基于 RB 曲线融合的数字图像隐藏技术

张大奇[1] 张永红[1] 康宝生[2]
[1](西北大学数学系,西安 710069) [2](西北大学计算机科学系,西安 710069)

摘 要 基于融合的数字图像隐藏技术具有隐藏信息量大、方法简便等优点。为此,在已有方法的基础上,通过对信息融合实质的分析,运用数字图像"分存"的思想,提出了基于 RB(rational Bézier)曲线的多幅数字图像融合方法。该方法利用 n 次有理 Bézier 曲线、k 阶[n/n]型 RB 曲线、附权的[n/n]型 RB 曲线将一幅秘密图像隐藏于 n 幅公开图像中。该方法具有更多的融合因子,而且这些因子可以组合成更多的密钥,不仅能保证融合图像和恢复图像的质量,也增强了抵抗攻击的能力。该方法结合对图像的"置乱"处理,将更能增强整个隐藏系统的安全性。通过与其他方法的对比实例分析显示,采用该方法可得到更好的融合效果,方法简单易行,并有一定程度的鲁棒性。此外,该方法还可以推广到数字水印的研究与应用中。

关键词 数字图像信息隐藏 融合图像 分存 数字水印
中图法分类号: TP309 **文献标识码**: A **文章编号**: 1006-8961(2006)02-0235-09

Digital Image Information Hiding Technology Based on RB Curve Blending

ZHANG Da-qi[1], ZHANG Yong-hong[1], KANG Bao-sheng[2]
[1](*Department of Mathematics, Northwest University, Xi'an* 710069)
[2](*Department of Computer Science, Northwest University, Xi'an* 710069)

Abstract On the basis of digital image's information sharing, a new blending approach based on RB curve is presented. The approach makes use of a n-degree rational Bézier curve or a k-degree-[n/n] RB curve or a [n/n] RB curve with weights to hide information of one image into n images. These blending schemes have more blending parameters to act as the private keys, which can enhance the security and robustness of the hiding image. Furthermore, the schemes can be combined with the scrambling technology, which is usually used as pre-process and post-process of digital image information hiding. Experimental results show that these schemes can be realized expediently and have some degree of robustness. These blending schemes can also be used in the field of digital watermarking and other digital application.

Keywords digital image information hiding, blending image, image sharing, digital watermark

1 引 言

随着 Internet 的日益普及,数字化多媒体信息的交流已达到了前所未有的深度和广度。网上发布信息极为便利,但是作品侵权更加容易,篡改和非法复制也更加方便。因此信息的安全与保密显得越来越重要。信息隐藏技术作为防止盗版和篡改的有效工具,已在保密信息的网络传输、电子出版物的版权保护等领域得到广泛应用。根据处理方法和应用领域不同,信息隐藏技术分为水印技术和数据隐藏技术两大类。数字图像信息隐藏是近年信息隐藏技术中的热点,但是数字图像信息的隐藏与传统加密方法不尽相同,利用图像所具有的迷惑性产生的信息

基金项目:国家自然科学基金项目(60372072)
收稿日期:2004-12-17;**改回日期**:2005-06-10
第一作者简介:张大奇(1976 ~),男。硕士研究生。主要研究方向为计算机辅助几何设计、计算机图形学。E-mail:dqzhang2005@126.com

隐藏更能经得起恶意者的攻击。

数字图像隐藏算法主要有空间域算法和变换域算法。置乱和融合都是空间域算法。置乱变换能够有效地“打乱”秘密图像的轮廓信息，所以利用它对图像进行预处理(前处理和后处理)，可为更有效地利用融合方法打下基础。基于融合的数字图像隐藏算法，具有隐藏信息量大、计算简单、易实现、恢复图像质量好等特点。利用 Bernstein 多项式基函数对 $n+1$ 幅图像进行融合的方法[1]中，对某一个基函数 $B_n^i(u)=C_n^i u^i(1-u)^{n-i}$ 来讲，只有当融合参数 $u=i/n$ 时才达到局部最大。如果把这组基函数作为与融合图像相似的公开图像的权值，就会影响融合图像质量；基于迭代混合的数字图像隐藏技术[2]实质上是重复利用一次 Bézier 曲线融合两幅图像或在多幅图像之间多次利用一次 Bézier 曲线融合达到隐藏一幅秘密图像的目的，该方法需要多次设定融合参数、重复加密，不利于用户一次加密成功。为此，在以上算法的基础上，提出了基于 n 次有理 Bézier 曲线、k 阶 $[n/n]$ 型 RB 曲线、附权 $[n/n]$ 型 RB 曲线将一幅秘密图像隐藏于 n 幅公开图像中的融合算法。该算法非常便于交互式修改所使用的融合参数及权因子。由于该算法融合因子更多，因此更便于图像的隐藏且增加了抵抗攻击的能力，是一种能很好地实现秘密分割和秘密共享的图像信息隐藏技术。

