

基于 DCT 变换的图像伪装技术¹

夏光升 陈明奇 杨义先 胡正名

(北京邮电大学信息安全中心 126 信箱 北京 100876)

摘要 该文提出一种频域的信息伪装技术,该技术具有以下几个优点:(1)隐藏效果好,人眼系统不能发觉隐藏了秘密图像的载体图像与原载体图像之间的差别;(2)口令控制,只有知晓伪装口令的人才能解密;(3)可以有效地抵抗 JPEG 等图像压缩编码的破坏;(4)利用载体图像的部分内容可以恢复原秘密图像;(5)该算法可以用于数字水印,而且可以将水印图像由二值图像扩展到灰度图像;(6)算法可以进行多址伪装,即在同一幅载体图像中隐藏多幅秘密图像。

关键词 信息伪装,数字水印, DCT, DWT

中图分类号 TN911.73

1 引言

随着多媒体技术和计算机网络的飞速发展,数字产品的版权和信息安全问题日益倍受关注。数字水印技术和信息伪装技术正是适应这一要求发展起来的。前者是为了保护数字产品的版权,而要对数字产品加载所有者的水印信息,以便在产品的版权产生纠纷时作为证据,而后者是指把不便于公开的信息,通过伪装算法加载到可以公开的信息载体中去,在信息的接收端利用解伪装算法,恢复出被伪装的信息。前者是为了保护载体数字产品的版权问题,而后者则是为了被伪装信息的安全与保密。二者似乎没有本质的差别,而只不过是使用的目的不同而已。但是,从技术要求来看,二者又有很大的差别,一般的,数字水印的技术要求较高,要求所加载的水印不仅要具有安全性,还要具有很强的稳健性。而后者则更加偏重于安全与保密性。

目前,数字水印技术已经成为人们研究的重点,已经出笼的水印算法很多,基本上可以分为空间域、频域变换域等几种。但是对信息伪装技术的研究较少。数字水印技术可以用于信息伪装,但所伪装的信息较少,伪装之后的冗余太大,因而有必要专门研究信息伪装技术,以供保护信息的安全和保密使用。

2 研究现状

自从信息伪装和数字水印的概念提出以来,信息伪装技术和数字水印技术都得到了迅速发展。但用于保密通信的信息伪装技术远没有数字水印技术发展得迅速。由于图像在信息的表达中扮演了重要的角色,人们也将会越来越多地使用图像。因此,如何保证图像信息的安全已成为人们关注的重要问题。

近年来,人们已提出了几种保护图像信息的密码系统^[1,2]。它们都是将要保密的图像加密变成一幅经过编码的密图(Cipher image)。如果密图在传送过程中被非法拦截,当拦截者试图查看密图内容时,他只能看到一幅由一堆乱码所构成的毫无意义的图像。但另一方面,这也容易引起拦截者的怀疑,从而激发起拦截者的破解密图信息的兴趣。为了弥补这个缺点,人们开始研究基于信息伪装的保护图像信息的方法,其基本思想是经过编码的密图仍是有意义的,因此不易引起拦截者的注意,从而大大减少了遭受拦截者试图破译的可能。这方面的工作见文献[3,4],图像经过伪装后,多了一层保护,仿佛是自然界中生物的保护色,增加了图像的保密性和安全性。

¹ 2000-03-20 收到, 2000-07-19 定稿

国家自然科学基金资助项目(批准号 69882002, 60073049), 国家“973”项目(G1999035805), 高等学校骨干教师资助项目, 国家杰出青年基金资助项目(69425001)

本文提出了一种频域的信息伪装技术, 该技术隐藏效果好, 人眼系统不能发觉隐藏了秘密图像的载体图像与原载体图像之间的差别; 隐藏的内容是安全的; 可以有效地抵抗 JPEG 等图像压缩编码的破坏, 稳健性很好. 此外, 该算法还可以用于数字水印, 而且可以将水印图像由二值图像扩展到灰度图像; 可以在同一幅载体图像中隐藏多幅秘密图像.

