High Capacity Information Hiding Algorithm in DCT Domain

XIE Jian-quan^{1,2)}, YANG Chun-hua¹⁾, HUANG Da-zu^{1,2)}, XIE Duo-si³⁾

¹⁾(School of Information Science and Engineering, Central South University, Changsha 410083)

²⁾(Department of Information Management, Hunan Finance and Economics College, Changsha 410205)

³⁾(School of Automation, Nanjiang University of Science and Technology, Nanjiang 210094)

Abstract So far information hiding algorithm based on DCT domain is the most extensive one in all transformation domain algorithm applications. Its most serious disadvantage is the low capacity for information hiding. The reason why only small capacity information can be hidden in DCT domain of an image is analyzed, and a high capacity blind information hiding algorithm based on DCT domain is proposed. In our algorithm, the uniform spectrum processing is first applied to the original image. Then, a global DCT transformation of the image is finished. Finally, the information, which is to be hidden, is embedded into the low frequency coefficients in DCT domain. Moreover, the information hiding is implemented by using segment quantification method, extracting the hidden information without using the original image. Experiment shows that our algorithm has a high capacity of information hiding and good imperceptibility.

Keywords information hiding, DCT, uniform spectrum, quantification, blind extracting

1 引言

目前用来作为信息隐藏的载体有文字、图像、语音或视频等多种不同格式的文件,但使用方法没有本质的区别,都是利用人类的感知局限性来隐藏信息。图像由于冗余空间大,是目前用得最多的信息

隐藏载体。基于图像的信息隐藏技术,可以归类于两种:基于变换域的隐藏技术和基于空间域的隐藏技术。一般意义上,空间域方法算法简便,信息隐藏量大,信息嵌入和提取速度快。但目前大多数空间域隐藏算法都是基于图像像素 LSB(即最不重要比特位)的嵌入或进行了一定改进的思想^[1],这种水印算法对多数攻击的鲁棒性不强,而且许多空间域

基金项目:国家自然科学基金项目(60574030)

收稿日期:2008-01-30;改回日期:2008-05-19

第一作者简介:谢建全(1964 ~),男,教授。中南大学计算机应用技术专业博士研究生。主要研究方向为信息安全技术。

E-mail: xiejianquan@sina.com

隐藏算法还容易被检测到^[2],因而安全性不高。为提高隐藏信息的鲁棒性,不少学者提出了多种变换域方法,比如 DCT(离散余弦变换)域算法、DWT(离散小波变换)域算法、DFT(离散傅里叶变换)域算法、哈德码变换域算法、Fourier-Mellin 算法和脊波变换域算法等多种,其中 DCT 域算法由于与压缩标准(JPEG, MPEG, H261/263)兼容,因此是应用最广的变换域算法。目前的变换域算法的最大不足是嵌入信息量小、算法复杂、嵌入和提取信息速度较慢^[3]。所以,空间域方法更适合于机密信息的通信,而变换域方法更适合于版权保护(如数字水印)等领域,而很难用于隐藏储存和隐蔽通信等领域。如何提高变换域隐藏方法的隐藏容量,使其适合信息隐蔽通信的需要,是众多学者关注的研究方向,比如文献[4]提出的用 1 比特承载多比特信息的方法,但它的实质只是提高了嵌入效率,并没有提高嵌入容量。本文分析了 DCT 变换域方法隐藏信息容量少的原因,提出了提高 DCT 变换域隐藏容量的实现方法,在保持其隐藏信息的鲁棒性和安全性的前提下,大大提高其信息隐藏量,并且提取信息时不需要原始图像及其他辅助信息。

2 DCT 域算法隐藏容量分析

绝大多数自然图像都是低频信号^[5],由于 DCT 变换的良好能量压缩能力,可以将图像的能量汇集到有限的几个低频系数上,即具有较大幅度的 DCT 变换系数数目相对较少。文献[6]指出自然图像的 DCT 变换交流分量的系数的概率分布符合拉普拉斯分布模型:

$$p(x) = \frac{\lambda}{2} e^{-\lambda|x|} \quad (1)$$

式中, $\lambda = \frac{\sqrt{2}}{\sigma}$, σ 为图像的标准差。

由式(1)可知,DCT 变换后多数系数的绝对值比较小,由于 DCT 反变换时舍入误差的原因,当为嵌入较多的隐藏信息而修改较多的系数时,这些绝对值小的系数不管采用加性、乘性或量化中的哪一种方法进行隐藏信息的嵌入,均很难保证隐藏信息的正确提取。因此,将秘密信息嵌入到自然图像的 DCT 域时,由于可用于嵌入的系数有限,导致变换域算法的隐藏信息量变得很少,一幅 $512 \times 512 \times 8$ 的灰度图像在满足视觉不可感知性要求时的嵌入容

