基于融合的数据隐藏算法

柳葆芳[1], 平西建[1], 邓宇虹[2]
(1. 郑州信息工程大学, 河南郑州 450002; 2. 北京市 2651 信箱, 北京 100084)

摘 要: 本文在讨论基于融合的数字图像隐藏技术算法的基础上, 提出了一种基于融合的数据隐藏算法. 该算法利用一次 Bézier 曲线, 将秘密数据隐藏在原始图像中. 该算法可以在数字图像中嵌入任意形式的数字化数据, 在选取适当的参数时, 可以完全正确地恢复出数字化数据. 该算法的特点是数据隐藏能力强, 在以灰度图像为原始图像的情况下, 其最大隐藏能力可以达到 3bits/ pixel.

关键词: 信息隐藏; 数据隐藏; 融合
中图分类号: TP919 文献标识码: A 文章编号: 0372-2112 (2001) 11-1445-04

Data Hiding Algorithm Based on Harmonic Amalgamation

LIU Bao-fang[1], PING Xi-jian[1], DENG Yu-hong[2]
(1. *Dept. of Info. Sci., University of Information Engineering, Zhengzhou, Henan* 450002, *China*; 2. *P. O. Box* 2651, *Beijing* 100084, *China*)

Abstract: A novel approach to embedding digital data into a cover image using simple Bézier curve is proposed on the base of harmonic amalgamation algorithm whose purpose is to hide digital images. A message embedded by this approach can be in the form of text, imagery, or any other digital signal. The data to be embedded is treated as a binary stream and is partitioned into a number of sub-streams. Each sub-stream of data is converted into values that are then embedded into the public original image. Given appropriate parameters, it could be proved that digital data embedded by this approach could all be recovered correctly by data recovering process with the knowledge of original image. The advantage of this approach is high efficiency of data hiding. Its maximal efficiency of data hiding could come up to 3 bits/ pixel when using gray images as public original images. Experimental results show that the proposed approach is feasible.

Key words: information hiding; data hiding; harmonic amalgamation

1 引言

在当今的数字化和信息化社会中, 飞速发展的信息处理技术和通信手段, 使得关系国家安全、经济发展乃至个人隐私等方面的信息安全更加突出, 一种新的信息安全技术——信息隐藏技术应运而生, 成为信息技术研究的热点之一. 信息隐藏技术是指将特定信息隐藏在数字化宿主信息(如文本、数字化的声音、图像等) 中的方法[1,2]. 信息隐藏技术的主要应用除了信息的保密传输外, 还可以用在版权保护和信息确认上. 根据处理方法和应用领域的不同, 信息隐藏主要可以分为数字水印技术[3] 和数据隐藏技术[4] 两大类.

数据隐藏的技术方法主要有空间域算法[5,6] 和变换域算法[7~9]. 基于融合的数字图像隐藏算法就是一种空间域算法[10], 该算法利用一次 Bézier 曲线, 将秘密图像隐藏在同样大小的原始图像中. 这种算法具有计算简单, 易实现, 恢复的秘密图像质量好的特点. 但是这种算法只能嵌入图像数据, 而不能对其他数据进行操作. 本文在基于融合的数字图像隐藏算法的基础上, 提出了一种基于融合的数据隐藏算法, 该算法可以在数字图像中嵌入任意形式的二值流文件, 在选取适当的参数时, 可以完全正确地恢复出二值流文件. 该算法的特点是数据隐藏能力强, 在以灰度图像为原始图像的情况下, 其最大隐藏能力可以达到 3bits/ pixel.

2 基于融合的数字图像隐藏技术

在计算机图形学与计算辅助设计中经常使用的一种调配函数方法[11,12]. 假设在空间给定 $n+1$ 个点 $P_0, P_1, \cdots, P_n$, 则称如下参数曲线为以 $\{P_i,\ i=0, 1, \cdots, n\}$ 为控制点的 n 次 Bézier 曲线:

$$P(t)=\sum_{i=0}^{n} P_i B_i^n(t) \tag{1}$$

其中 $B_i^n(t)$ 为 Berntein 基函数:

$$B_i^n(t)=\binom{n}{i}(1-t)^{n-i}t^i \tag{2}$$

一般称折线 $P_0P_1\cdots P_n$ 为 $P(t)$ 的控制多边形, 点 $P_0, P_1, \cdots, P_n$ 为 $P(t)$ 的控制顶点.

下面以 1 次 Bézier 曲线为例, 讨论 2 幅数字图像的融合.