2 原 理

信息隐藏技术的基本原理是利用信息中普遍存在的冗余性向其中嵌入秘密信息，从而达到隐蔽重要信息的目的。由于人类视觉系统(HVS)对图像的冗余信息不敏感，人眼感受到的两幅质量相似的图像像素灰度值可能存在较大的差别。比如，一幅灰度图像的 4 个最低有效位用另一幅灰度图像的 4 个最高有效位代替，肉眼通常无法分辨出它们的区别，因此可以利用信息融合的方法将一幅秘密图像隐藏在其他图像中。通过对文献[1]、[2]中的融合方法的研究不难发现，只要能选出具有非负性、归一性、交互性这 3 种性质的一组基函数，就可以这组基函数作为权值，将多幅数字图像融合为一幅图像，从而也将一幅秘密图像隐藏在其中。通过对图像信息隐藏原理和信息融合实质的分析，给出一般的基于融合的数字图像隐藏方法的定义。

定义 1 假设 $A_0(x),A_1(x),\cdots,A_n(x)$ 是定义在区间 $[0,1]$ 上的一组基函数，对任意的 $x\in[0,1]$

$$\sum_{i=0}^{n}A_i(x)\equiv 1,\quad A_i(x)\geqslant 0(i=0,1,\cdots,n)$$

$F_0,F_1,\cdots,F_n$ 是 $n+1$ 幅尺寸都为 $M\times N$ 的数字图像，其中，$F_j(0\leqslant j\leqslant n)$ 为秘密图像，$F_0,F_1,\cdots,F_{j-1},F_{j+1},\cdots,F_n$ 为公开图像，则称图像

$$S=Round\left(\sum_{i=0}^{n}A_i(x)F_i\right)$$

为公开图像 $F_0,F_1,\cdots,F_{j-1},F_{j+1},\cdots,F_n$ 和秘密图像 F_j 基于基函数 $A_0(x),A_1(x),\cdots,A_n(x)$ 的融合图像。其中，$Round()$ 表示上取整。称

$$F^*=Round\left(\frac{S\cdot\sum_{i=0}^{n}A_i(x)-\sum_{\substack{i=0\\i\neq j}}^{n}F_iA_i(x)}{A_j(x)}\right)$$

为恢复图像，x 称为融合参数，其中，$0\leqslant i,j\leqslant n$ 且 $i\neq j$。

3 两幅数字图像的融合

两幅图像融合可以利用加权平均的方法进行，因此直接选取基函数 $\{t,1-t\}$，$t\in[0,1]$。这两个基函数在计算机辅助几何设计中构成一次 Bézier 曲线的基函数[3]，一次 Bézier 曲线为

$$P(t)=(1-t)P_0+tP_1,t\in[0,1] \quad (1)$$

其中，P_0,P_1 为控制顶点，这是一个简单的线性插值。

定义 2 设 F 和 G 表示尺寸都为 $M\times N$ 的数字图像，F 是公开图像，G 是秘密图像，α 为满足 $0\leqslant\alpha\leqslant 1$ 的任一实数。利用式(1)，融合以后的图像 S 为

$$S=Round(\alpha F+(1-\alpha)G) \quad (2)$$

通过式(2)，恢复的秘密图像为

$$G^*=Round\left(\frac{S-\alpha F}{1-\alpha}\right)$$

则称 S 为关于 F 和 G 基于一次 Bézier 曲线的融合图像，G^* 为关于 F 和 G 基于一次 Bézier 曲线的恢复图像，其中 $\alpha(0\leqslant\alpha\leqslant 1)$ 称为融合参数。

基于一次 Bézier 曲线的图像融合方法提取秘密图像时解密密钥为融合图像 S、公开图像 F 及融合参数 α。两幅图像的加权平均法是一种最简单的图像融合方法，简单直观、适合实时处理。但是，将系统的安全性维系于一幅公开图像上是很危险的。此外，受融合图像和恢复图像客观保真度及相像程度的影响，融合参数的经验取值范围也很受限，所以需要建立多幅图像的融合算法。

图 1 是两幅图像融合与恢复的实验结果。

(a) 公开图像　(b) 秘密图像

(c) 公开图像　(d) 公开图像

图 1　两幅图像的融合与恢复($\alpha=0.6$)

Fig. 1　Blending and recovering of two images ($\alpha=0.6$)

4　$n+1$ 幅图像的融合

4.1　基于 n 次有理 Bézier 曲线的融合

n 次有理 Bézier 曲线为

$$P(t)=\frac{\sum_{i=0}^{n}\omega_i P_i B_i^n(t)}{\sum_{i=0}^{n}\omega_i B_i^n(t)},\quad t\in[0,1] \tag{3}$$