量一般只有 1 000 bits 左右^[7],远远低于空间域的 LSB 算法的 262 144 (512×512) bits。要提高 DCT 变换域算法的信息隐藏量,对于一幅具体图像来说,如果能提升中、高频系数的能量值,就可相应引入更多的可用系数,进而增加信息的嵌入容量。

要提升中、高频系数的能量值,需要想办法改变载体图像的低频特性,有效的方法是对载体图像进行频谱均匀化处理。数字图像的频谱均匀化是指在保持图像总能量和信息量不损失的前提下,对其进行适当处理和变换,使频谱不再具有低通特性,而具有均匀谱特性。频谱均匀化可以使图像的能量散布到所有的频率上,从通信理论的角度来讲,如果把载体图像看作一个信道,那么频谱均匀化处理相当于展宽信道的带宽^[8],使得更多的信号可以通过信道传输,进而增加信道容量。

频谱均匀化过程可以通过对数字图像“预白化”滤波的方法实现,也可以通过像素伪随机排序方法实现。考虑到计算的复杂性和重构图像的精度,采用伪随机排序的方法更切合实际。在像素伪随机排序后的图像中,相邻像素彼此之间不具有任何相关性,图像具有均匀频谱特性,即大多数的变换系数基本相等。当然对一幅具体图像而言,经过伪随机排序的图像并非完全“白化”,其频谱也并非完全平坦,但其中高频系数的能量会有明显提高。图 1 所示的 512×512 的 Lena 图像,进行伪随机排序后如图 2 所示,进行伪随机排序前后图像的 DCT

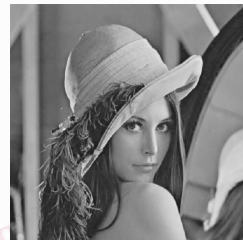


图 1 原始图像

Fig. 1 The original image

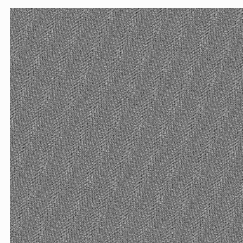
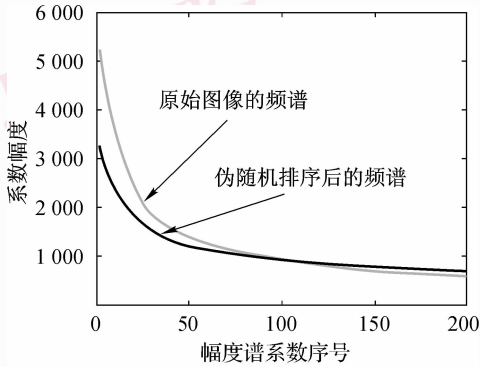


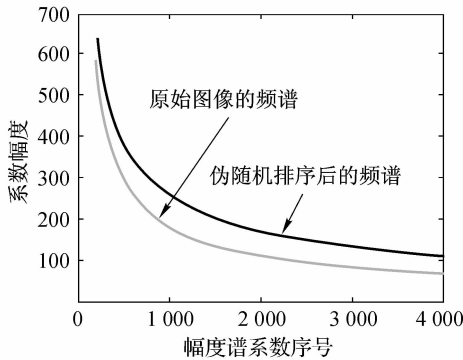
图 2 伪随机排序后图像

Fig. 2 The image after pseudo-random sort is used

系数的排序幅度谱的前 200 个系数对比如图 3(a) 所示(不包括直流系数),第 200 至第 4 000 个 DCT 系数的排序幅度谱对比如图 3(b) 所示。从图 3 可以看出图像经伪随机排序后,频谱特性有明显改变,图像在伪随机排序后的排序幅度谱前面 110 个系数的能量有所下降,但后面的系数的能量大幅度上升,可用来隐藏信息的系数数量有显著增长。



(a) 幅度谱前 200 个系数对比图



(b) 幅度谱第 200 至第 4 000 个系数对比图

图 3 图像的排序幅度谱

Fig. 3 Sort amplitude spectrum of image

3 大容量 DCT 域隐藏算法

基于 DCT 域的信息隐藏方法目前有多种,比较典型的有 Koch 等人最早提出的基于 DCT 变换域的信息隐藏方法^[9],其特点是对图像进行分块,再对每个分块进行 DCT 变换,并在变换域的中频系数上改变一个三元组以隐藏二进制序列信息。Cox 等人提出了基于图像全局 DCT 变换域的信息隐藏方法^[7],并明确提出水印应嵌入到图像信息感知重要的部分,达到提高水印鲁棒性的目的,同时可防止分块 DCT 变换域信息隐藏方法可能在视觉上出现的块状效应。可见要提高鲁棒性和不可感知性,采用全局 DCT 方法更好,虽然其计算量比分块 DCT 方