收稿日期: 2000-11-20; 修回日期: 2001-03-10

由式(1)、(2), 有

$$P(t)=(1-t)P_0+tP_1 \tag{3}$$

这是一个简单的线性插值公式.

对于原始图像 F_0 和 F_1, 设其尺寸同为 $M\times N$, 即有 $F_0=\{f_{ij}^0, 0\le f_{ij}^0\le 255, 0\le i< M, 0\le j< N\}$ 和 $F_1=\{f_{ij}^1, 0\le f_{ij}^1\le 255, 0\le i< M, 0\le j< N\}$. 对 F_0 和 F_1 中相同位置的每对像素 f_{ij}^0 和 f_{ij}^1, 应用公式(3), 有

$$f_{ij}^2=\lfloor(1-t)f_{ij}^0+tf_{ij}^1\rfloor,\quad 0\le i< M, 0\le j< N \tag{4}$$

得到融合图像 $F_2=\{f_{ij}^2, 0\le f_{ij}^2\le 255, 0\le i< M, 0\le j< N\}$, 其中 $\lfloor x\rfloor$ 表示取小于等于 x 的最大整数. 以 Lena 图为 F_0, 以 Peppers 图为 F_1, t 取不同值时得到的融合图像见图 1.

通过公式(5)、(6), 可以从融合图像中恢复原始图像和秘密图像:

$$tf_{ij}^0=\left\lfloor\frac{f_{ij}^2-tf_{ij}^1}{1-t}\right\rfloor, 0\le i< M, 0\le j< N \tag{5}$$

$$tf_{ij}^1=\left\lfloor\frac{f_{ij}^2-(1-t)f_{ij}^0}{1-t}\right\rfloor, 0\le i< M, 0\le j< N \tag{6}$$

将式(6)应用于图 1(c), 得到的恢复图像见图 2.

图 1 两个图像按一次 Bézier 曲线的融合

3 基于融合的数据隐藏技术

3.1 构造秘密图像

图 2 由融合图像图 1(c)得到的恢复图像, PSNR= 38.90

该算法可以嵌入任何形式的数据文件. 数据文件以比特流的形式输入. 定义串长 L, 将比特流分解成长为 L 的子串, 按照从上到下, 从左到右的顺序, 将子串排列成大小为 $M\times N$ 的矩阵

$$\boldsymbol{S}_{M\times N}=\begin{bmatrix} s_{11}, s_{12}, \cdots, s_{1N} \\ \cdots \\ s_{M1}, s_{M2}, \cdots, s_{MN}\end{bmatrix}$$

, 其中, s_{ij} 为长为 L 的比特子串. 注意: 此处限定比特流的总长度不大于 $M\times N\times L$, 不足的补"0"处理.

令大小为 $M\times N$ 矩阵 $\boldsymbol{T}_{M\times N}$ 中的元素 t_{ij} 等于矩阵 $\boldsymbol{S}_{M\times N}$ 中相应位置的比特子串十进制数值, 即 $\boldsymbol{T}_{M\times N}=\begin{bmatrix} t_{11}, t_{12}, \cdots, t_{1N} \\ \cdots \\ t_{M1}, t_{M2}, \cdots, t_{MN}\end{bmatrix}$, 其中 $(ts_{ij})_{10}=(s_{ij})_2$. 此时矩阵 $\boldsymbol{T}_{M\times N}$ 的元素的取值范围为 $[0, 2^L-1]$. 为了使所构造的秘密图像 F_1 的像素值在 $[0, 255]$ 之间, 令 $tf_{ij}^1=t_{ij}\times 2^{8-L}$, 此时秘密图像 F_1 的像素值 tf_{ij}^1 的取值为 $\{tf_{ij}^1 | tf_{ij}^1=i\times 2^{8-L}, i\in[0, 2^L-1]\}$.

3.2 利用数据融合嵌入数据

利用 2 中基于融合的数字图像隐藏技术的思想来嵌入数据. 对于原始图像 F_0 和 F_1, 设其尺寸同为 $M\times N$, 即有 $F_0=\{f_{ij}^0, 0\le f_{ij}^0\le 255, 0\le i< M, 0\le j< N\}$ 和 $F_1=\{f_{ij}^1, 0\le f_{ij}^1\le 255, 0\le i< M, 0\le j< N\}$. 为了减小数据嵌入和恢复所引入的误差, 对式(4)进行修改, 对 F_0 和 F_1 中相同位置的每对像素 f_{ij}^0 和 f_{ij}^1,

$$f_{ij}^2=\mathrm{round}(f_{ij}^0\times(1-t))+\mathrm{round}(f_{ij}^1\times t) \tag{7}$$

应用公式(7)得到融合图像 $F_2=\{f_{ij}^2, 0\le f_{ij}^2\le 255, 0\le i< M, 0\le j< N\}$, 其中 round(x)表示取距离 x 最近的整数.