其中,$B_i^n(t)$ 为 n 次 Bernstein 基函数,$P_0,P_1,\cdots,P_n$ 为控制顶点,$\omega_0,\omega_1,\cdots,\omega_n$ 为权因子。

因为

$$\frac{B_i^n(t)\omega_i}{\sum_{i=0}^{n}B_i^n(t)\omega_i}\geqslant 0$$

$$\sum_{i=0}^{n}\left[\frac{B_i^n(t)\omega_i}{\sum_{i=0}^{n}B_i^n(t)\omega_i}\right]\equiv 1$$

所以可用这组基函数 $B_i^n(t)\omega_i\Big/\sum_{i=0}^{n}B_i^n(t)\omega_i(i=0,1,2,\cdots,n)$ 来融合 $n+1$ 幅图像。

定义 3　设秘密图像为 F_j,n 幅公开图像为 $F_0,F_1,\cdots,F_{j-1},F_{j+1},\cdots,F_n$,其尺寸均为 $M\times N$,α 为满足 $0\leqslant\alpha\leqslant 1$ 的任一实数,$\omega_0,\omega_1,\cdots,\omega_n$ 为一组权因子,$0\leqslant j\leqslant n$。由式(3),其融合图像为

$$S=Round\left(\frac{\sum_{i=0}^{n}\omega_i F_i B_i^n(\alpha)}{\sum_{i=0}^{n}\omega_i B_i^n(\alpha)}\right) \tag{4}$$

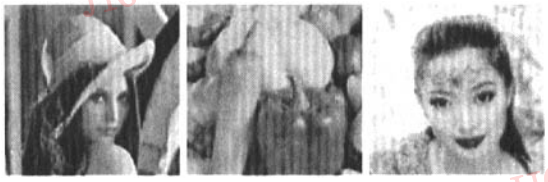
通过式(4),恢复的秘密图像 F^* 为

$$F^*=Round\left(\frac{S\cdot\sum_{i=0}^{n}\omega_i B_i^n(\alpha)-\sum_{\substack{i=0\\ i\neq j}}^{n}\omega_i F_i B_i^n(\alpha)}{\omega_j B_j^n(\alpha)}\right)$$

则称 S 为公开图像 $F_0,F_1,\cdots,F_{j-1},F_{j+1},\cdots,F_n$ 和秘密图像 F_j 基于 n 次有理 Bézier 曲线的融合图像,F^* 为 $F_0,F_1,\cdots,F_{j-1},F_{j+1},\cdots,F_n$ 和 F_j 基于 n 次有理 Bézier 曲线的恢复图像,其中,$\alpha(0\leqslant\alpha\leqslant 1)$ 称为融合参数,$\omega_0,\omega_1,\cdots,\omega_n$ 为融合权因子。

上述方法提取秘密图像时的解密密钥为融合图像 S、公开图像 $F_0,F_1,\cdots,F_{j-1},F_{j+1},\cdots,F_n$(包括其排列顺序)、融合参数 α 以及权因子 $\omega_0,\omega_1,\cdots,\omega_n$(包括其排列顺序)。该方法中权因子和融合参数非常有利于交互式地进行修改以达到较好的图像隐藏和恢复效果。应用基于 n 次有理 Bézier 曲线的融合方法时,可适当减小图像 $F_0,F_1,\cdots,F_{j-1},F_{j+1},\cdots,F_n$ 具有的基函数值,以便于增强图像隐藏和恢复的效果。此外,也可以将部分权因子作为公钥,部分权因子作为私钥,以实现密钥共享。

相应地实验结果如图 2 所示。



(a) 公开图像 1　(b) 公开图像 2　(c) 秘密图像

(d) 融合图像　(e) 恢复图像

图 2　多幅图像的融合与恢复

Fig. 2　Blending and recovering of many images ($\omega_1=8,\omega_2=1,\omega_3=3,\alpha=0.3$)

4.2　基于 k 阶[n/n]型 RB 曲线的融合

k 阶[n/n]型 RB 曲线为

$$P_n^{(k)}(t)=\sum_{i=0}^{n}P_i A_{RBn,i}^{(k)}(t)$$

$$=\frac{1}{(1+kt)^n}[C_n^0(1-t)^n,\cdots,C_n^i(1-t)^{n-i}t^i,\cdots,$$

$$C_n^n t^n] \cdot [(1+k)^0 P_0, \cdots, (1+k)^i P_i, \cdots, (1+k)^n P_n]^{\mathrm{T}} \tag{5}$$