3 信息伪装算法

3.1 信息隐藏

设 CI 是 $M \times N$ 大小的载体图像, SI 为想要隐藏的 $P \times Q$ 大小的秘密图像, $P = M/2$, $Q = N/2$. 通过本算法, 我们要把图像 SI 隐藏到图像 CI 中. 算法分以下几步进行:

(1) 压缩 为了将秘密图像 SI 隐藏到载体图像 CI 中, 首先利用二维小波变换对 SI 进行变换, 为了达到图像压缩的最大效果, 我们只保留下式中的低频部分 SI_{LL} . $[SI_{LL}, SI_{HL}, SI_{LH}, SI_{HH}] = DWT(SI)$.

(2) 随机置换 由事先选定的口令 K 控制生成两个分别从 1 到 $P/2$ 和从 1 到 $Q/2$ 的随机置换 RP_{row} 和 RP_{col} , 并按照下式对 SI_{LL} 进行变换: $SI'_{LL}(i, j) = SI_{LL}(RP_{row}(i), RP_{col}(j))$.

(3) 分块 将 CI 分解为 $(M/8) \times (N/8)$ 个 8×8 大小的方块 $BCI_{m,n}$; 同时, 将 SI'_{LL} 也分解为 $(M/8) \times (N/8)$ 个 2×2 大小的方块 $BSI'_{LL}{}^{m,n}$, $1 \leq m \leq M/8, 1 \leq n \leq N/8$.

(4) DCT 变换 对每一个 $BCI_{m,n}$, 进行 DCT 变换: $DBCI'_{m,n} = DCT(BCI_{m,n})$.

(5) 数据隐藏 对每一个 $DBCI'_{m,n}$ 和 $BSI'_{LL}{}^{m,n}$, 按照下式将 $DBCI'_{m,n}(s_i)$ 用 $BSI'_{LL}{}^{m,n}(t_i)$ 来代替, s_i 和 t_i 如图 1 所示. $DBCI''_{m,n}(s_i) = \alpha \times BSI'_{LL}{}^{m,n}(t_i)$.

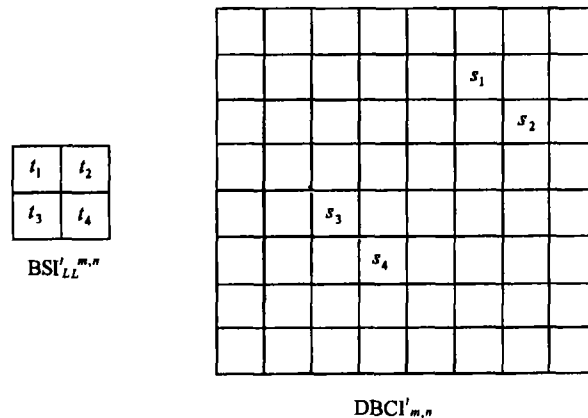


图 1 修改系数区域

(6) 逆 DCT 变换 对以上得到的每一个 $DBCI''_{m,n}$ 进行逆 DCT 变换: $IDBCI_{m,n} = IDCT(DBCI''_{m,n})$. 并将各方块 $IDBCI_{m,n}$ 合并为一个整图 CI' , 即为隐藏有秘密图像的新图像.

以上提到的系数 α 将对隐藏后的载体图像 CI 的质量以及由其恢复的新秘密图像的质量产生重大的影响, α 越大, 恢复的新秘密图像的质量越好; 相反, α 越小, 图像 CI 的质量越好. 一般的, 可以将 α 的值取为 0.01~0.1 之间.

同时, 由于以上算法中采用的是变换域的方法, 改变的是 DCT 系数, 可以抵抗 JPEG 等压缩编码的破坏. 由于在图像隐藏之前首先用小波压缩技术对秘密图像进行了压缩, 因而可以隐藏更多的信息.