3.3 数据恢复

从融合图像中恢复秘密信息的过程是嵌入数据的逆过程. 首先从融合图像中恢复出秘密图像, 其方法如下:

$$tf_{ij}^1=\mathrm{round}((f_{ij}^2-\mathrm{round}((1-t)\times f_{ij}^0))/t) \tag{8}$$

得到秘密图像 $rF_1=\{tf_{ij}^1, 0\le tf_{ij}^1\le 255, 0\le i\le M, 0\le j\le N\}$.

从秘密图像中提取秘密信息以前, 必须对秘密图像中误差进行修正, 其过程如下:

$$tf_{ij}^{1'}=\begin{cases} tf_{ij}^1, & \text{if } tf_{ij}^1 \bmod 2^{8-L}\leqslant 2^{8-L-1}-1 \\ tf_{ij}^1+2^{8-L-1}-1, & \text{otherwise}\end{cases} \tag{9}$$

修正的像素值 $tf_{ij}^{1'}$ 取值范围仍为 $[0, 255]$, 这可从后面的误差分析中得到证明. 最后从修正的像素值 $tf_{ij}^{1'}$ 中提取其高 L 位比特得到 rs_{ij}:

$$(rs_{ij})_2=(rt_{ij})_{10}=\lfloor tf_{ij}^{1'}/2^{8-L}\rfloor \tag{10}$$

然后按照构造秘密图像的逆过程就可以得到所嵌入的比特流.

4 误差分析

秘密图像的嵌入和恢复过程所引入的误差为:

$$\begin{aligned} e1&=tf_{ij}^1-f_{ij}^1=\mathrm{round}((f_{ij}^2-\mathrm{round}((1-t)\times f_{ij}^0))/t)-f_{ij}^1 \\ &=\mathrm{round}(\mathrm{round}(f_{ij}^1\times t)/t)-f_{ij}^1\end{aligned} \tag{11}$$

设取整数运算 $\mathrm{round}(f_{ij}^1\times t)$ 所引入的误差为 $e11$, 其范围为 $|e11|\le 0.5$, 则式(10)可写成:

$$\begin{aligned} e1&=\mathrm{round}((f_{ij}^1\times t+e11)/t)-f_{ij}^1=f_{ij}^1+\mathrm{round}(e11/t)-f_{ij}^1 \\ &=\mathrm{round}(e11/t)=e11/t+e12\end{aligned} \tag{12}$$

其中, $e12$ 为 $\mathrm{round}(x)$ 所引入的误差, 其范围为 $|e12|\le 0.5$. 则:

$$|e1|\le\frac{0.5}{t}+0.5 \tag{13}$$

下面要证明误差满足一定的条件时, 通过公式(8~10)可以正确恢复秘密数据.

定理 1: 当 $-0.5/t+0.5\le 2^{8-L-1}-1$ 时, $rs_{ij}=s_{ij}$.

证明: 只要证明 $0.5/t+0.5\le 2^{8-L-1}-1$ 时, $rt_{ij}=t_{ij}$ 即可. 由条件 $0.5/t+0.5\le 2^{8-L-1}-1$ 和式(13), 有 $|e1|\le 2^{8-L-1}-1$, 即 $|tf_{ij}^1-f_{ij}^1|\le 2^{8-L-1}-1$. 若 $0\le e1\le 2^{8-L-1}-1$, 则 $tf_{ij}^1 \bmod 2^{8-L}=(f_{ij}^1+e1) \bmod 2^{8-L}=e1 \bmod 2^{8-L}=e1$, 即 $0\le tf_{ij}^1 \bmod$

$2^{8-L} \le 2^{8-L-1} - 1$. 由式(9), $0 \le f'^{1}_{ij} = f^{1}_{ij} \le 255$. 由式(10), 有:

$$(rs_{ij})_2 = (rt_{ij})_{10} = \lfloor f'^{1}_{ij} / 2^{8-L} \rfloor = \lfloor f^{1}_{ij} / 2^{8-L} \rfloor = \lfloor (f^{1}_{ij} + e1) / 2^{8-L} \rfloor$$
$$= f^{1}_{ij} / 2^{8-L} = (t_{ij})_{10} = (s_{ij})_2 \quad (14)$$