其中，$t \in [0,1]$，

$$A_{\mathrm{RBn},i}^{(k)}(t) = \frac{(1+k)^i B_n^i(t)}{(1+kt)^n} = \frac{(1+k)^i C_n^i (1-t)^{n-i} t^i}{(1+kt)^n}$$

$P_0, P_1, \cdots, P_n$ 为控制顶点，k 为统一权因子。

因为

$$\frac{(1+k)^i C_n^i (1-t)^{n-i} t^i}{(1+kt)^n} \geqslant 0$$

$$\sum_{i=0}^{n} \frac{(1+k)^i C_n^i (1-t)^{n-i} t^i}{(1+kt)^n} \equiv 1$$

所以可用这组基函数 $A_{\mathrm{RBn},i}^{(k)}(t) \Big/ \sum_{i=0}^{n} A_{\mathrm{RBn},i}^{(k)}(t) (i = 0, 1, 2, \cdots, n)$ 来融合 $n+1$ 幅图像。

定义 4 设秘密图像 F_j 和 n 幅公开图像 $F_0, F_1, \cdots, F_{j-1}, F_{j+1}, \cdots, F_n$ 尺寸均为 $M \times N$，α 为满足 $0 \leqslant \alpha \leqslant 1$ 的任一实数，k 为一实数，$0 \leqslant j \leqslant n$。根据式(5)得到的融合图像是

$$S = Round\left(\sum_{i=0}^{n} A_{\mathrm{RBn},i}^{(k)}(\alpha) F_i \right) \tag{6}$$

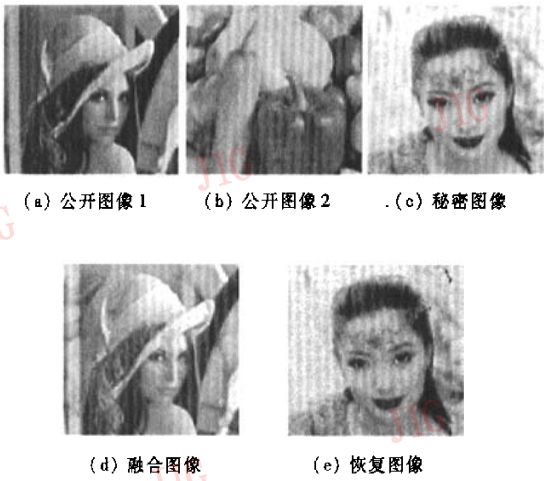
相应地，由式(6)恢复的秘密图像为

$$F^* = Round\left(\frac{S - \sum_{\substack{i=0 \\ i \neq j}}^{n} A_{\mathrm{RBn},i}^{(k)}(\alpha) F_i}{A_{\mathrm{RBn},j}^{(k)}(\alpha)} \right)$$

则称 S 为公开图像 $F_0, F_1, \cdots, F_{j-1}, F_{j+1}, \cdots, F_n$ 和秘密图像 F_j 基于 k 阶 $[n/n]$ 型 RB 曲线的融合图像，F^* 为 $F_0, F_1, \cdots, F_{j-1}, F_{j+1}, \cdots, F_n$ 和 F_j 基于 k 阶 $[n/n]$ 型 RB 曲线的恢复图像，其中 $\alpha (0 \leqslant \alpha \leqslant 1)$ 称为融合参数，k 为融合权因子。

上述方法提取秘密图像时的解密密钥为融合图像 S、公开图像 $F_0, F_1, \cdots, F_{j-1}, F_{j+1}, \cdots, F_n$（包括其排列顺序）、融合参数 α 及权因子 k。与基于 n 次有理 Bézier 的融合方法相比，基于 k 阶 $[n/n]$ 型 RB 曲线的融合方法中的权因子少。这就减少了权因子的选取时间，有利于快速恢复秘密图像，只需用参数 α 和 k 同时控制隐藏和恢复时的客观保真度和相像程度，因而算法更简单。当 $-1 < k < 0$ 时，图像序列中位于前面的图像对融合和恢复的图像客观保真度和相像程度影响较大；当 $k > 0$ 时，图像序列中位于后面的图像对融合和恢复的图像客观保真度和相像程度影响较大。利用统一的权因子固然好，但是也可能会使中间的公开图像对整个系统的安全性降低。

图 3 是基于 k 阶 $[n/n]$ 型 RB 曲线的多幅图像融合与恢复的实验结果。



(a) 公开图像 1　(b) 公开图像 2　(c) 秘密图像

(d) 融合图像　(e) 恢复图像

图 3 多幅图像的融合与恢复

Fig. 3 Blending and recovering of many images ($k = 0.9, \alpha = 0.1$)