3.2 信息提取

设图像 TCI 为已经隐藏了秘密图像的载体图像。现要根据使用者输入的口令，将所隐藏的秘密图像从 TCI 中提取出来。其过程为上述隐藏算法的逆运算：

(1) DCT 变换 将 TCI 分解为 $(M/8) \times (N/8)$ 个 8×8 大小的方块 $BTCI_{m,n}$ ，并对每一个 $BTCI_{m,n}$ 进行二维 DCT 变换： $BTCI'_{m,n} = DCT(BTCI_{m,n})$ 。

(2) 提取数据 对每一个 $BTCI'_{m,n}$ ，按照下式得到 $BWSI_{LL}^{m,n}$ ： $BWSI_{LL}^{m,n}(s_i) = (1/\alpha) \times BTCI'_{m,n}(t_i)$ ， s_i 和 t_i 如图 1 所示。

(3) 逆随机变换 将上面得到的所有 $BWSI_{LL}^{m,n}$ 合并为一个整图 $NWSI_{LL}$ 。

根据给定的口令 K 控制生成两个分别从 1 到 $M/4$ 和从 1 到 $N/4$ 的随机置换 RP_{row} 和 RP_{col} ，并按照下式对 SI_{LL} 进行变换： $NWSI_{LL}(RP_{row}(i), RP_{col}(j)) = WSI_{LL}(i, j)$ 。

(4) 逆 DWT 变换 对 $NWSI_{LL}$ 进行二维逆小波变换： $NSI = IDWT(NWSI_{LL}, 0_{HL}, 0_{LH}, 0_{HH})$ ，其中 $0_{HL}, 0_{LH}, 0_{HH}$ 皆为与 $NWSI_{LL}$ 同样大小的 0 矩阵。

4 多址伪装

利用 3 节中的算法，可以实现多址图像伪装。所谓多址图像伪装，是指将两个或两个以上的图像，隐藏到载体图像的不同位置。3 节中的算法在每一个 8×8 的方块中只有四个 DCT 系数上隐藏了数值，在中频部分尚有许多位置可以隐藏信息（秘密图像或数字水印）。实现时可以选择其他位置和 α 的值，实现多址伪装。但应注意，由于算法中利用新的数值完全代替了选中的 DCT 系数的值，所以要隐藏的信息不宜过多。

5 实验结果

本文对以上算法进行实验。使用 Lena 图像（见图 2）作为载体图像，Airplane 图像（见图 3）作为秘密图像。系数 $\alpha = 0.05$ 。隐藏了 Airplane 的 Lena 图像见图 4，恢复的 Airplane 图像见图 5，采用峰值信噪比作为图像性能的度量，其峰值信噪比分别为 42.58dB 和 26.91dB。

实验中我们对图 4 中的图像进行了破坏，只保留了部分图像内容（参见图 6），由其恢复的 Airplane 的新图像为图 7 所示，其峰值信噪比为 14.02dB，虽然效果比较差，但仍然可以看清楚。

图 9 是将图 3 和图 8 中的图像隐藏到图 2 中的 Lena 图像后的结果，其峰值信噪比为 40.4dB。图 10 和图 11 是从图 9 恢复的两个秘密图像，其峰值信噪比分别为 26.31dB 和 23.89dB。