若 $-(2^{8-L-1} - 1) \le e1 < 0$, 则 $f'^{1}_{ij} \bmod 2^{8-L} = (f^{1}_{ij} + e1) \bmod 2^{8-L} = e1 \bmod 2^{8-L} = 2^{8-L} + e1$, 即 $2^{8-L-1} + 1 \le f'^{1}_{ij} \bmod 2^{8-L} < 2^{8-L}$. 由式(9), $0 \le f'^{1}_{ij} = f^{1}_{ij} + 2^{8-L-1} = f^{1}_{ij} + e1 + 2^{8-L-1} \le 255$. 由式(10), 有:

$$(rs_{ij})_2 = (rt_{ij})_{10} = \lfloor f'^{1}_{ij} / 2^{8-L} \rfloor = \lfloor (f^{1}_{ij} + 2^{8-L-1}) / 2^{8-L} \rfloor$$
$$= \lfloor (f^{1}_{ij} + e1 + 2^{8-L-1}) / 2^{8-L} \rfloor$$
$$= f^{1}_{ij} / 2^{8-L} + \lfloor (e1 + 2^{8-L-1}) / 2^{8-L} \rfloor \quad (15)$$

因为 $-(2^{8-L-1} - 1) \le e1 < 0$, 所以 $1 \le e1 + 2^{8-L-1} < 2^{8-L-1}$, 则式(15)可写成:

$$(rs_{ij})_2 = (rt_{ij})_{10} = f^{1}_{ij} / 2^{8-L} = (t_{ij})_{10} = (s_{ij})_2 \quad (16)$$

证明完毕.

5　参数取值

对于原始图像, 由式(7)知其峰值信噪比 *PSNR* 为:

$$PSNR = 10\lg\left[\frac{M \times N \times 255}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(f^{2}_{ij} - f^{0}_{ij})^2}\right]$$
$$\approx 10\lg\left[\frac{M \times N \times 255}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(t(f^{0}_{ij} - f^{1}_{ij}))^2}\right] \ge 20\lg\left[\frac{1}{t}\right] \quad (17)$$

根据 *PSNR* 的经验值要求, 应有:　　$20\lg[1/t] \ge 28$　　(18)

由式(18), 得到:　　$t \le 0.03981$　　(19)

因为只有当满足 $0.5/t + 0.5 \le 2^{8-L-1} - 1$ 时, 才能正确恢复秘密信息. 由条件 $0.5/t + 0.5 \le 2^{8-L-1} - 1$ 和式(19), 可以求出串长 L 的取值范围:

$$L \le 3.1926 \quad (20)$$

又因为 L 为比特子串的长度, 只能取正整数, 所以 L 的取值为[1, 2, 3]. 表 1 中给出了 L 取不同值时, t 的取值范围以及以 8bits/ pixel 灰度图像作为原始图像时的最大隐藏能力.

表 1　取不同值时, t 的取值范围和最大嵌入能力

	$L=1$	$L=2$	$L=3$
t 的取值范围	(0.008, 0.03981]	(0.01639, 0.03981]	(0.03448, 0.03981]
最大隐藏能力	1 bit/ pixel	2 bits/ pixel	3 bits/ pixel

6　实验结果

以大小为 256× 256 的 Lena, peppers, mandrill 图像作为原始图像, 取串长 $L=3$, 则它们最大隐藏字节数为 256× 256× 3/8= 24576. 实验中所要隐藏的数据是长度为 23872 字节的 montage.png 文件(见图 3). 当然, 所隐藏的数据可以是任意形式的二值流文件.

表 2　取不同值时, 原始图像的峰值信噪比

t	0.035	0.036	0.037	0.038	0.039
Lena	37.76	37.61	37.55	37.09	37.06
Peppers	37.39	37.24	37.18	36.75	36.66
Mandrill	38.10	37.95	37.93	37.47	37.35

表 2 中给出了 t 取不同值时, 原始图像的峰值信噪比. 图 4~ 6 给出了 t 取不同值时的融合图像. 而且 t 取表 2 中的值时, 可以完全正确地恢复所隐藏的数据文件.