4.3 基于附权 $[n/n]$ 型 RB 曲线的融合

附权 $[n/n]$ 型 RB 曲线为

$$P_n^k(t) = \frac{\sum_{i=0}^{n} (1+k)^i C_n^i (1-t)^{n-i} t^i \omega_i P_i}{\sum_{i=0}^{n} (1+k)^i C_n^i (1-t)^{n-i} t^i \omega_i} \quad t \in [0,1] \tag{7}$$

其中，$P_0, P_1, \cdots, P_n$ 为控制顶点，$\omega_0, \omega_1, \cdots, \omega_n$ 为权因子，k 为附加权因子。

因为

$$\frac{(1+k)^i C_n^i (1-t)^{n-i} t^i \omega_i}{\sum_{i=0}^{n} (1+k)^i C_n^i (1-t)^{n-i} t^i \omega_i} \geqslant 0$$

$$\sum_{i=0}^{n} \left(\frac{(1+k)^i C_n^i (1-t)^{n-i} t^i \omega_i}{\sum_{i=0}^{n} (1+k)^i C_n^i (1-t)^{n-i} t^i \omega_i} \right) \equiv 1$$

所以

$$\frac{(1+k)^i C_n^i (1-t)^{n-i} t^i \omega_i}{\sum_{i=0}^{n} (1+k)^i C_n^i (1-t)^{n-i} t^i \omega_i}, \quad i = 0, 1, 2, \cdots, n$$

可用作一组基函数来融合 $n+1$ 幅图像。

定义 5 设 $F_0, F_1, \cdots, F_n$ 为 $n+1$ 幅同样尺寸大小的图像，F_j 为秘密图像，$F_0, F_1, \cdots, F_{j-1}, F_{j+1}, \cdots, F_n$ 为公开图像，α 为满足 $0 \leqslant \alpha \leqslant 1$ 的任一实数，$\omega_0, \omega_1, \cdots, \omega_n$ 为一组权因子，k 为附加权因子，$0 \leqslant j \leqslant n$。利用式(7)得到的融合图像为

$$S = Round\left(\frac{\sum_{i=0}^{n}(1+k)^i C_n^i (1-\alpha)^{n-i}\alpha^i \omega_i F_i}{\sum_{i=0}^{n}(1+k)^i C_n^i (1-\alpha)^{n-i}\alpha^i \omega_i}\right) \quad (8)$$

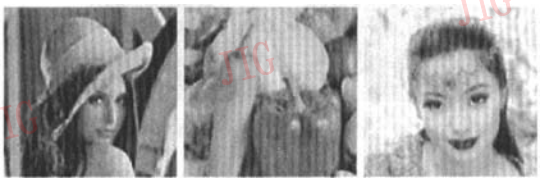
通过式(8),恢复图像为

$$F^* = Round\left(\frac{S\cdot\sum_{i=0}^{n}B_i^n(\alpha)(1+k)^i\omega_i - \sum_{\substack{i=0\\ i\neq j}}^{n}B_i^n(\alpha)F_i(1+k)^i\omega_i}{B_j^n(\alpha)(1+k)^j\omega_j}\right)$$

则称 S 为公开图像 $F_0,F_1,\cdots,F_{j-1},F_{j+1},\cdots,F_n$ 和秘密图像 F_j 基于 k 阶[n/n]型 RB 曲线的融合图像,F^* 为 $F_0,F_1,\cdots,F_{j-1},F_{j+1},\cdots,F_n$ 和 F_j 基于 k 阶[n/n]型 RB 曲线的恢复图像,其中 $\alpha(0\leqslant\alpha\leqslant1)$称为融合参数,$k$ 为融合附加权因子,$\omega_0,\omega_1,\cdots,\omega_n$ 为融合权因子。

上述方法提取秘密图像时的解密密钥为融合图像 S、公开图像 $F_0,F_1,\cdots,F_{j-1},F_{j+1},\cdots,F_n$(包括其排列顺序)、融合参数 α、权因子 $\omega_0,\omega_1,\cdots,\omega_n$ 以及附加权因子 k。基于附权的[n/n]型 RB 曲线的融合方法在生成融合图像时,效果可以由 n 幅图像、权因子和附加权因子以及参数来调整,控制更加灵活。此方法也可以考虑将部分权因子作为公钥,部分权因子作为私钥,以实现密钥共享。

图 4 给出了多幅图像融合与恢复的实验结果。



(a) 公开图像 1　(b) 公开图像 2　(c) 秘密图像

(d) 融合图像　(e) 恢复图像

图 4　多幅图像融合与恢复

Fig. 4　Blending and recovering of many images

($\omega_1=0.6,\omega_2=0.1,\omega_3=0.3,\alpha=0.4,k=-0.3$)