法要大些。但 Cox 等人在文献[7]中提出的 DCT 算法不能进行盲提取,而需要原始图像的参与,这只适合版权等水印的处理,而不适合于隐秘通信,同时容量也比较有限,使其应用场合受到很大限制。为实现信息的盲提取,本文算法采用对 DCT 系数双极性参数抖动调制进行量化的方法。采用量化的方法嵌入信息时,量化参数的选取很关键,参数过小则鲁棒性差,参数过大则不可感知性差。考虑到图像伪随机排序后 DCT 中、高频系数的能量虽有明显提升,但频谱并非完全平坦的特点,不同频率的系数采用不同的量化系数,从而在保证不可感知的前提下,增加可隐藏的信息量。设载体图像为 $I = \{f(x, y), x, y = 0, 1, \dots, N - 1\}$,待隐藏信息为 $W = \{w_j, j = 0, 1, \dots, L - 1\}$,DCT 变换域系数为 $S = \{s(u, v), u, v = 0, 1, \dots, N - 1\}$,隐藏信息后的图像为 $I^* = \{f^*(x, y), x, y = 0, 1, \dots, N - 1\}$,嵌入算法如下:

(1) 对图像 I 进行置乱得到伪随机排序后的图像 I' ;

(2) 对图像 I' 进行全局 DCT 变换得到 DCT 变换域系数矩阵 $S = \{s(u, v), u, v = 0, 1, \dots, N - 1\}$;

(3) 按 zig_zag 方法取出 S 中除 DC 系数外的前 L 个系数,并排列成 1 维数组 S_1 。

$$S_1 = \{s_1(i), i = 0, 1, \dots, L - 1\}$$

(4) 对 S_1 进行修改实现信息的嵌入,每个 DCT 系数采用双极性参数抖动调制量化方法隐藏 1 比特信息,得到 S_1^* 。考虑到 DCT 系数在低频段的幅度值互相之间相差较大的原因,不同位置的 DCT 系数采用不同的量化参数,其嵌入原则如下:

① 当待嵌入的信息 $w_i = 0$ 时,

$$s_1^*(i) = \text{sgn}(s_1(i)) \lfloor (|s_1(i)| + \Delta_i/2) / \Delta_i \rfloor \Delta_i;$$

② 当待嵌入的信息 $w_i = 1$ 时,

$$s_1^*(i) = \text{sgn}(s_1(i)) (\lfloor (|s_1(i)|) / \Delta_i \rfloor \Delta_i + \Delta_i/2);$$

(5) 用 S_1^* 来替换 S 中按 zig_zag 方法排列的除 DC 系数外的前 L 个系数,得到嵌入有隐藏信息的 DCT 系数矩阵 S^* 。

(6) 对 S^* 进行反 DCT 变换(IDCT)得到嵌入有秘密信息的图像 I'^* 。

(7) 对图像 I'^* 逆置乱得到含隐藏信息的图像 I^* 。

隐藏信息的提取算法如下:

(1) 对图像 I^* 进行置乱得到置乱后的图

像 I^* ;

(2) 对图像 I^* 进行全局 DCT 变换, 得到 DCT 变换域系数矩阵 $S^* = \{s^*(u, v), u, v = 0, 1, \dots, N-1\}$;

(3) 按 zig_zag 方法取出 S^* 的除 DC 系数外的前 L 个系数, 并按顺序排列成 1 维数组:

$$S_1^* = \{s_1^*(k), k = 0, 1, \dots, L-1\}.$$

(4) 根据 S_1^* 计算出 $H = \{h(i), i = 0, 1, \dots, L-1\}$, 其中

$$h(i) = |s_1^*(i)| - \lfloor |s_1^*(i)| / (\Delta_i/2) \rfloor (\Delta_i/2);$$

(5) 根据 H 各元素的值, 提取隐藏信息的各比特:

$$w(i) = \begin{cases} 0 & h(i) < \Delta_i/4 \\ 1 & h(i) \geq \Delta_i/4 \end{cases}$$

4 仿真实验

采用如图 1 所示的 512×512 的 Lena 图像作为载体, 分别隐藏如图 4(a) 所示的 $30 \times 30, 64 \times 64$ 秘密图像, 采用文献[7]算法进行实验, 提取的图像分别如图 4(b) 所示, 采用本文算法进行实验, 提取的图像分别如图 4(c) 所示, 隐藏信息后含密图像的 PSNR(峰值信噪比)如表 1 所示。

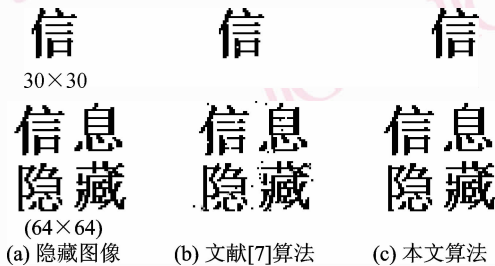


图 4 文献[7]算法与本文算法试验对比结果 1
Fig. 4 The first result of comparing Ref. [7] with our algorithm