图 2

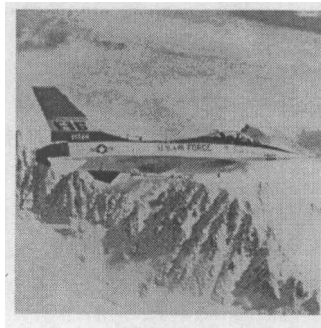


图 3



图 4



图 5

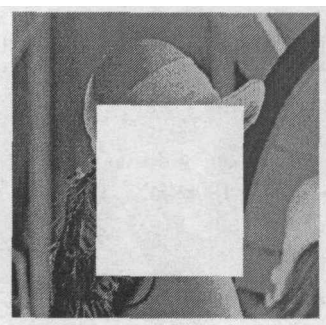


图 6

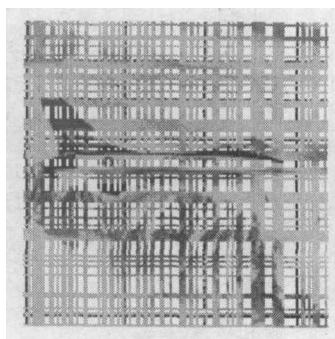


图 7

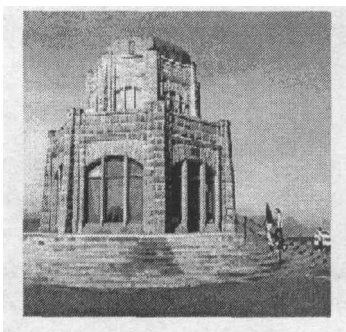


图 8



图 9

6 结 论

本文借助 DCT 变换和小波变换, 提出了一种图像伪装技术, 主要应用于保密通信等领域, 也可以用于数字水印, 来实现数字产品的版权保护。由于本算法可以将一幅或几幅图像隐藏于同一图像中, 因而也可以考虑到用于图像压缩领域。

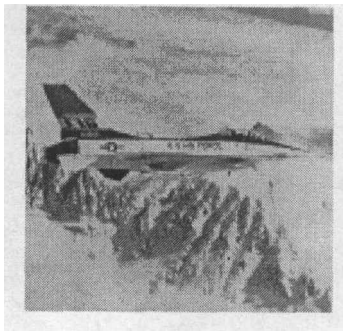


图 10

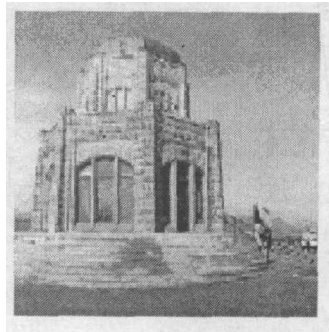


图 11

参 考 文 献

- [1] C. J. Kuo, Novel image encryption technique and its application in progress transmission, *Journal of Electronic Imaging*, 1993, 2(4), 345-351.
- [2] S. Schwartz, A new graphical method for encryption of computer data, *Cryptologia*, 1991, 15(1), 43-46.
- [3] Tung-Shou Chen, Chin-Chen Chang, Min-Shiang Hwang, A virtual image cryptosystem based upon vector quantization, *IEEE Trans. on Image Processing*, 1998, IP-7(10), 1485-1488.
- [4] 丁玮, 齐东旭, 数字图像变换及信息隐藏与伪装技术, *计算机学报*, 1998, 21(9), 838-843.

DCT-BASED IMAGE HIDING ALGORITHM

Xia Guangsheng Chen Mingqi Yang Yixian Hu Zhengming

(*Information Centre, Beijing Univ. of Posts and Telecommunications, Beijing 100876, China*)

Abstract A new DCT-based information hiding algorithm is presented in this paper. The excellent features of the new method are: (1) the difference between the carrier image containing the secret and the original one is perceptually invisible; (2) the embedded secret image can be retrieved only by using a secret key; (3) it is robust against JPEG encode; (4) the embedded secret image can be extracted from part of carrier image containing the secret; (5) the method can be used to embed watermark into images, and the watermark may be an image ranged from 2 color to 256 or more color; (6) more than one secret image can be hide into a single carrier image.

Key words Information hiding, Digital watermark, DCT, DWT

夏光升: 男, 1973 年生, 博士生, 研究兴趣涉及信号处理、信息伪装、数字水印、密码学、网络安全等领域。
 陈明奇: 男, 1973 年生, 博士生, 研究领域包括信号处理、信息安全、计算机安全等。
 杨义先: 男, 1961 年生, 教授, 博士生导师, 研究兴趣甚广, 涉及编码理论、密码学、信息安全、网络安全、通信原理、信号处理、图像处理、离散数学等领域。目前已在国内外刊物上发表论文 400 余篇, 出版十余部专著。
 胡正名: 男, 教授, 博士生导师, 研究方向涉及编码理论、密码学、信号处理、应用数学等领域。