5　算法评价

算法评价包括秘密图像隐藏后融合图像质量评价和恢复图像质量评价两部分。可以采用能见度指标,从视觉感受上主观的评价隐藏秘密图像前后图像间的差异,也可利用定量指标如均方根误差 RMSE、峰值信噪比 PSNR 等客观保真度准则对图像质量做出评价。

(1)均方根误差定义为

$$RMSE = \sqrt{\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[F'(i,j)-F(i,j)]^2}{MN}}$$

RMSE 越小,说明两幅图像越相像。

(2)峰值信噪比定义为

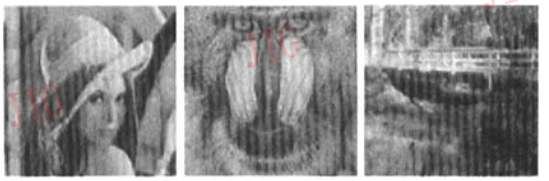
$$PSNR = 10\lg\left[\frac{MN\times255^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}[F'(i,j)-F(i,j)]^2}\right]$$

峰值信噪比 PSNR 值越大,说明图像的保真度越好,两幅图像越相似。

6　数值实验结果与分析

对文献[1]中数字图像的多幅迭代混合方法、文献[2]中利用 Bernstein 多项式基函数融合方法以及基于 n 次有理 Bézier 曲线、k 阶[n/n]型 RB 曲线、附权的[n/n]型 RB 曲线的融合方法进行了图像隐藏和恢复的对比实验。Fabien 等人提出的图像质量基准测试模型中使用峰值信噪比(PSNR)作为衡量标准,但是峰值信噪比中不考虑任何人类视觉系统特性,所以在算法比较时需要用许多不同图像作为公开图像进行测试,以基于多幅图像迭代混合的方法为例说明不能仅以峰值信噪比作为衡量标准。

实验均以 girl 为秘密图像,公开图像集为{(Lena, peppers); (bridge, peppers); (baboon, peppers)},然后把利用上述算法加入秘密图像 girl 后得到的 3 幅融合图像作为图像质量测试集合,而且固定融合参数($\alpha_1=0.8,\alpha_2=0.7$)。测试后的融合图像质量结果如图 5 所示。



(a) PSNR=28.19　(b) PSNR=28.15　(c) PSNR=28.20

图 5　不同公开图像隐藏同幅秘密图像后的融合图像

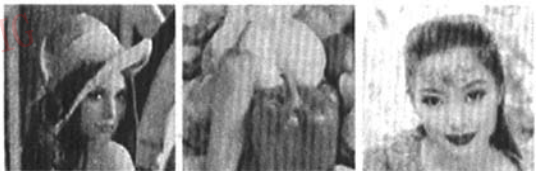
Fig. 5　Blending images with the same private image and different public images

虽然几个融合图像结果的峰值信噪比很接近，但是可以明显地从主观上看出用相同方法隐藏同一幅秘密图像后融合图像质量的差异，所以评价时不能仅从理论统计值上考虑，还要考虑结合人类视系统的主观感觉。

基于融合的多幅数字图像隐藏技术实质是利用一组基函数作为权值将一幅秘密图像隐藏于其他几幅公开图像中。要使隐藏后的融合图像与公开图像 $F_i(i\neq j)$ 相似，需要调整融合参数和权因子使这幅公开图像具有的基函数值 $A_i(x)$ 较大，本文给出的方法正是由于参与的参数多能很好地保证这个需要，而且参数的不同值的组合又增加了密钥，所以本文的方法较文献[1]和文献[2]的方法为优。

为了说明本文方法的优点，应选取相同的公开图像和秘密图像，以 Lena 和 peppers 为公开图像，girl 为秘密图像，对文献[1]中利用 Bernstein 多项式对 $n+1$ 幅图像融合的方法，文献[2]中数字图像的多幅迭代混合方法和基于 n 次有理 Bézier 曲线、k 阶[n/n]型 RB 曲线、附权的[n/n]型 RB 曲线的融合方法进行了图像隐藏和恢复实验对比，实验中按上述原则选取权因子和参数值以确保融合图像和恢复图像的质量。

图 6～图 11 是各种融合方法测试后的部分实验结果，表 1～表 5 为相关的统计数据。



(a) 公开图像 1　(b) 公开图像 2　(c) 秘密图像

图 6　公开图像与秘密图像

Fig. 6　Public image and private image

(a) 融合图像　(b)恢复图像

图 7　基于 Bernstein 多项式融合(融合参数为 0.22)

Fig. 7　Image blending based on Bernstein polynomial (blending parameter: 0.22)

(a) 融合图像　(b)恢复图像

图 8　多幅迭代混合方法[2](融合参数为 0.8,0.7)

Fig. 8　Image blending based on iteration blending of many images(blending parameter: 0.8,0.7)