表 1 隐藏信息后载密图像的 PSNR 值

Tab.1 PSNR after information hiding 单位: dB

隐藏图像大小	文献[7]算法	本文算法
30 × 30	35.56	45.35
64 × 64	35.09	42.31

再采用 256×256 的 Lena 图像作为载体, 采用文献[7]的算法隐藏如图 4(a) 所示的 30×30 秘密图像, 提取的图像如图 5(a) 所示, 采用本文算法隐藏如图 4(a) 所示的 64×64 秘密图像, 提取的图像

如图 5(b) 所示, 隐藏信息后含密图像的 PSNR 分别为 34.82 dB 和 36.75 dB。



(a) 文献[7]算法 (b) 本文算法

图 5 文献[7]算法与本文算法实验对比结果 2
Fig. 5 The second result of comparing Ref. [7] with our algorithm

由以上实验结果可知, 文献[7]在大小为 512×512 的载体图像上能准确提取嵌入信息的可嵌入容量约为 1 000 bits(这也是文献[7]所给出的结论), 当嵌入量达到 64×64 时, 即使没有加入任何干扰也不能准确提取嵌入的信息, 其主要原因是 DCT 反变换为图像时, 由实数变为整数时的误差累积造成的, 这是所有 DCT 域隐藏算法嵌入容量过大时都有可能碰到的问题; 本文算法在 512×512 和 256×256 的载体图像上嵌入 64×64 的信息均能准确提取, 可见本文算法的嵌入容量有明显提高, 同时由表 1 可知本文算法的不可感知性比文献[7]更佳。

5 结 论

DCT 域信息隐藏算法是目前变换域中应用最广的隐藏算法, 其主要不足之一是嵌入信息量小, 且分块 DCT 变换域隐藏算法可能在视觉上出现块状效应, 因此多数不适合于隐秘通信。本文分析了 DCT 变换域方法隐藏信息容量少的原因, 通过频谱均匀化处理, 获得更多的可用于隐藏信息的 DCT 系数, 从而大大提高算法的可嵌入容量。然后对图像进行全局 DCT 变换域, 并将隐藏信息嵌入到载体图像的低频 DCT 系数上, 由于信息是嵌入在感知重要的低频系数上, 有利于提高其鲁棒性, 同时由于是在全局 DCT 系数上嵌入信息, 因此可防止分块 DCT 域隐藏算法可能在视觉上出现的块状效应。实验结果表明, 本文算法的嵌入容量比同样是在全局 DCT 低频系数嵌入信息的文献[7]算法容量大很多, 且不可感知性更好。同时本文算法在提取隐藏信息时, 不需要原始图像及其他辅助信息, 是一种完全意义上的盲提取, 可应用于隐秘通信。

参考文献 (References)

- 1 Neil F J. Steganography Tools [EB/OL]. <http://www.jjtc.com/Security/stegtools.htm>, 2005-08-16/2008-01-08.
- 2 Zang T, Ping X J. Reliable detection of spatial LSB steganography based on difference histogram [J]. *Journal of Software*, 2004, **15**(1): 151-158. [张涛, 平西建. 基于差分直方图实现 LSB 信息伪装的可靠检测[J]. *软件学报*, 2004, **15**(1): 151-158.]
- 3 Shih F Y, Wu S Y T. Combinational image watermarking in the spatial and frequency domains [J]. *Pattern Recognition*, 2003, **36**(4): 969-975.
- 4 Munuera C. Steganography and error-correcting codes [J]. *Signal Processing*, 2007, **87**(6): 1528-1533.
- 5 Jain A K. *Fundamentals of Digital Image Processing* [M]. Upper Saddle River, NJ, USA: Prentice Hall, 1989.
- 6 Smoot S R, Rowe L A. Study of DCT coefficient distributions [A]. In: *Proceedings of the SPIE Symposium on Electronic Imaging* [C], San Jose, CA, USA, 1996: 403-411.
- 7 Cox I J, Kilian J, Leighton F T, *et al.* Secure spread spectrum watermarking for multimedia [J]. *IEEE Transactions on Image Processing*, 1997, **6**(12): 1673-1687.
- 8 Sun S H, Lu Z M, Niu X M, *et al.* *Techniques and Application of Digital Watermarking* [M]. Beijing: Science Press, 2004: 170-175. [孙圣和, 陆哲明, 牛夏牧等. *数字水印技术及应用* [M]. 北京: 科学出版社, 2004: 170-175.]
- 9 Koch E, Zhao J. Toward robust hidden image copyright labeling [A]. In: *Proceedings of IEEE Workshop on Nonlinear Signal and Image Processing* [C], Neos Marmaras, Greece, 1995: 452-455.