图 3　所隐藏的 montage.png 文件

图 4　t 取不同值时的融合图像

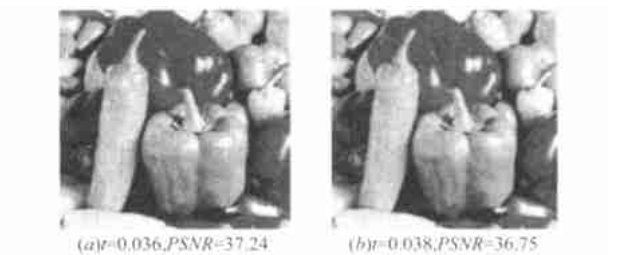

图 5　t 取不同值时的融合图像

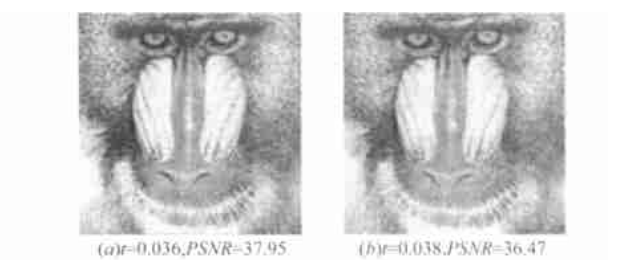

图 6　t 取不同值时的融合图像

7　结论

本文在讨论基于融合的数字图像隐藏技术算法的基础上, 提出了一种基于融合的数据隐藏算法. 该算法利用一次 Bézier 曲线, 将秘密数据隐藏在原始图像中. 该算法可以在数字图像中嵌入任意形式的数字化数据. 在选取适当的参数时, 可以完全正确地恢复出数字化数据. 该算法的特点是数据隐藏能力强, 在以灰度图像为原始图像的情况下, 其最大隐藏能力可以达到 3bits/ pixel. 该算法是在空间域上直接修改像素的灰度值来表达保密数据的信息, 这样, 对于一些引起像素灰度值扰动的图像处理过程来说, 该方法的鲁棒性就显的很弱. 同时该算法在恢复数据时需要原始图像, 所以该算法的主要应用是秘密数据的隐藏.

参考文献:

[1] W Bender, D Gruhl, N Morinoto, A Lu. Technique for Data Hiding [J]. IBM Systems Journal, 1996, 35(3&4): 313- 335.

[2] Fabien A P Petitcolas, Ross J Anderson, Markus G Kuhn. Information hiding-a survey[J]. Proc. of IEEE, 1999, 87(7): 1062- 1078.

[3] N Nikolaidis, I Pitas. Robust image watermarking in the spatial domain [J]. Signal Processing, 1998, 66(3): 385- 403.

[4] Mitchell D Swanson, Mei Kobayashi, Ahmed H Tewfik. Multimedia data embedding and watermarking technologies [J]. Proc. of the IEEE,

1998,86(6):1064- 1087.

[5] Neil F Johnson, Sushil Jajodia. Steganography: seeing the unseen [J]. Computer, 1998, 31(2): 26- 34.

[6] Dar Chun Wu, Werr Hsiang Tsai. Embedding of any type of data in images based on a human visual model and multiple-based number conversion [J]. Pattern Recognition Letters, 1999, 20(11): 1511- 1517.

[7] J J K Ruanaidh. T Pun. Rotation, scale and translation invariant digital image watermarking [A]. Proc. IEEE Int. Conf. Image Processing 1997 * ICIP97 [C], Santa Barbara, 1997: 536- 539.

[8] I Cox, J Kilian, T Leighton, T Shamoon. Secure spread spectrum watermarking for multimedia [J]. IEEE Trans. Image Processing, 1997, 6(12): 1673- 1687.

[9] W Zeng, Bede Liu. A statistical watermark detection technique without using original images for resolving rightful ownership of digital images [J]. IEEE Trans. On image Proceeding, 1999, 8(11): 1534- 1548.

[10] 丁玮. 数字图像信息安全的算法研究 [D]. 博士学位论文. 北京: 中国科学院, 2000.

[11] 孙家广, 杨长贵. 计算机图形学 [M]. 北京: 清华大学出版社, 1995.

[12] Donald Hearn, M Pauline Baker. Computer Graphics (C Version) [M]. 北京: 清华大学出版社, 1998.

作者简介:

柳葆芳 女. 1974 年 3 月生于山东莱州. 1999 年 3 月毕业于郑州信息工程学院, 获硕士学位, 现为郑州信息工程大学信息技术学院信息科学系博士研究生. 主要研究方向: 图象处理与分析, 图象压缩编码, 信息隐藏.

平西建 1982 年 12 月毕业于北京航空学院、获硕士学位, 现任郑州信息工程大学信息技术学院信息科学系教授, 博士生指导教师. 主要研究方向: 图象信源编码理论与方法、图象处理与识别、计算机视觉, 信息隐藏.

邓宇红 1973 年 11 月生于北京. 解放军 61886 部分软件工程师, 感兴趣的研究领域为图像处理与分析.