(a) 融合图像　(b)恢复图像

图 9　n 次有理 Bézier 曲线的融合(融合参数为 8,0.5,5,0.2)

Fig. 9　Image blending based on n-degree rational Bézier curve (blending parameters: 8.0,0.5,5,0.2)

(a) 融合图像　(b)恢复图像

图 10　k 阶[n/n]型 RB 曲线的融合(融合参数为 0.2,0.2)

Fig. 10　Image blending based on k-order [n/n] RB curve (blending parameter:0.2,0.2)

(a) 融合图像　(b)恢复图像

图 11　附权的[n/n]型 RB 曲线的融合(融合参数为 0.5,0.08,0.2,0.3,−0.1)

Fig. 11　Image blending based on weighted [n/n] RB curve (blending parameter: 0.5,0.08,0.2,0.3,−0.1)

数值实验结果表明，本文提出的 3 种方法在融合图像和恢复图像的客观保真度和相像程度上的确

表 1　基于 Bernstein 多项式图像融合的部分测试结果

Tab. 1　Experimental results based on Bernstein polynomial

融合参数 α	融合图像 PSNR	融合图像 RMSE	恢复图像 PSNR	恢复图像 RMSE
0.1	26.0890	12.6500	19.4866	27.0526
0.2	20.5132	24.0370	31.0289	7.1630
0.3	17.4077	34.3680	38.1148	3.1681
0.5	13.6576	52.9249	46.4109	1.2190
0.7	11.1598	70.5584	50.9674	0.7214

表 2　多幅迭代混合[2]的部分测试结果

Tab. 2　Experimental results based on iteration blending

混合[2]参数 α_1,α_2	混合[2]图像 PSNR	混合[2]图像 RMSE	恢复图像 PSNR	恢复图像 RMSE
0.9,0.85	28.2990	9.9082	16.4091	38.5553
0.85,0.8	25.7176	13.2025	22.3313	19.4973
0.8,0.7	22.0731	20.0856	28.1940	9.9275
0.75,0.6	19.4398	27.1989	33.2280	5.5226

表 3　基于 n 次有理 Bézier 曲线融合的部分测试结果

Tab. 3　Experimental results based on n-degree rational

融合参数 $\omega_1,\omega_2,\omega_3,\alpha$	融合图像 PSNR	融合图像 RMSE	恢复图像 PSNR	恢复图像 RMSE
8,0.5,4,0.3	27.8113	10.3747	36.9313	3.6306
15,0.5,3,0.5	22.8137	18.4363	42.6828	1.8724
4,0.5,3,0.2	30.9344	7.2414	31.3366	6.9137
10,1,3,0.3	29.1308	8.9125	32.5855	5.9878
8,0.5,5,0.2	33.8973	5.1482	30.2516	7.8336
12,0.2,3,0.5	21.7103	20.9424	44.7184	1.4812

表 4　基于 k 阶[n/n]型 RB 曲线融合的部分测试结果

Tab. 4　Experimental results based on k-order [n/n] RB curve

融合参数 α,k	融合图像 PSNR	融合图像 RMSE	恢复图像 PSNR	恢复图像 RMSE
0.06,0.9	21.4406	21.6209	15.1642	44.4972
0.1,0.1	25.0960	14.1837	14.5776	47.6060
0.2,0.2	17.9407	32.3224	27.6801	10.5326
0.2,−0.2	21.8519	20.6037	20.8865	23.0258
0.2,−0.05	21.1204	22.4141	23.7782	16.5055

表 5　基于附权的[n/n]型 RB 曲线融合的部分测试结果

Tab. 5　Experimental results based on weighted [n/n] RB curve

融合参数 $\omega_1,\omega_2,\omega_3,\alpha,k$	融合图像 PSNR	融合图像 RMSE	恢复图像 PSNR	恢复图像 RMSE
0.5,0.06,0.25,0.3,−0.1	27.8667	10.3087	28.5975	9.4769
0.6,0.1,0.3,0.4,−0.3	24.6361	14.9533	30.9702	7.2116
1,0.2,0.5,0.4,−0.4	25.5973	13.3867	28.6829	9.3842
0.6,0.1,0.3,0.3,0.1	26.7042	11.7580	31.1689	7.0485
2,1,0.2,0.2	31.5922	6.7132	24.9323	14.4519
2,0.2,1,0.2,1	25.1548	14.0864	32.5574	6.0071
5,0.2,0.5,0.1,10	24.2467	15.6389	33.9058	5.2840
4,0.3,1,0.2,0.8	30.6415	7.4897	25.7750	13.1157
3.5,0.3,0.15,0.14,8	23.3371	17.3655	29.1897	8.8522

优于文献[1]和文献[2]的方法。在本文提出的 3 种方法,又以基于有理 Bézier 曲线融合和基于附权的[n/n]型 RB 曲线融合两种方法为优,其融合图像和恢复图像的客观保真度和相像程度高。由于融合选用的基函数值可以由融合参数和权因子共同调配,使得某个基函数在整组基函数中的比重更容易调节,所以融合参数的经验取值范围宽,即密钥组合很多,而且这些密钥组合能很好地兼顾融合图像和

恢复图像的客观保真度和相像程度。

7 算法的抗攻击性分析

数字图像隐藏算法应具备抗攻击性(无意攻击和恶意攻击)。图 12 给出了基于附权的[n/n]型 RB 曲线的融合方法的鲁棒性实验。实验中分别对融合图像进行了增污、中心切除和随机切除处理。

融合图像 恢复图像

(a) 带有噪声的图像融合与恢复

融合图像 恢复图像

(b) 带有中心切除的图像融合与恢复

融合图像 恢复图像

(c) 带有随机切除的图像融合与恢复

图 12 图像融合的鲁棒性

Fig. 12 Robustness of blending image

恢复秘密图像时需要的 n 幅公开图像在传输时也有可能受到攻击或噪声污染。分别给公开图像 Lena 加高斯噪声(Gauss)、脉冲噪声(salt and pepper)、乘性噪声(speckle)。3 种噪声各有特性,高斯噪声的均值为 0,方差为 0.01;脉冲噪声的脉冲概率为 20%;乘性噪声方差为 0.05。

图 13 为各种噪声污染图像。

以基于附权的[n/n]型 RB 曲线融合为例,假设公开图像在传输时受到以上 3 种噪声的污染,图 14 给出了融合图像受到噪声污染时,恢复的秘密图像所受影响的鲁棒性实验。通过解密后恢复的秘密图

(a) 高斯噪声污染图像 (b) 脉冲噪声污染图像 (c) 乘性噪声污染图像

图 13 各种噪声污染图像

Fig. 13 Image polluted by the different noises

(a) 高斯噪声污染恢复图像 (b) 脉冲噪声污染恢复图像 (c) 乘性噪声污染恢复图像

图 14 公开图像受到各种噪声污染后的恢复图像

Fig. 14 Recovering image with public image polluted by the different noises

像的质量受到的影响结果可通过图 14 看出,公开图像受到高斯噪声、脉冲噪声时,其对恢复出的秘密图像质量影响非常大,而这些影响是致命的。

基于融合的数字图像隐藏技术都存在一个共同的缺点,即解密图像时需要传输 n 幅公开图像和一幅融合图像,如果它们在传输中受到噪声的污染,将会对秘密图像的恢复造成严重的影响,而且本文提出的 3 种方法要设置更多的融合参数和权因子,融合参数有明确的取值范围[0,1],但是权因子就没有具体的取值范围,它们在整个实数域上取值,所以选用起来不太方便。本文仅给出了几种可能经受的攻击,数字图像隐藏算法还要经受各种有意或无意的攻击,因此还需进一步研究以提高算法的抗攻击性和鲁棒性。

8 结 论

本文利用数字图像"分存"的思想,提出了通过 n 次有理 Bézier 曲线、k 阶[n/n]型 RB 曲线、附权的[n/n]型 RB 曲线将一幅秘密图像隐藏于 n 幅公开图像中的融合方法。算法简单、便于实现。由恢复

算法可知,图像的恢复必须依赖于 n 幅融合图像、融合参数、权因子、以及图像和权因子的次序,所以上述 3 种隐藏技术有很强的安全性,附加权的融合方法更提高了安全性,能很好地实现秘密分割和秘密共享。数值实验结果证明算法可行,且可以推广到数字水印的研究和应用中。

参考文献(References)

1 Ding Wei, Yan Wei-qi, Qi Dong-xu. Digital image information hiding technology and its application based on scrambling and amalgamation[J]. Journal of Image and Graphics, 2000, 5(8): 644~649. [丁玮, 闫伟齐, 齐东旭. 基于置乱与融合的数字图像隐藏技术及其应用[J]. 中国图象图形学报, 2000, 5(8): 644~649.]

2 Zhang Gui-cang, Wang Rang-ding, Zhang Yu-jin. Digital image information hiding technology based on iterative blending[J]. Chinese Journal of Computers, 2003, 26(5): 569~574. [张贵仓, 王让定, 章毓晋. 基于迭代混合的数字图像隐藏技术[J]. 计算机学报, 2003, 26(5): 569~574.]

3 Wang Guo-jin, Wang Guo-zhao, Zheng Jian-min. Computer Aided Geometric Design[M]. Beijing: Higher Education Press, 2001. [王国瑾, 汪国昭, 郑建民. 计算机辅助几何设计[M]. 北京: 高等教育出版社, 2001.]